Publications du **La**boratoire de
Combinatoire et d'
Informatique
Mathématique

8

Guy Melançon

Réécritures dans l'algèbre de Lie libre, le groupe libre et l'algèbre associative libre

Département de mathématiques et d'informatique

Université du Québec à Montréal

Responsable de la collection:

Srecko Brlek
LACIM
Université du Québec à Montréal
C.P. 8888, Succ. A
Montréal, Qc.
Canada H3C 3P8 .
e-mail: brlek@lacim.uqam.ca

Ce numéro constitue la publication d'une thèse soutenue devant jury, pour l'obtention du Ph.D.

Composition du Jury

P.M. COHN	*University College, London*
A. JOYAL	*UQAM,*
P. LEROUX	*UQAM,*
C. REUTENAUER	*UQAM,* Directeur
D. THÉRIEN	*Mc Gill University*

Dépôt légal, deuxième semestre 1991, Bibliothèque nationale du Québec.

ISBN 2-89276-094-1 LACIM Montréal

Laboratoire de combinatoire et d'informatique mathématique
Département de mathématiques et d'informatique
Université du Québec à Montréal
C.P. 8888, Succ. A
Montréal, Qc.
Canada H3C 3P8

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

THÈSE PRÉSENTÉE
COMME EXIGENCE PARTIELLE
DU DOCTORAT EN MATHÉMATIQUES

PAR

GUY MELANÇON

RÉÉCRITURES DANS L'ALGÈBRE DE LIE LIBRE, DANS LE GROUPE LIBRE ET DANS L'ALGÈBRE ASSOCIATIVE LIBRE

AVRIL 1991

Résumé

On élabore des systèmes de réécriture et on les applique à la théorie et aux calculs effectifs dans certaines structures algébriques libres.

Dans le monoïde libre, on étudie une famille de factorisations complètes; les mots d'une telle factorisation sont appelés des 'mots de Hall'. Le système de réécriture qu'on y développe permet d'effectuer le calcul de la factorisation (unique) en produit de mots de Hall des mots du monoïde libre. Nous l'utilisons aussi pour montrer d'importantes caractérisations des mots de Hall, qui n'étaient connues que dans le cas où la factorisation est celle formée des 'mots de Lyndon'.

On fait ensuite l'étude détaillée, dans l'algèbre de Lie libre, du redressement des bases de Hall généralisées, à l'aide du système de réécriture développé dans le monoïde libre. Une version adaptée de ce système de réécriture nous permet de faire un travail analogue dans le groupe libre. Dans ce contexte, on montre que les éléments du groupe libre s'écrivent de façon unique comme produit de certains commutateurs. On donne aussi des identités pour calculer les multiplicités de ces commutateurs dans la décomposition d'un élément du groupe libre.

On met au point des algorithmes de calcul des bases standard des idéaux à droite dans l'anneau des polynômes non commutatifs. Une des principales applications de nos résultats est de rendre effectif le travail avec les idéaux et dans le quotient de l'anneau par un idéal. Les résultats sur les idéaux sont ensuite généralisés aux modules à droite sur l'anneau des polynômes non commutatifs.

Remerciements

Je tiens à remercier:

Monsieur P. M. Cohn pour l'honneur et le plaisir qu'il me fait en acceptant de se joindre au jury de cette thèse.

Mon directeur C. Reutenauer, qui m'a amené à la combinatoire des mots. Je lui suis reconnaissant pour tout le temps qu'il m'a dédié et pour ses encouragements constants durant les années d'étude et de recherche qui m'ont conduit à la rédaction de cette thèse.

Messieurs A. Joyal, P. Leroux et D. Thérien de s'être intéressés à ce travail et d'avoir accepté de faire partie du jury.

Je remercie aussi les membres de l'équipe du LaCIM de leur soutien et leurs encouragements tout au long de ce travail.

Enfin, cette thèse n'aurait pas vu le jour si je n'avais été chaudement entouré des membres de ma famille: Milicska, Maya et Elie.

Je dédie ce travail à mes parents.

Table des matières

Introduction

Dans un travail sur l'étude de certains p-groupes, P. Hall [HP 33] effectuait des calculs profonds sur les commutateurs itérés et sur la série centrale descendante du groupe libre. Cet article allait être suivi de plusieurs autres travaux d'importance dans la 'théorie combinatoire des groupes'. Parmi ceux-là, les travaux de Magnus [Ma 35, Ma 37] et de Witt [Wi 37] ont permis de lier le groupe libre à une autre structure algébrique fondamentale: l'algèbre de Lie libre. M. Hall a construit dans [HM 50a] une suite ordonnée de commutateurs dans le groupe libre (qu'il a appelé les 'commutateurs basiques'), qui donnent une base de la série centrale descendante du groupe libre. Dans le même article, il a utilisé les commutateurs basiques pour obtenir une base de l'algèbre de Lie libre qui, depuis, est appelée la 'base de Hall'. Divers auteurs ont par la suite proposé des généralisations des commutateurs basiques (Meier-Wunderli [MW 52], Schützenberger [Sc 58], Širšov [Ši 62], Gorčakov [Go 69], Ward [Wa 69]). Peu de temps après M. Hall, Lyndon [Ly 54, CFL 58] construisait une autre base de la série centrale descendante, qui à l'origine semblait d'une nature différente de celle de la base de Hall.

Les travaux de Viennot [Vi 76] ont réuni dans une même famille toutes les bases qui avaient alors été construites. Il a donné des conditions précises qui décrivent une large famille de bases de l'algèbre de Lie libre qui inclut la base classique de M. Hall et la base de Lyndon. Il a montré comment ces bases peuvent être obtenues à l'aide d'une généralisation de la *'méthode d'élimination de Lazard'*. De plus, il ramenait l'étude des bases de l'algèbre de Lie libre à celle des factorisations du monoïde libre. Ce sont les bases considérées par Viennot que nous appellerons les *'bases de Hall générales'*. Les factorisations qui leur correspondent dans le monoïde libre sont appelées par Viennot 'les factorisations de Lazard'; nous appellerons les mots d'une telle factorisation, des *'mots de Hall'*. On peut construire, à l'aide d'une base de Hall générale, une base de l'algèbre enveloppante de l'algèbre de Lie libre, en vertu du théorème de Poincaré-Birkhoff-Witt (cf. [Hu 72, Ja 62]). On est donc amené à une autre structure algébrique libre. En effet, l'algèbre enveloppante de l'algèbre de Lie libre est précisément l'algèbre associative libre (cf. [Ja 62, Lo 82]). Cette algèbre est celle des polynômes en variables non commutatives; elle est aussi le module libre engendré par les mots du monoïde libre. Dans [MR 89], Melançon et Reutenauer présentaient un système de réécriture qui permet de calculer les mots dans la base de Poincaré-Birkhoff-Witt associée à la base de Lyndon de l'algèbre

de Lie libre. C'est ce système de réécriture qui est ici généralisé pour travailler avec les bases de Hall générales, dans l'algèbre de Lie et son algèbre enveloppante.

Nous démontrons aussi certains résultats sur la factorisation des mots, de façon complètement combinatoire, en utilisant les propriétés du système de réécriture. Dans son travail, Lyndon [CFL 58] donne quatre caractérisations des mots de Lyndon. Un paragraphe entier de [Lo 82] est consacré à l'étude des propriétés très fines de ces mots, par rapport à l'ordre lexicographique sur les mots. Nous montrons dans ce travail que plusieurs des propriétés des mots de Lyndon sont aussi partagées par les mots de Hall, par rapport à un ordre qui généralise l'ordre lexicographique.

Ces calculs dans l'algèbre de Lie libre et dans le monoïde libre trouvent leurs analogues dans le groupe libre. En effet, Magnus [Ma 35, Ma 37] a donné un plongement du groupe libre dans l'algèbre des séries formelles en variables non commutatives. Il met ainsi la filtration naturelle de l'algèbre associative libre en correspondance avec la suite centrale descendante du groupe libre. Aux bases de Hall générales de l'algèbre de Lie libre, il correspond des familles de commutateurs basiques, que nous appelons des '*commutateurs de Hall*'. Il nous a semblé naturel de chercher dans quelle mesure nos méthodes pouvaient être utilisées pour retrouver les résultats dans le groupe libre. On y développe un système de réécriture qui permet de calculer la décomposition des éléments du groupe libre en produit de commutateurs de Hall. Cependant, on n'a plus dans le groupe libre toute la rigidité d'une structure de monoïde et par conséquent, le système de réécriture ne suffit plus à lui seul pour montrer l'unicité de cette décomposition. Pour y arriver, nous avons développé un argument algébrique, comme l'ont fait entre autres M. Hall [HM 50a] et Lyndon [CFL 58]. Nos calculs montrent que les fonctions qui calculent l'exposant d'un commutateur de Hall, dans la décomposition des éléments du groupe libre, sont dans l'algèbre des fonctions sous-mot. Ce résultat permet d'étendre au groupe libre tout entier des identités qui avaient été montrées par Thérien [Th 83] pour le monoïde libre. On en tire de nouvelles démonstrations de deux importants théorèmes. L'un de Magnus [Ma 37] qui caractérise les éléments du $n^{\text{ème}}$ groupe de la série centrale decendante du groupe libre; et l'autre de P. Hall [HP 33] qui donne une expression polynomiale pour l'exposant d'un commutateur de Hall, dans la décomposition d'une puissance d'un élément du groupe libre. Ce théorème lui avait permis de montrer plusieurs résultats importants de la théorie des p-groupes.

Le calcul avec les sous-algèbres de Lie de l'algèbre de Lie libre est lié aux calculs avec les idéaux à droite dans l'algèbre associative libre. En effet, une sous-algèbre de Lie de l'algèbre de Lie libre est exactement égale à la partie de l'idéal à droite qu'elle engendre (dans l'algèbre associative libre), et qui se trouve dans l'algèbre de Lie libre (cf. [Di 74] et [Reu 90]). C'est ce résultat qui motive l'étude que nous faisons des idéaux à droite de l'anneau des polynômes non commutatifs. Il est connu depuis P. M. Cohn [Co 61, Co 69] que les idéaux à droite de cet anneau sont des modules libres (sur l'anneau). Notre point de départ est un théorème de Berstel et Reutenauer [BR 88], qui affirme l'existence

de bases des idéaux à droite liées aux codes préfixes du monoïde libre. L'un des buts recherchés était d'arriver à donner un calcul effectif des bases de Berstel et Reutenauer. Nous avons puisé notre inspiration dans les travaux de P. M. Cohn [Co 61, Co 69] et défini les concepts *'d'indépendance d'une famille de polynômes'*, puis de *'base indépendante'* et de *'base standard'* d'un idéal. Nous donnons des caractérisations de ces bases en termes de codes préfixes associés; de sorte que, en particulier, les bases standard sont des bases qui satisfont les exigences du théorème de Berstel et Reutenauer. Les méthodes que nous employons pour le calcul des bases indépendantes et des bases standard sont analogues aux méthodes utilisées pour le calcul des bases des idéaux des anneaux de polynômes en variables commutatives.

Chapitre 1

Réécritures dans le monoïde libre et dans l'algèbre de Lie libre

1.1 Introduction.

Les bases des algèbres de Lie libres apparaîssent pour la première fois dans un article de M. Hall [HM 50a], bien qu'elles soient implicites dans les travaux de Philip Hall [HP 33] et de Wilhem Magnus [Ma 37] sur le calcul des commutateurs dans le groupe libre. Ces bases, connues sous le nom de 'Bases de Hall', ont inspirées plusieurs auteurs et ont données lieu à plusieurs généralisations: Meier-Wunderli [MW 52], Schützenberger [Sc 58], Širšov [Ši 62], Gorčakov [Go 69], Ward [Wa 69]. Lyndon [CFL 58] a introduit des bases qui à l'origine semblaient différentes des bases de Hall.

Viennot a donné une généralisation de toutes ces constructions et il a montré que, dans un certain sens, sa construction était optimale [Vi 76, Th. 1.2]. Il a aussi montré que sa construction est équivalente au processus d'élimination de Lazard. Ce sont les bases considérées par Viennot que nous appellerons les 'Bases de Hall'.

La construction de ces bases repose sur une construction d'arbres et de mots. Nous appelons ces arbres et ces mots, les arbres de Hall et les mots de Hall. Ils sont définis à l'aide de certaines inégalités (voir (1.1), (1.2) et (1.3) du paragraphe 1.2). L'ensemble des mots de Hall forme une factorisation du monoïde libre, telle que définie par Schützenberger [Sc 65]. Viennot [Vi 76] a exposé de façon exhaustive le lien entre algèbres de Lie libres et factorisations du monoïde libre.

Dans [MR 89], Melançon et Reutenauer présentaient un système de réécriture de suites de mots de Lyndon. Ce système de réécriture permettait de montrer plusieurs identités,

satisfaites par des polynômes construits à partir de la base de Lyndon, dans l'algèbre de polynômes non commutatifs et dans l'algèbre de shuffle. Bien avant, Schützenberger [Sc 58] montrait des formules analogues pour un cas particulier de bases de Hall. C'est dans le but d'unifier ces résultats que nous avons entrepris nos travaux sur les arbres et les mots de Hall. Certaines démonstrations des résultats de [MR 89] utilisaient des propriétés très fines des mots de Lyndon. Il semblait naturel d'une part, de chercher à voir jusqu'à quel point elles étaient ou n'étaient pas exclusives aux mots de Lyndon. D'autres part, il fallait tenter de montrer les identités de [Sc 58] et [MR 89] pour le cas des bases de Hall générales.

Le premier chapitre contient les résultats de ces recherches, qui ont en parties déjà été publiées (voir [Me 91]). Il comporte trois volets. Nous donnons d'abord une nouvelle preuve combinatoire de la factorisation des mots en produit décroissant de mots de Hall, différente de celle de Viennot (Th. 1.4.6). Notre méthode se rapproche de Schützenberger [Sc 58]. Nous utilisons un système de réécriture de suites de mots de Hall et exploitons ses propriétés: convergence, confluence (Prop. 1.4.8) et inversibilité (Prop. 1.4.11). L'algorithme que nous fournit le système de réécriture pour calculer la factorisation des mots est semblable au 'collecting process' de P. Hall [HP 33] et de M. Hall [HM 50a], bien que plus général, et généralise le système de réécriture de [MR 89] (voir Rem. 1.4.3). L'unicité de la factorisation est aussi une conséquence d'une propriété très subtile de la factorisation des facteurs gauches du feuillage des arbres de Hall en produit de feuillages de leurs sous-arbres, qui généralise la 'décomposition normale gauche' de [Sc 58] (Lemme 1.3.1).

Après avoir défini un ordre adéquat sur les mots du monoïde libre, nous montrons que les propriétés des mots de Lyndon se généralisent aux mots de Hall. Les bases de Lyndon se construisent directement des mots de Lyndon, qui s'obtiennent en considérant certaines inégalités par rapport à l'ordre lexicographique sur les mots (voir [Ga 88, Lo 82] pour une présentation). C'est l'ordre lexicographique sur les mots que nous généralisons: étant donné un ensemble H de mots de Hall, on définit un ordre total $<_H$ sur le monoïde libre. Cet ordre coïncide avec l'ordre lexicographique lorsque H est l'ensemble des mots de Lyndon (Prop. 1.5.2). Nous montrons que les mots de Hall satisfont les mêmes propriétés que les mots de Lyndon. Ils sont caractérisés, par rapport à cet ordre $<_H$, par les conditions équivalentes:

(i) ils sont minimaux dans leur classe de conjugaison (Th. 1.5.5),

(ii) ils sont strictement plus petits que leurs facteurs gauches propres (Th. 1.5.13).

De plus, comme c'est le cas pour les mots de Lyndon, la factorisation standard d'un mot de Hall et la factorisation d'un mot en produit décroissant de mots de Hall s'obtiennent en calculant le facteur gauche minimal de ce mot.

Nous montrons aux paragraphes 1.6 et 1.7 que la plupart des résultats de [MR 89] se généralisent au cas des bases de Hall. Nous utilisons le système de réécriture pour calculer dans la base de Poincaré-Birkhoff-Witt associé aux mots de Hall (PBWH). L'écriture d'un mot dans cette base est obtenu en cueillant les éléments de la base PBWH qui pendent aux feuilles d'un arbre de dérivation du mot (Th. 1.6.7). On retrouve les résultats du Th. 2 de [MR 89], en utilisant une propriété du système de réécriture (Lemme 1.4.7). Le théorème du paragraphe 4 du même article reprenait un résultat de Radford [Ra 79] et affirmait que l'algèbre de mélange est isomorphe à une algèbre de polynômes commutatifs. La démonstration de ce résultat repose sur une propriété des mots de Lyndon qui n'est pas vérifiée pour les mots de Hall généraux. Nous montrons pourquoi on ne peut obtenir une autre démonstration de ce résultat à l'aide des bases de Hall générales en fournissant un contre-exemple (Rem. 1.7.9).

1.2 Arbres et mots de Hall: définitions et notations.

Soit A un ensemble; on appellera les éléments de A des *lettres* et A lui-même un *alphabet*. On désigne par $M(A)$ le *magma libre* sur A. Rappelons qu'un *arbre binaire* est un graphe orienté $T = (V, E, r)$ où V est l'ensemble des sommets, E est l'ensemble des arcs et r est un sommet distingué, la *racine de l'arbre*, tels que: (i) il n'y a pas d'arc arrivant en r, (ii) en chaque sommet s qui n'est pas la racine: il arrive en s exactement un arc et soit aucun arc, soit deux arcs sont issus de s, (iii) chaque sommet est accessible depuis la racine. Les *feuilles* de T sont les sommets d'où n'est issu aucun arc. Les éléments de $M(A)$ s'identifient à des arbres binaires dont les feuilles sont étiquettées par des lettres. Le *degré d'un arbre* t est le nombre de feuilles qui pendent à ses branches; on le note $|t|$. Les arbres de degré un sont les lettres de l'alphabet. Tout arbre de degré au moins deux s'écrit $t = [t', t'']$ où t'' (respectivement t') est son *sous-arbre droit immédiat* (resp. *sous-arbre gauche immédiat*). Un *sous-arbre droit* de t est soit t'', soit un sous-arbre droit de t' ou t''; un *sous-arbre d'extrême droite de* t est soit t'', soit un sous-arbre d'extrême droite de t''. On définit de façon analogue les sous-arbres gauches et sous-arbres d'extrême gauche de t. Un *sous-arbre de* t est un sous-arbre gauche ou droit de t, ou t lui-même. Par exemple, soit $A = \{a, b\}$; la représentation en arbre de l'élément $[[a, b][[a, b]b]]$ de $M(A)$ est donnée à la Fig. 1.1. Pour cet élément, $[a, b]$ est à la fois un sous-arbre gauche et un sous-arbre d'extrême gauche. Son sous-arbre droit immédiat est $[[a, b]b]$.

On utilisera les notations $'$ et $''$ pour désigner les sous-arbres immédiats gauches et droits. Par exemple, si $t = [t', t'']$ alors $(t')''$ et $(t'')''$ sont les sous-arbres droits immédiats respectifs de t' et t''.

On désigne par A^* le *monoïde libre* sur A; les éléments de A^* seront appelés des *mots*. Le produit sur A^* est le produit de concaténation. Si $u = a_1 \dots a_n$ et $v = b_1 \dots b_m$ sont des mots de A^* alors leur produit est le mot $uv = a_1 \dots a_n b_1 \dots b_m$. On définit une application canonique f qui va de $M(A)$ vers A^*, par $f(a) = a$ si $a \in A$ et $f(t) = f(t')f(t'')$ si

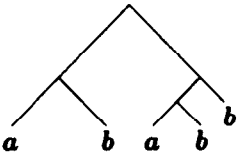

Figure 1.1: Représentation par arbre de $[[a,b][[a,b]b]]$.

$t = [t', t'']$ est de degré au moins deux. Le mot $f(t)$ est appelé le *feuillage* de t. Par exemple, le feuillage de l'arbre de la Fig. 1.1 est $f([[a,b][[a,b]b]]) = ababb$. Appliquer f revient donc à supprimer les crochets. Comme le degré de l'arbre t est égal à la longueur du mot $w = f(t)$, on note la longueur de w aussi par $|w|$.

Soit $H(A)$ un sous-ensemble de $M(A)$, muni d'un ordre total $\leq$, qui contient l'alphabet A, et qui est tel que: pour tout $t = [t', t''] \in H(A)$ de degré ≥ 2, on a $t'' \in H(A)$ et:

$$t < t''. \tag{1.1}$$

Ce sous-ensemble sera appelé un *ensemble de Hall* si de plus, pour tout arbre h de degré ≥ 2, on a $h \in H(A)$ si et seulement si les deux conditions suivantes sont satisfaites:

$$h', h'' \in H(A) \quad \text{et} \quad h' < h'', \tag{1.2}$$

$$\text{soit } h' \text{ est une lettre, soit } h' = [k', k''] \text{ et alors } k'' \geq h''. \tag{1.3}$$

Le deuxième cas de la condition (1.3) est équivalent à dire: si $h = [h', h'']$ alors $(h')'' \geq h''$. Les arbres de $H(A)$ seront appelés des *arbres de Hall*.

Il est important de remarquer que les sous-arbres des arbres de Hall sont eux-mêmes des arbres de Hall. Les arbres de Hall de degré un sont les lettres de A et les arbres de Hall de degré deux sont tous de la forme $[a,b]$ avec $a, b \in A$ et $a < b$.

Exemple 1.2.1 Voici la liste, en ordre ascendant, des arbres de degré au plus cinq d'un ensemble de Hall sur $A = \{a, b\}$ avec $a < b$.

$$[[[[a,b]a]a]a] \ , \ [[[a,b]a][a,b]] \ , \ [[a,b]a] \ , \ [[[a,b]a]a] \ ,$$
$$[a,b] \ , \ [[a,b][[a,b]b]] \ , \ [[[a,b]b]a] \ , \ [[a,b]b] \ ,$$
$$[[[[a,b]b]a]a] \ , \ a \ , \ [[[[a,b]b]b]b] \ , \ [[[a,b]b]b] \ , \ b \ .$$

◇

Lemme 1.2.2 *Soient h, k des arbres de Hall tels que $h < k$ et $h'' \geq k$. Alors*

$$r_p = [[\ldots[h, \underbrace{k]\ldots]k}_{p}]$$

est un arbre de Hall, pour tout $p \geq 1$.

Démonstration. On procède par récurrence sur p. On vérifie que les hypothèses sur h et k satisfont aux conditions (1.2) et (1.3); de sorte que $r_1 = [h, k]$ est bien un arbre de Hall. Maintenant, supposons que r_p est un arbre de Hall. Selon la condition (1.1), on a $r_p < r_p'' = k$ et par construction de l'arbre r, $r_p' = r_{p-1}$, donc $(r_p')'' = k \geq k$. De sorte que les conditions (1.2) et (1.3) sont satisfaites (avec $h' = r_p, h'' = k$) et $r_{p+1} = [r_p, k]$ est un arbre de Hall. ◇

Lemme 1.2.3 *Soit $h = [h', h'']$ un arbre de Hall. Si h_1'' est un sous-arbre droit de h alors $h_1'' \geq h''$.*

Démonstration. On procède par récurrence sur le degré de l'arbre h. Soit h_1'' est h'' lui-même, soit h_1'' est un sous-arbre droit de h' ou h'', par définition. Dans le premier cas on a bien $h_1'' \geq h''$. Par récurrence, on a dans le second cas $h_1'' \geq (h')''$; et dans le troisième cas $h_1'' \geq (h'')''$. Comme les conditions (1.3) et (1.1) donnent respectivement les inégalités $(h')'' \geq h''$ et $(h'')'' > h''$, on obtient bien dans tous les cas $h_1'' \geq h''$. ◇

1.3 Factorisations des facteurs de mots de Hall.

Nous allons maintenant nous intéresser aux facteurs gauches et aux facteurs droits des mots de Hall. Nous allons montrer que l'application *feuillage* est injective, ce qui nous conduira éventuellement à montrer l'unicité de la factorisation des mots en produits décroissants de mots de Hall. Le lemme suivant est d'une importance cruciale.

Lemme 1.3.1 *Soit h un arbre de Hall et $w = f(h)$ son feuillage. Supposons que soit donné une factorisation en mots non vides de w, $w = uv$. Alors il existe des arbres de Hall $k_1, \ldots, k_m, h_1, \ldots, h_n$ tels que:*

$$u = f(k_1) \ldots f(k_m) \ , \ v = f(h_1) \ldots f(h_n) \tag{1.4}$$

et $k_1, \ldots, k_m < h_1, \ h_1 \geq \ldots \geq h_n \geq h''$.

Démonstration. En fait, nous allons montrer plus que ne contient l'énoncé du lemme. Nous allons voir en cours de démonstration que les arbres $h_1, \ldots, h_n$ sont des sous-arbres droits de h. Soit $h = [h', h'']$. Par définition, on a $f(h) = f(h')f(h'')$, et par hypothèse, $f(h) = uv$. Il se peut que $u = f(h')$ et $v = f(h'')$ auquel cas on pose $m = n = 1$, et $k_1 = h', h_1 = h''$. Les conditions annoncées sont alors satisfaites puisque $k_1 < h_1$ et que h_1 est le sous-arbre droit immédiat de h.

Sinon, on considère deux cas et on procède par récurrence sur le degré de h.

Cas 1: $f(h') = ux, v = xf(h'')$, avec x non vide (voir Fig. 1.2). Par récurrence, appliquée

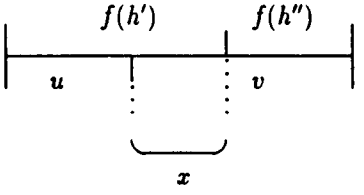

Figure 1.2: $f(h') = ux, v = xf(h'')$.

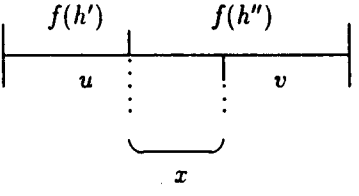

Figure 1.3: $u = f(h')x, f(h'') = xv$.

à h', il existe des arbres $k_1, \ldots, k_m, h_1, \ldots, h_{n-1}$ tels que:

$$u = f(k_1) \ldots f(k_m) \ , \ x = f(h_1) \ldots f(h_{n-1})$$

et $k_1, \ldots, k_m < h_1, h_1 \geq \ldots \geq h_{n-1} \geq (h')''$, où $h_1, \ldots, h_{n-1}$ sont des sous-arbres droits de h'. Comme h' est le sous-arbre gauche immédiat de h, $h_1, \ldots, h_{n-1}$ sont bien des sous-arbres droits de h. On a, par (1.3), $(h')'' \geq h''$. Si on pose $h_n = h''$, on a alors $v = xf(h'') = f(h_1) \ldots f(h_n)$ et on obtient le résultat.

Cas 2: $u = f(h')x, f(h'') = xv$, avec x non vide (voir Fig. 1.3). Par récurrence, appliquée à h'', il existe des arbres $k_2, \ldots, k_m, h_1, \ldots, h_n$ tels que:

$$x = f(k_2) \ldots f(k_m) \ , \ v = f(h_1) \ldots f(h_n)$$

et $k_2, \ldots, k_m < h_1, h_1 \geq \ldots \geq h_n \geq (h'')''$, où $h_1, \ldots, h_n$ sont des sous-arbres droits de h'. Comme h'' est le sous-arbre droit immédiat de h, $h_1, \ldots, h_n$ sont bien des sous-arbres droits de h. On a, par (1.1), $h'' < (h'')''$ et par (1.2), $h' < h''$. On combine ces inégalités pour obtenir $h' < h'' < (h'')'' \leq h_1$. Si on pose $k_1 = h'$, on a alors

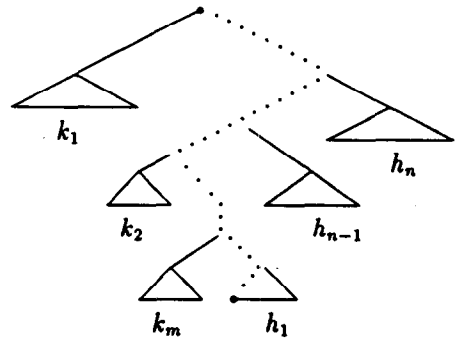

Figure 1.4: Décomposition des facteurs gauche et droit d'un mot de Hall.

$u = f(h')x = f(k_1)\dots f(k_m)$, $v = f(h_1)\dots f(h_n)$ et on obtient encore une fois le résultat. ◇

Remarques 1.3.2 Cette factorisation du facteur droit v peut se calculer en suivant pas à pas les étapes de la récurrence. En particulier, si le Cas 1 est rencontré au moins une fois durant le calcul de la factorisation, alors $v = f(h_1)\dots f(h_n)$ avec $n \geq 2$, et $h_1 \geq (h')''$. Remarquez que le Cas 1 est rencontré si on a $|v| > |h''|$.

Si le Cas 2 est rencontré à la première étape du calcul, alors

$$v = f(h_1)\dots f(h_n), \text{ avec } h_1 \geq \dots \geq h_n \geq (h'')'',$$

puisque dans ce cas, v est un facteur droit de h''. Remarquez que si à chaque étape de la récurrence, on ne rencontre que le Cas 2, alors on est assuré que v est le feuillage d'un sous-arbre d'extrême droite de h. En d'autres mots, si v ne se réduit pas au feuillage d'un sous-arbre d'extrême droite de h alors sa factorisation compte au moins deux facteurs. Ces observations nous seront utiles au paragraphe 1.5.2. ◇

Le Lemme 1.3.1 possède une intéressante interprétation géométrique. Les factorisations (1.4) du facteur gauche u et du facteur droit $v = av'$ peuvent être obtenues en suivant l'unique chemin qui va de la racine de l'arbre à la feuille a, qui est la première lettre de v. Imaginons qu'on suit ce chemin, et qu'à chaque sommet interne de l'arbre on laisse tomber le sous-arbre qui y pend. Les sous-arbres qui tombent à la droite de a (y compris le sous-arbre dont a fait partie) donnent la factorisation de v en produit décroissant de feuillages d'arbres de Hall. Les arbres qui tombent à la gauche de a donnent la factorisation de u et satisfont la condition annoncée. (Voir Fig. 1.4).

A partir de maintenant nous dirons qu'un mot est un *mot de Hall* s'il est le feuillage d'un arbre de Hall. Le prochain lemme nous dit que l'application 'feuillage' f est injective. Désignons par H_d l'ensemble des arbres de Hall de degré au plus d. Remarquez que si $h \in H_{d+1}$ alors $h', h'' \in H_d$.

Théorème 1.3.3 *Tout mot de Hall est l'image d'un unique arbre de Hall. Si un mot de Hall, $w = f(h)$, peut être écrit en un produit décroissant de mots de Hall:*

$$w = f(h_1)\dots f(h_n), \text{ avec } h_1 \geq \dots \geq h_n,$$

alors on a $n = 1$.

Démonstration. On montre le résultat par récurrence sur d, le degré des arbres. Le cas $d = 1$ est facilement vérifié. Supposons le théorème vrai pour les arbres de degré d et soit $t = [t', t'']$ un arbre de Hall de degré $d + 1$ tel que:

$$f(t) = f(t')f(t'') = f(h_1)\dots f(h_n), \text{ avec } h_1 \geq \dots \geq h_n. \tag{1.5}$$

Nous allons montrer que $n = 1$. Il nous faut distinguer trois cas selon les longueurs respectives de t'' et h_n.

Cas 1: $|t''| = |h_n|$. Comme f préserve les longueurs, on a par (1.5), que $f(t') = f(h_1)\dots f(h_{n-1})$ et $f(h_n) = f(t'')$. La récurrence appliquée à t' nous donne $h_1 = t'$ et $n-1 = 1$, donc $n = 2$. La récurrence appliquée à t'' nous donne $h_n = t''$. Mais par (1.2), on a $t' < t''$ et par hypothèse $h_1 \geq h_2$. On obtient donc une contradiction; le Cas 1 ne peut survenir.

Cas 2: $|t''| > |h_n|$. Encore une fois, par (1.5), on a $f(t'') = vf(h_{i+1})\dots f(h_n)$ où v est un facteur droit propre de $f(h_i)$. Observez que v est non vide: si on suppose au contraire que v est vide, alors c'est que $f(t'') = f(h_{i+1})\dots f(h_n)$; de sorte que par récurrence, cette factorisation ne contient qu'un seul facteur, d'où $n = i + 1$, ce qui contredit l'inégalité stricte $|t''| > |h_n|$.

Comme v est facteur propre de $f(h_{i+1})$, on déduit du Lemme 1.3.1 une factorisation $v = f(k_1)\dots f(k_m)$ où $k_1, \dots, k_m$ sont des arbres de Hall satisfaisant $k_1 \geq \dots \geq k_m \geq h_i''$. De la condition (1.1) appliquée à h_i, et de l'inégalité $h_i \geq h_{i+1}$, on obtient $k_1 \geq \dots \geq k_m \geq h_{i+1} \geq \dots \geq h_n$; on a donc:

$$f(t'') = f(k_1)\dots f(k_m)f(h_{i+1})\dots f(h_n).$$

Il y a dans ce produit au moins deux facteurs puisque $i < n$ et $m \geq 1$. On contredit donc l'hypothèse de récurrence faite sur t''. Le Cas 2 ne peut survenir.

Cas 3: $|t''| < |h_n|$. Encore une fois, par (1.5), on a $f(h_n) = vf(t'')$ où v est un facteur droit de t'. Le facteur v est non vide, en vertu de l'inégalité stricte $|t''| < |h_n|$. Maintenant, si $n > 1$ alors v doit être un facteur droit propre de t' et selon le Lemme 1.3.1, il existe des arbres de Hall $k_1, \dots, k_m$ tels que:

$$v = f(k_1)\dots f(k_m), \text{ avec } k_1 \geq \dots \geq k_m \geq (t')''.$$

Comme par (1.3), $(t')'' \geq t''$, le mot de Hall $f(h_n)$ se factorise en:

$$f(h_n) = f(k_1)\dots f(k_m)f(t''), \text{ avec } k_1 \geq \dots \geq k_m \geq t''.$$

Observez aussi que $n > 1$ implique $h_n \in H_d$, donc la récurrence s'applique à h_n. Mais, comme dans le Cas 2, la factorisation de h_n qu'on vient d'exhiber nous mène à une contradiction puisqu'elle compte au moins deux facteurs.

On est donc forcé d'avoir $n = 1$.

Il reste à montrer que si h et k sont des arbres de Hall tels que $f(h) = f(k)$ alors $h = k$. On procède par récurrence sur le degré des arbres; on vérifie facilement que f est injective sur A. Soit $h = [h', h'']$ et $k = [k', k'']$, de sorte que $f(h) = f(h')f(h'') = f(k')f(k'') = f(k)$. On peut supposer que $|h''| \geq |k''|$. Si $|h''| = |k''|$, alors c'est que $f(h') = f(k'), f(h'') = f(k'')$ et par récurrence $h' = k', h'' = k''$, d'où $h = k$. Si $|h''| > |k''|$, alors $f(h'') = vf(k'')$ où v est un facteur droit propre de k'. Selon le Lemme 1.3.1, on peut factoriser v en:

$$v = f(r_1)\dots f(r_m),$$

où $r_1, \dots, r_m$ sont des arbres de Hall satisfaisant $r_1 \geq \dots \geq r_m \geq (k')''$. Selon la condition (1.3), $(k')'' \geq k''$, de sorte que:

$$f(h'') = f(r_1)\dots f(r_m)f(k''), \text{ avec } r_1 \geq \dots \geq r_m \geq k''.$$

Cette factorisation compte au moins deux facteurs. On aboutit donc à une contradiction puisque par hypothèse $f(h'')$ ne peut être écrit en un produit décroissant de feuillages d'au moins deux arbres de Hall. ◇

Le Th. 1.3.3 nous permet d'identifier un mot de Hall à l'unique arbre de Hall dont il est le feuillage. Nous désignerons aussi par $H(A)$ l'ensemble des mots de Hall dans A^*. Cet ensemble de mots est totalement ordonné par l'ordre $\leq$ sur les arbres de Hall.

1.4 Réécritures de suites standard de mots de Hall.

En transportant, à l'aide de f, les arbres de Hall de $H(A)$ dans A^*, on importe aussi les propriétés que satisfont les arbres. Soit h un mot de Hall et t l'unique arbre de Hall dont il est le feuillage, $h = f(t)$. Si h n'est pas une lettre alors $t = [t', t'']$; soit $h' = f(t'), h'' = f(t'')$. On a donc $h = h'h''$; nous appelons cette factorisation de h, sa *factorisation standard.* Nous utiliserons les notations $'$ et $''$ pour désigner la factorisation standard des mots de Hall. Nous reprenons les inégalités (1.1), (1.2) et (1.3) dans le contexte des mots de Hall.

Soit h un mot de Hall et $h = h'h''$ sa factorisation standard. Alors:

$$h < h'', \tag{1.6}$$

$$h' < h''. \tag{1.7}$$

Soit k un autre mot de Hall tel que $h < k$. Alors hk est un mot de Hall de factorisation standard $(hk)' = h, (hk)'' = k$ si et seulement si

$$\text{soit } h \text{ est une lettre, soit } h'' \geq k. \tag{1.8}$$

Nous considérons maintenant des suites de mots de Hall:

$$s = (h_1, \ldots, h_n), \quad h_1, \ldots, h_n \in H(A).$$

La *longueur* de la suite s, qu'on note $|s|$, est égale au nombre de termes qui la composent. Une telle suite sera appelée *suite standard* si pour tout $i = 1, \ldots, n-1$:

$$\text{soit } h_i \text{ est une lettre, soit } h_i = h_i' h_i'' \text{ et alors } h_i'' \geq h_{i+1}, \ldots, h_n. \tag{1.9}$$

Une suite de lettres est une suite standard. Une suite décroissante de mots de Hall est standard. En effet, soit $s = (h_1, \ldots, h_n)$, avec $h_1 \geq \ldots \geq h_n$. Alors $h_i = h_i' h_i''$ et par (1.6), $h_i'' > h_i$, de sorte que $h_i'' > h_{i+1}, \ldots, h_n$.

Une *montée* d'une suite $s = (h_1, \ldots, h_n)$ est un couple de mots *consécutifs* (h_i, h_{i+1}) tels que $h_i < h_{i+1}$. Une *montée éloignée* d'une suite est un couple de mots de la suite:

$$(h_i, h_j) \text{ tels que } i < j \text{ et } h_i < h_j. \tag{1.10}$$

Soit s une suite standard qui n'est pas décroissante; une *montée légale* de cette suite est une montée (h_i, h_{i+1}) telle que:

$$h_{i+1} \geq h_{i+2}, \ldots, h_n. \tag{1.11}$$

Remarque 1.4.1 Toute sous-suite d'une suite standard est une suite standard. De plus, si $\bar{s}$ est une sous-suite d'une suite standard s et si h et k sont des termes consécutifs de $\bar{s}$ tels que (h, k) est une montée légale de s, alors (h, k) est une montée légale de $\bar{s}$. ◇

On définit deux suites s' et s'' obtenues de s par réécriture:

$$s' = (h_1, \ldots, h_{i-1}, h_i h_{i+1}, h_{i+2}, \ldots, h_n), \tag{1.12}$$

$$s'' = (h_1, \ldots, h_{i-1}, h_{i+1}, h_i, h_{i+2}, \ldots, h_n). \tag{1.13}$$

Remarque 1.4.2 En d'autres mots, s' est obtenue de s en concaténant les deux mots h_i et h_{i+1}, et s'' est obtenue de s en échangeant les deux mots h_i et h_{i+1}. Si $s = (h_1, \ldots, h_n)$ est une suite standard le mot $w = h_1 \ldots h_n$ obtenu de s en concaténant ses facteurs sera appelé *le mot associé à* s. Par conséquent, les mots associés à s et s' sont égaux. ◇

Remarques 1.4.3 La suite s est donc réécrite en deux suites s' et s''. Dans [MR 89], un système de réécriture similaire est défini; on y réécrit des suites standard de mots de Lyndon (voir la Rem. 1.5.1), en réécrivant à chaque étape la montée la plus à droite de la suite. Comme dans ce cas on a $h_{i+1} \geq h_{i+2} \geq \ldots \geq h_n$, la condition (1.11) est assurément vérifiée.

Dans [Sc 58], on ajoute à (1.6), (1.7) et (1.8) la condition supplémentaire $h < h'$, pour que le mot h soit un mot de Hall. Un système de réécriture qui travaille sur des *suites licites* y est défini. La suite $s = (h_1, \ldots, h_n)$ est appelée *licite* si pour tout couple de mots consécutifs (h_i, h_{i+1}), soit $h_i \geq h_{i+1}$, soit $h_i h_{i+1}$ est un mot de Hall. La condition supplémentaire $h < h'$ est alors utilisée pour montrer qu'on obtient une suite licite en réécrivant la montée la plus à droite d'une suite licite.

Dans [HM 50a] et [HM 59, Chap. 11], les arbres de Hall sont considérés comme des commutateurs dans le groupe libre sur l'alphabet A. Les suites de tels commutateurs sont réécrites en utilisant le '*collecting process*'. On réécrit les montées $h_i < h_{i+1}$ où h_{i+1} est un mot maximal parmi les mots de la suite. La condition (1.11) est alors trivialement vérifiée puisqu'on a $h_{i+1} \geq h_j$, pour tout j. Nous aborderons la réécriture des suites standard de commutateurs de Hall au Chap. **2**. ◇

Proposition 1.4.4 *Soit $s = (h_1, \ldots, h_n)$ une suite standard de mots de Hall. Si la montée (h_i, h_{i+1}) est légale, alors s' et s'' sont des suites standard de mots de Hall. De plus, la factorisation standard du produit $h_i h_{i+1}$ est $(h_i h_{i+1})' = h_i$ et $(h_i h_{i+1})'' = h_{i+1}$.*

Démonstration. On a $h_i < h_{i+1}$. Soit h_i est une lettre, soit $h_i = h_i' h_i''$ et alors $h_i'' \geq h_{i+1}$, selon (1.9). Donc, en vertu de (1.8), $h_i h_{i+1}$ est un mot de Hall avec la factorisation standard annoncée.

Pour montrer que s' est standard il faut montrer que (i) $h_j'' \geq h_i h_{i+1}$ pour $j = 1, \ldots, i-1$ et (ii) $h_{i+1} \geq h_{i+2}, \ldots, h_n$. Le point (ii) est vérifié puisque (h_i, h_{i+1}) est une montée légale de s. Soit $h_j = h_j' h_j''$ la factorisation standard de h_j. Alors, par (1.9) on a $h_j'' \geq h_{i+1}$ pour $j < i$, et par (1.6) on a $h_{i+1} > h_i h_{i+1}$. Donc $h_j'' > h_i h_{i+1}$, et la suite s' est standard.

Pour montrer que s'' est standard, il suffit de vérifier que $h_{i+1}'' \geq h_i$. Mais on a $h_i < h_{i+1}$, puisque (h_i, h_{i+1}) est une montée de la suite et $h_{i+1} < h_{i+1}''$, par (1.6). Donc $h_{i+1}'' > h_i$ et la suite s'' est standard. ◇

Remarque 1.4.5 Le système de réécriture peut être utilisé pour effectuer des calculs dans l'algèbre de Lie libre et dans son algèbre enveloppante. En effet, lorsqu'aux suites on associe un produit de polynômes de Lie (obtenus des arbres de Hall), on a, dans l'algèbre des polynômes non commutatifs, $s = s' + s''$. Cet aspect ne nous intéressera qu'aux paragraphes 1.6 et 1.7. Pour l'instant, nous concentrerons notre attention sur la suite s'. ◇

Le résultat suivant a déjà été trouvé par plusieurs auteurs à divers degré de généralité (par rapport à l'ordre sur $H(A)$) (voir [Vi 76]). Nous en donnons une nouvelle démonstration.

Théorème 1.4.6 *Tout mot $w \in A^*$ peut être écrit de façon unique en un produit décroissant de mots de Hall:*

$$w = h_1 \dots h_n, \text{ avec } h_1 \geq \dots \geq h_n.$$

Nous donnons d'abord un lemme qui sera utile dans la preuve du Th. 1.4.6 et ailleurs.

Lemme 1.4.7 *Soient $w = h_1 \dots h_n$, avec $h_1 \geq \dots \geq h_n$, et v un facteur droit propre du mot h_i. Alors si $v = r_1 \dots r_m$ est la factorisation de v donnée par le Lemme 1.3.1, on a $r_m > h_{i+1}$ et le mot $vh_{i+1} \dots h_n$ peut être écrit comme produit décroissant de mots de Hall:*

$$vh_{i+1} \dots h_n = r_1 \dots r_m h_1 \dots h_n.$$

Démonstration. Si v est vide il n'y a rien à montrer. Si v est non vide alors soit $v = r_1 \dots r_m$ la factorisation de v donnée par le Lemme 1.3.1. On a $r_1, \dots, r_m \in H(A)$ et $r_1 \geq \dots \geq r_m \geq h_i''$. Comme $h_i'' > h_i$, par (1.6), et $h_i \geq h_{i+1}$, par hypothèse, on a $r_m > h_{i+1}$ et on peut écrire le mot $vh_{i+1} \dots h_n$ comme un produit décroissant de mots de Hall: $vh_{i+1} \dots h_n = r_1 \dots r_m h_1 \dots h_n$. ◇

Démonstration du Th. 1.4.6. **Existence.** Le système de réécriture nous fournit un algorithme pour calculer une factorisation d'un mot w en un produit de mots de Hall. On peut calculer des suites standard successives $s_0, s_1 = s_0', \dots, s_p = s_{p-1}'$ avec $s_p = (h_1, \dots, h_n)$, $h_1 \geq \dots \geq h_n$ et $w = h_1 \dots h_n$.

Si $w = a_1 \dots a_n$ alors $s = (a_1, \dots, a_n)$ est une suite standard. On prend $s_0 = (a_1, \dots, a_n)$ et on calcule $s_1 = s_0', s_2 = s_1', \dots$ Après un moment, on arrive à $s_p = (h_1, \dots, h_n)$, $h_1 \geq \dots \geq h_n$. En vertu de la Rem. 1.4.2, on a $w = h_1 \dots h_n$; on a donc montré l'existence de la factorisation.

Unicité. Supposons que le mot w possède plus d'une factorisation:

$$w = k_1 \dots k_m = h_1 \dots h_n,$$

où les k_i et les h_j sont des mots de Hall satisfaisant $k_1 \geq \dots \geq k_m, h_1 \geq \dots \geq h_n$. On procède par contradiction. On peut supposer $n > 1$ et $m > 1$, en vertu du Th. 1.3.3. De plus, on peut supposer que $|k_m| > |h_n|$ (puisque $|k_m| = |h_n|$ implique, par récurrence, $m = n$ et $k_i = h_i$).

On doit donc avoir $k_m = vh_{i+1} \dots h_n$ où $i < n$ et v est un facteur droit non vide de h_i. Le cas $v = h_i$ ne peut se produire, en vertu du Th. 1.3.3. Donc, v est un facteur droit propre et non vide de h_i et selon le Lemme 1.4.7, k_m se factorise en:

$$k_m = vh_{i+1} \dots h_n = r_1 \dots r_p > h_{i+1} \dots h_n,$$

avec $r_1, \ldots, r_p \in H(A)$ et $r_1 \geq \ldots \geq r_p h_{i+1} \geq \ldots \geq h_n$. On contredit donc le Th. 1.3.3; ce qui termine la démonstration. ◇

Nous allons donner une deuxième démonstration de l'unicité de la factorisation des mots (voir Cor. 1.4.12) en utilisant les propriétés du système de réécriture. On définit une relation, qu'on note $\rightarrow$, sur l'ensemble des suites standard de mots de Hall, en posant: $s \rightarrow t$ si et seulement si $t = s'$ où s' est définie par (1.12). En d'autres mots, $s \rightarrow t$ si et seulement si t est obtenue de s en concaténant deux mots d'une montée légale de s. Si $s \rightarrow t$, on dit que t est dérivée de s.

Proposition 1.4.8 *La relation $\rightarrow$ est confluente. Plus précisément, si s, s_1 et s_2 sont des suites standard dérivées de s, alors il existe une suite standard t telle que $s_1 \rightarrow t$ et $s_2 \rightarrow t$.*

Nous formulons en un lemme un résultat nécéssaire dans la preuve de la proposition, et que nous utiliserons au Chap. 2.

Lemme 1.4.9 *Soit s une suite standard et soient $(h_i, h_{i+1}), (h_j, h_{j+1})$ deux montées légales distinctes de la suite s, avec $i < j$. Alors on a $i + 1 < j$.*

Démonstration. Supposons qu'au contraire on ait $i + 1 = j$. Alors $h_{i+1} = h_j$, de sorte que $h_{i+1} < h_{j+1}$ puisque (h_j, h_{j+1}) est une montée de la suite. Comme la montée (h_i, h_{i+1}) est légale, on a aussi $h_{i+1} \geq h_{i+2}, \ldots, h_n$, en vertu de (1.11); de sorte que $h_{i+1} \geq h_{j+1}$, et on obtient une contradiction. ◇

Démonstration de la Prop. 1.4.8. Comme $s \rightarrow s_1$ et $s \rightarrow s_2$, il existe deux montées légales distinctes dans s, (h_i, h_{i+1}) et (h_j, h_{j+1}). On sait, en vertu du Lemme 1.4.9, que $i+1 < j$, de sorte que:

$$s_1 = (h_1, \ldots, h_{i-1}, h_i h_{i+1}, \ldots, h_j, \ldots, h_n),$$

$$s_2 = (h_1, \ldots, h_i, h_{i+1}, \ldots, h_j h_{j+1}, \ldots, h_n).$$

Nous allons montrer que (h_j, h_{j+1}) est une montée légale de s_1 et que (h_i, h_{i+1}) est une montée légale de s_2. Il est clair que (h_j, h_{j+1}) est une montée légale de s_1, puisque les termes qui se trouvent à droite de h_{j+1} dans s_1 sont les mêmes que ceux qui se trouvent à droite de h_{j+1} dans s. Pour montrer que la montée (h_i, h_{i+1}) est légale dans s_2, il suffit de montrer que $h_{i+1} \geq h_j h_{j+1}$. Or, comme (h_i, h_{i+1}) est une montée légale de s, et que $i + 1 < j$, on obtient de (1.11), $h_{i+1} \geq h_{j+1}$. De (1.6), on a $h_{j+1} > h_j h_{j+1}$, de sorte que $h_{i+1} \geq h_j h_{j+1}$. Par conséquent, on peut effectuer dans s_1 et s_2 les réécritures sur les montées (h_j, h_{j+1}) et (h_i, h_{i+1}), respectivement. Ces réécritures donnent la même suite t:

$$t = (h_1, \ldots, h_i h_{i+1}, \ldots, h_j h_{j+1}, \ldots, h_n).$$

◇

On notera $\stackrel{*}{\rightarrow}$ la fermeture réflexive et transitive de la relation $\rightarrow$. On dira encore que t est dérivée de s si $s \stackrel{*}{\rightarrow} t$. Si $s \stackrel{*}{\rightarrow} t$ est la chaine de réécritures $s = s_0 \rightarrow s_1 \rightarrow \ldots \rightarrow s_n = t$, alors on dira que la dérivation $s \stackrel{*}{\rightarrow} t$ est de longueur n. On montre facilement, par récurrence sur la longueur des dérivations et en utilisant la Prop.1.4.8, le corollaire suivant:

Corollaire 1.4.10 *La relation $\stackrel{*}{\rightarrow}$ est confluente.* ◇

Les suites de lettres sont standard. Selon la Prop. 1.4.4, toutes les suites dérivées des suites de lettres sont standard. La proposition qui suit montre que toute suite standard est une suite dérivée d'une suite de lettres.

Proposition 1.4.11 *Soit $t = (h_1, \ldots, h_n)$ une suite standard. Si les mots de Hall $h_1, \ldots, h_n$ ne sont pas tous des lettres alors il existe une suite standard s telle que $s \rightarrow t$.*

Démonstration. Soit h_i un mot de Hall dans t, non réduit à une lettre et tel que pour tout $j = 1, \ldots, i-1$, soit h_j est une lettre, soit $h''_j \geq h_i$ (un tel mot existe, il suffit de prendre le mot le plus à gauche dans t qui n'est pas une lettre). Nous allons montrer que la suite:

$$s = (h_1, \ldots, h_{i-1}, h'_i, h''_i, h_{i+1}, \ldots, h_n)$$

est standard et que (h'_i, h''_i) en est une montée légale.

On a par (1.6) que $(h''_i)'' > h''_i$, et par (1.8) que $(h'_i)'' > h''_i$, et que $h''_i \geq h_j$ pour $j = i+1, \ldots, n$, puisque t est standard. Comme $h''_j \geq h''_i$ pour $j = 1, \ldots, i-1$, par hypothèse, et $h''_i > h'_i$ par (1.7), on a $h''_j \geq h'_i, h''_i$ pour $j = 1, \ldots, i-1$. Cela montre que s est standard. Comme t est standard, la montée (h'_i, h''_i) est légale puisque par (1.9), $h''_i \geq h_{i+1}, \ldots, h_n$. On peut donc dériver t de s. ◇

Corollaire 1.4.12 (Unicité de la factorisation)

Démonstration. Premièrement, soit $s = (h_1, \ldots, h_m)$ une suite standard et $w = h_1 \ldots h_m = a_1 \ldots a_p$ ($a_i \in A$) le mot associé à s. Alors, à l'aide d'une récurrence utilisant la Prop. 1.4.11, on montre qu'il existe une dérivation $(a_1, \ldots, a_p) \stackrel{*}{\rightarrow} s$.

Supposons que w possède plus d'une factorisation en produit décroissant de mots de Hall:

$$w = h_1 \ldots h_m = k_1 \ldots k_n,$$

avec $h_1 \geq \ldots \geq h_m$ et $k_1 \geq \ldots \geq k_n$. Comme on l'a remarqué précédemment, les suites décroissantes $s_1 = (h_1, \ldots, h_m)$ et $s_2 = (k_1, \ldots, k_n)$ sont standard. Il existe donc des dérivations:

$$(a_1, \ldots, a_p) \stackrel{*}{\rightarrow} (h_1, \ldots, h_m) \text{ et } (a_1, \ldots, a_p) \stackrel{*}{\rightarrow} (k_1, \ldots, k_n).$$

Selon le Cor. 1.4.10, il existe une suite standard t telle que $s_1 \stackrel{*}{\rightarrow} t$ et $s_2 \stackrel{*}{\rightarrow} t$. Or, la seule suite qu'il est possible de dériver d'une suite décroissante est elle-même. On doit donc avoir $s_1 = t = s_2$, ce qui montre l'unicité de la factorisation. ◇

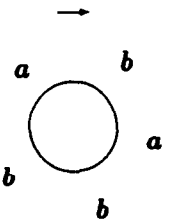

Figure 1.5: Mot circulaire associé à la classe de conjugaison de *ababb*.

1.5 Propriétés 'à la Lyndon' des mots de Hall.

1.5.1 Conjugaison.

Un mot non vide $w \in A^*$ est un mot *primitif* s'il n'est pas puissance d'un autre mot; c'est-à-dire w est primitif s'il est non vide et si $w = z^n$ implique $n = 1$ et $w = z$. Par exemple, le mot *ababb* est primitif alors que *abbabb* ne l'est pas puisque $abbabb = (abb)^2$. Nous allons voir que les mots de Hall sont des mots primitifs.

Deux mots $w, z \in A^*$ sont *conjugués* si et seulement s'il existe deux mots $u, v \in A^*$ tels que $w = uv$ et $z = vu$. Par exemple, les mots *ababb* et *abbab* sont conjugués; on peut prendre dans ce cas-ci $u = ab$ et $v = abb$. La relation 'être conjugué à' est une relation d'équivalence sur A^*, puisque w est conjugué à z si ce dernier peut être obtenu de w par une permutation circulaire de ses lettres. La *classe de conjugaison* d'un mot peut être vue comme un mot circulaire. Les membres de la classe sont alors obtenus en lisant le mot circulaire, en commençant par chacune de ses lettres. Par exemple, le mot circulaire associé à la classe de conjugaison du mot $w = ababb$ apparaît à la Fig. 1.5. Sa classe de conjugaison est $\{ababb, babba, abbab, bbaba, babab\}$.

Si w et z sont conjugués, alors w est primitif si et seulement si z l'est. Supposons que w n'est pas primitif, c'est-à-dire que $w = z^n$, avec z non vide et $n \geq 2$. Alors si on prend $u = z^i$ et $v = z^j$ avec $i + j = n$, on obtient $w = uv = vu$. On voit donc que si w n'est pas primitif, ses conjugués ne sont pas tous distincts. Pour plus de détails le lecteur est renvoyé à [Lo 82].

Soit $H(A)$ un ensemble de Hall fixé dans A^*. On introduit un ordre $<_H$ sur A^* qui utilise la factorisation des mots en produit décroissant de mots de Hall. Soient w et z deux mots de A^* et leurs factorisations en produits décroissants de mots de Hall:

$$w = k_1 \dots k_m, \quad z = h_1 \dots h_n \ .$$

On dit que w précède z, et on écrit $w <_H z$, si et seulement si l'une des deux conditions suivantes est satisfaite:

soit $m < n$ et $k_i = h_i$ pour tout $i = 1, \dots, m$,

soit il existe un indice i tel que:

$$k_1 = h_1, \ldots, k_{i-1} = h_{i-1}, \text{ et } k_i < h_i \ ,$$

où les mots k_i et h_i sont comparés selon l'ordre $<$ sur l'ensemble des mots de Hall.

Remarque 1.5.1 Nous allons tourner momentanément notre attention sur les *mots de Lyndon*. Ils forment un exemple important d'ensemble de mots de Hall. Nous allons montrer que l'ordre $<_L$ construit avec cet ensemble de Hall particulier coïncide avec l'ordre lexicographique $<_{lex}$ à partir duquel les mots de Lyndon sont construits. Cette observation nous a mené aux résultats des paragraphes 1.5.1 et 1.5.2. Ils généralisent des propriétés connues des mots de Lyndon aux mots des ensembles de Hall arbitraires.

Pour plus de détails sur ce qui est discuté dans cette remarque le lecteur est renvoyé à [Ga 88, Lo 82]. On désigne par $<_{lex}$ l'ordre lexicographique sur A^*. Plus précisément, supposons que soit donné un ordre total $<$ sur l'alphabet A; on étend cet ordre à A^* tout entier en posant: $w <_{lex} z$ si et seulement si soit w est un facteur gauche de z, soit il existe des mots s, t_1, t_2 et des lettres a, b tels que:

$$w = sat_1, \quad z = sbt_2, \quad \text{avec } a < b.$$

L'ensemble des mots de Lyndon L est l'ensemble des mots qui sont strictement plus petits que leurs facteurs droits propres, pour l'ordre $<_{lex}$. On peut montrer, de façon équivalente, que les mots de Lyndon sont les représentants minimaux des classes de conjugaison de mots primitifs. Maintenant, si $u \in L$ et si y est le plus long facteur droit de u qui est un mot de L, alors $u = xy$ et x est aussi un mot de Lyndon et ils vérifient $x <_{lex} xy <_{lex} y$. Cette factorisation de u est appelée sa factorisation standard. On peut montrer que si v est un autre mot de Lyndon tel que $u <_{lex} v$ alors uv est un mot de Lyndon, et la factorisation uv est standard si et seulement si $y \geq_{lex} v$. Les mots de Lyndon satisfont donc les conditions (1.6), (1.7) et (1.8). La factorisation standard des mots de Lyndon est utilisée pour associer à chaque mot un arbre de $M(A)$. On peut montrer que l'ensemble des arbres de Lyndon, muni de l'ordre $<_{lex}$ est un ensemble de Hall.

En vertu du Th. 1.4.6, tout mot se factorise de façon unique en produit décroissant de mots de Lyndon et par conséquent, on peut considérer l'ordre $<_L$ sur le monoïde libre A^*.

Proposition 1.5.2 *L'ordre $<_L$ coïncide avec l'ordre lexicographique sur A^*.*

Démonstration. Notez que $w <_{lex} z$ si et seulement si $uw <_{lex} uz$, pour tout $u \in A^*$. On procède par récurrence sur $|w| + |z|$ pour montrer que $w <_L z$ implique $w <_{lex} z$. Cela montrera que les deux ordres sont les mêmes.

Si w et z sont des lettres le résultat est vrai. Supposons que $w <_L z$. C'est-à-dire:

$$w = u_1 \dots u_m,\ z = v_1 \dots v_n,$$

avec $u_i, v_j \in L$, $u_1 \geq_{lex} \dots \geq_{lex} u_m, v_1 \geq_{lex} \dots \geq_{lex} v_n$ et:

soit $m < n$ et $u_1 = v_1, \dots, u_m = v_m$,

soit $u_1 = v_1, \dots, u_{k-1} = v_{k-1}$ et $u_k \geq_{lex} v_k$.

Dans le premier cas, on tire de la définition de l'ordre $<_{lex}$, que $w <_{lex} z$. Il reste à considérer le second cas. Si u_k n'est pas un facteur gauche de v_k, ou si u_k est un facteur gauche de v_k et que $k = m$ alors on obtient facilement $w <_{lex} z$. Supposons donc que u_k est un facteur gauche propre de v_k et que $k < m$. On a $v_k = u_k x$ où x est non vide. Soit $x = h_1 \dots h_p$, avec $h_1 \geq_{lex} \dots \geq_{lex} h_p$, sa factorisation en produit décroissant de mots de Lyndon. Comme les mots de Lyndon sont plus petits que leurs facteurs droits propres, on a $h_p > v_k$. On obtient donc la factorisation en produit décroissant de mots de Lyndon: $xv_{k+1} \dots v_n = h_1 \dots h_p v_{k+1} \dots v_n$. On utilise maintenant l'ordre $<_L$ pour comparer les mots $u_{k+1} \dots u_m$ et $xv_{k+1} \dots v_n$. Comme $xv_{k+1} \dots v_n = h_1 \dots h_p v_{k+1} \dots v_n$ et que $h_1 \geq_{lex} h_p >_{lex} v_k >_{lex} u_k \geq_{lex} u_{k+1}$, on voit que $u_{k+1} \dots u_m <_L xv_{k+1} \dots v_n$. Par récurrence, cela implique $u_{k+1} \dots u_m <_{lex} xv_{k+1} \dots v_n$, ce qui à son tour nous donne:

$$\begin{aligned} u_1 \dots u_k u_{k+1} \dots u_m &<_{lex} u_1 \dots u_k x v_{k+1} \dots v_n \\ &= v_1 \dots v_k v_{k+1} \dots v_n. \end{aligned}$$

◇

Nous sommes maintenant prêt à montrer que les mots de Hall forment une section de l'ensemble des classes de conjugaison de mots primitifs, chaque mot de Hall étant le représentant minimal de sa classe de conjugaison. Nous allons utiliser le système de réécriture pour effectuer le calcul de la factorisation des mots en produit décroissant de mots de Hall et exploiter quelques-unes de ses propriétés. Nous devons d'abord établir deux lemmes. Le premier des deux lemmes est une adaptation du Lemme 2 de [MR 89], aux mots de Hall généraux. Nous en redonnons la preuve, dans le contexte présent.

Nous reportons notre attention sur la suite s'', pour la durée de la démonstration du Lemme 1.5.3. Nous dirons que t se dérive de s s'il existe des suites $s = s_0, s_1, \dots, s_p = t$ telles que pour tout $i = 1, \dots, p$ on ait soit $s_i = s'_{i-1}$, soit $s_i = s''_{i-1}$.

Lemme 1.5.3 *(i) Soit $s = (h_1, \dots, h_n)$ une suite standard d'au moins deux mots de Hall tels que h_1 est maximal, c'est-à-dire $h_1 \geq h_2, \dots, h_n$. Alors toute suite dérivée de s est de longueur au moins deux et son premier terme est h_1.*

(ii) Soit $s = (h_1, \ldots h_n)$ une suite standard de mots de Hall telle que $h_2 \geq \ldots \geq h_n$. Alors si $k = h_1 \ldots h_n$ est un mot de Hall, il existe une unique dérivation $s \xrightarrow{*} t = (k)$; de plus, les autres suites dérivées de s sont de longueur au moins deux.

Démonstration. (i) On procède par récurrence sur la longueur de la dérivation $s \xrightarrow{*} t$. Par hypothèse, (h_1, h_2) n'est pas une montée de la suite s, de sorte que s' est de longueur au moins deux et est égale à:

$$s' = (h_1, \ldots, h_{i-1}, h_i h_{i+1}, h_{i+2}, \ldots, h_n),$$

avec $2 \leq i \leq n$. On a $h_1 \geq h_{i+1}$ et $h_{i+1} > h_i h_{i+1}$, en vertu de (1.6), de sorte que s' satisfait les hypothèses du lemme. On peut donc conclure par récurrence sur la longueur de la dérivation.

(ii) On procède par récurrence sur n. Si $n = 1$ il n'y a rien à montrer. Supposons que $n \geq 2$. Si $h_1 \geq h_2$ alors la suite est décroissante et on ne peut rien en dériver d'autre qu'elle-même. De plus, le mot $h_1 \ldots h_n$ n'est pas un mot de Hall, car sa factorisation compte au moins deux facteurs, et on a le résultat.

On peut donc supposer que $h_1 < h_2$. C'est la seule montée de la suite et elle est légale, car c'est la plus à droite. On a donc:

$$\begin{aligned} s' &= (h_1 h_2, h_3, \ldots, h_n), \\ \text{et } s'' &= (h_2, h_1, h_3, \ldots, h_n). \end{aligned}$$

Notez que h_2 est le terme maximal de s'', de sorte par la partie (i) du lemme toute suite dérivée de s'' est de longueur au moins deux. De plus, s' est de longueur plus petite que s et satisfait les hypothèses de l'énoncé. On peut donc conclure par récurrence. ◇

Lemme 1.5.4 *Soit $s = (h_1, h_2, \ldots, h_n)$ une suite d'au moins deux mots de Hall, telle que h_1 est maximal, $h_1 \geq h_2, \ldots h_n$. Il est possible de trouver une suite standard $t = (k_1, k_2, \ldots, k_m)$ d'au moins deux mots de Hall telle que:*

$$h_1 h_2 \ldots h_n = k_1 k_2 \ldots k_m, \; h_1 = k_1, \text{ et } k_1 \geq k_2, \ldots, k_m.$$

Démonstration. On définit l'*empâtement* $\eta(s)$ d'une suite $s = (h_1, \ldots h_n)$, comme étant la différence entre son degré total et sa longueur: $\eta(s) = |h_1| + \ldots + |h_n| - n$. Nous allons montrer le lemme par récurrence sur l'empâtement des suites. Les suites d'empâtement nul sont les suites de lettres et sont standard. Cependant, il se peut qu'une suite d'empâtement non nul soit standard.

Soit $s = (h_1, \ldots, h_n)$ une suite satisfaisant les hypothèses du lemme. Si s est standard on ne fait rien. Sinon, il existe des indices i et j tels que:

$$i < j, \; h_i \text{ n'est pas une lettre et } h_i'' < h_j.$$

On sait que $i > 1$ puisque par (1.6), $h_1'' > h_1$ et que $h_1 \geq h_2, \ldots, h_n$, par hypothèse. La suite:

$$t = (h_1, \ldots, h_{i-1}, h_i', h_i'', h_{i+1}, \ldots, h_n)$$

est d'empâtement $\eta(t) = \eta(s) - 1$. De plus, elle satisfait les hypothèses du lemme. En effet, on a $h_i' < h_i''$, par (1.7), donc:

$$h_i' < h_i'' < h_j \leq h_1.$$

Puisque $h_1 h_2 \ldots h_n = h_1 h_2 \ldots h_i' h_i'' \ldots h_n$, on peut conclure par récurrence. ◇

On est maintenant en mesure de montrer la moitié de l'enoncé du théorème suivant.

Théorème 1.5.5 *Soit $w \in A^*$, non vide. Alors w est un mot de Hall si et seulement si pour toute factorisation de w en mots non vides, $w = uv$, on a $w <_H vu$.*

Démonstration. Nous montrons que la condition est nécessaire. La preuve de la suffisance est reportée à la fin du paragraphe 1.5.1.

Traduisons le résultat du Lemme 1.3.1 sur les mots. Soit w un mot de Hall et $w = uv$ une factorisation de w en mots non vides. On a:

$$u = q_1 \ldots q_m, \ v = r_1 \ldots r_n,$$

où

$$q_i, r_j \in H(A) \text{ et } q_1, \ldots, q_m < r_1, \ r_1 \geq \ldots r_n \geq w''. \tag{1.14}$$

On a donc $w = uv = q_1 \ldots q_m r_1 \ldots r_n$; par conséquent, le conjugué vu de w peut être écrit comme:

$$vu = r_1 \ldots r_n q_1 \ldots q_m.$$

Il nous faut maintenant calculer la factorisation du mot vu en produit décroissant de mots de Hall, afin de le comparer à w. L'inégalité (1.14) nous assure que la suite:

$$s = (r_1, \ldots, r_n, q_1, \ldots, q_m)$$

satisfait les hypothèses du Lemme 1.5.4. On trouve donc une suite standard: $t = (k_1, \ldots, k_p)$ telle que:

$$vu = r_1 \ldots r_n q_1 \ldots q_m = k_1 \ldots k_p.$$

et

$$r_1 = k_1, \text{ et } k_1 \geq k_2, \ldots, k_p. \tag{1.15}$$

Maintenant, pour obtenir la factorisation du mot vu, on peut utiliser le système de réécriture sur la suite standard $t = (k_1, \ldots, k_p)$. Selon (1.15), cette suite satisfait les hypothèses du point (i) du Lemme 1.5.3. Par conséquent, toute suite dérivée de t a

longueur au moins deux et a pour premier terme k_1. On sait donc que la factorisation de vu en produit décroissant de mots de Hall compte au moins deux mots et que le premier est k_1. C'est-à-dire:

$$vu = h_1 h_2 \dots h_d, \text{ avec } d \geq 2 \text{ et } h_1 = k_1. \tag{1.16}$$

Afin de comparer w à vu, il faut donc comparer h_1 à w. Mais en vertu de (1.14), (1.15) et (1.16), on a $h_1 \geq w''$; de sorte que par (1.6), on obtient $h_1 > w$. Par définition de l'ordre $<_H$, on a $h_1 >_H w$ et conséquemment $vu >_H w$. ◇

Corollaire 1.5.6 *Soit $w \in A^*$, un mot de Hall. Alors w est primitif.*

Démonstration. Supposons qu'au contraire, w n'est pas primitif. Alors il existe des mots non vides u et v tel que $w = uv = vu$. Utilisant le Th. 1.5.5, on trouve $w <_H vu = w$, et on obtient une contradiction. Donc, w est primitif. ◇

Nous allons maintenant montrer que tout mot primitif est conjugué à un unique mot de Hall, et établir la seconde moitié de l'énoncé du Th. 1.5.5. Pour cela, il nous faut définir une variante de notre système de réécriture.

On dit qu'une suite de mots de Hall $\sigma = (h_1, \dots, h_n)$ est *circulairement standard* si pour tout $i = 1, \dots, n$:

$$\text{soit } h_i \text{ est une lettre, soit } h_i = h_i' h_i'' \text{ et alors } h_i'' \geq h_1, \dots, h_n. \tag{1.17}$$

De façon équivalente, σ est circulairement standard si toute suite:

$$(h_i, \dots, h_1, h_n, \dots h_{i-1}), \quad i = 1, \dots, n,$$

est standard. Par exemple, les suites de lettres sont des suites circulairement standard. Une *montée* (h_i, h_{i+1}) d'une suite circulairement standard est dite *légale* si $h_{i+1} \geq h_1, \dots, h_n$; c'est-à-dire que le facteur h_{i+1} doit être maximal parmi les termes de la suite. On admettra la montée (h_n, h_1) si $h_n < h_1$. On peut résumer ces cas en disant que les indices des montées sont pris *modulo* n.

Soit σ une suite circulairement standard et soit (h_i, h_{i+1}) une montée légale de cette suite, les indices étant pris modulo n. On définit une nouvelle suite σ'.

Si $i < n$, alors on définit σ' de la même façon que s':

$$\sigma' = (h_1, \dots, h_i h_{i+1}, \dots, h_n).$$

Si $i = n$, alors on pose:

$$\sigma' = (h_n h_1, h_2, \dots, h_{n-1}). \tag{1.18}$$

Contrairement au système de réécriture précédent, les mots associés à σ et à σ' ne sont plus égaux. Mais on voit facilement que le mot associé à σ' est conjugué au mot associé à σ.

Proposition 1.5.7 *Soit $\sigma = (h_1, \dots h_n)$ une suite circulairement standard. Alors σ' est circulairement standard. De plus, les mots associés à σ et σ' appartiennent à la même classe de conjugaison.*

Démonstration. Soit (h_i, h_{i+1}) la montée légale de σ que l'on réécrit, les indices étant pris modulo n. D'une part, h_{i+1} est maximal parmi les termes de la suite et d'autre part, on a $(h_i h_{i+1})'' = h_{i+1}$, selon la Prop. 1.4.4. On a donc, dans tous les cas, $(h_i h_{i+1})'' \geq h_1$, $\dots$, h_{i-1}, $h_i h_{i+1}$, h_{i+2}, $\dots$, h_n et σ' est circulairement standard. La deuxième partie de l'énoncé de la proposition est évidente. ◇

Comme l'ensemble des mots de Hall forment une factorisation du monoïde libre A^* (voir Th. 1.4.6), on sait, en vertu du Théorème de Schützenberger [Sc 65], que dans toute classe de conjugaison il existe un unique mot qui est une puissance d'un mot de Hall. Nous allons obtenir ce résultat comme corollaire de la Prop. 1.5.7, à l'aide de notre version *circulaire* du système de réécriture.

Corollaire 1.5.8 *Tout mot primitif est conjugué à un unique mot de Hall.*

Démonstration. Notez que le système de réécriture 'circulaire' opère sur les suites jusqu'à ce qu'il arrive à une suite qui est réduite à un seul mot ou une répétition du même mot, puisque seules ces suites 'circulaires' ne comptent pas de montées.

Maintenant, soit $w \in A^*$, un mot primitif. On utilise le système de réécriture circulaire pour calculer successivement des suites standard σ_0, $\sigma_1 = \sigma_0'$, $\sigma_2 = \sigma_1'$, $\dots$, $\sigma_p = \sigma_{p-1}'$ avec $\sigma_p = (h_1, \dots, h_n)$ et telles que les mots w et $h_1 \dots h_n$ sont conjugués.

Si $w = a_1 \dots a_m$ avec $a_i \in A$, alors la suite $\sigma = (a_1, \dots, a_m)$ est circulairement standard. On pose donc $\sigma_0 = \sigma$ et on calcule $\sigma_1 = \sigma_0', \sigma_2 = \sigma_1'$, etc ... On arrive à calculer une suite $\sigma_p = (h_1, \dots, h_n)$ avec $h_1 = \dots = h_n$. Selon la Prop. 1.5.7, les mots associés à σ_i et σ_{i+1} sont conjugués, de sorte que w est conjugué à $h_1 \dots h_n$. Maintenant, si w est primitif, il en est de même de tous ses conjugués. On doit donc avoir $n = 1$. Cela montre que w est le conjugué du mot de Hall h_1. Comme les mots de Hall sont minimaux dans leur classe de conjugaison (condition nécéssaire du Th. 1.5.5), h_1 est unique. ◇

En utilisant les résultats classiques de la combinatoire des mots (voir [Lo 82]), on obtient le corollaire suivant:

Corollaire 1.5.9 *Tout mot est conjugué, de façon unique, à une puissance d'un mot de Hall.* ◇

Nous terminons maintenant la démonstration du Th. 1.5.5.

Corollaire 1.5.10 *Soit $w \in A^*$, tel que pour toute factorisation de w en mots non vides, $w = uv$, on ait $w <_H vu$. Alors w est un mot de Hall.*

Démonstration. Observez que w doit être primitif. Si au contraire, w n'était pas primitif, alors on pourrait trouver deux mots non vides u et v tels que $w = uv = vu$; mais c'est impossible, en vertu des hypothèses. Le corollaire est donc une conséquence immédiate du Cor. 1.5.8 et de la partie démontrée de l'énoncé du Th. 1.5.5. ◇

1.5.2 Facteurs droits.

Nous donnons maintenant des propriétés des facteurs droits des mots de Hall, par rapport à l'ordre $<_H$ défini au début du paragraphe 1.5.1.

Proposition 1.5.11 *Soit $h = h'h''$ un mot de Hall de longueur au moins deux. Alors:*

(i) parmi tous les facteurs droits de h qui sont des mots de Hall, h'' est de longueur maximale,

(ii) parmi tous les facteurs droits de h, h'' est minimal pour l'ordre $<_H$.

Démonstration. (i) Soit v un facteur droit de h, dont la longueur excède celle de h''. Soit:

$$v = h_1 \dots h_n, \text{ avec } h_1, \dots, h_n \in H(A), \text{ et } h_1 \geq \dots \geq h_n,$$

la factorisation de v donnée par le Lemme 1.3.1. Selon la Rem. 1.3.2, cette factorisation compte au moins deux facteurs, de sorte que v n'est pas un mot de Hall.

(ii) Soit un facteur droit de h, dont la longueur excède celle de h''. Alors selon la Rem. 1.3.2, on a:

$$v = h_1 \dots h_n, \text{ avec } h_1, \dots, h_n \in H(A), \text{ et } h_1 \geq \dots \geq h_n,$$
$$n \geq 2 \text{ et } h_1 \geq (h')''. \tag{1.19}$$

Pour comparer v à h, il suffit de comparer h_1 à h. Utilisant, (1.6), (1.8) et (1.19) on trouve:

$$h < h'' \leq (h')'' \leq h_1.$$

Donc, $h <_H v$.

Soit v un facteur droit de h, dont la longueur est excédée par celle de h'' ($|v| < |h''|$). Selon la Rem. 1.3.2, on a:

$$v = h_1 \dots h_n, \text{ avec } h_1, \dots, h_n \in H(A), \text{ et } h_1 \geq \dots \geq h_n,$$

$$h_1 \geq \ldots \geq h_n \geq (h'')''. \tag{1.20}$$

Encore une fois, pour comparer v à h il suffit de comparer h_1 à h. Utilisant (1.6) et (1.20), on trouve:

$$h < h'' < (h'')'' \leq h_1.$$

Donc, $h <_H v$. ◇

Remarque 1.5.12 La partie (i) de la Prop. 1.5.11 est connue. Viennot [Vi 76] en a donné une preuve sensiblement différente. ◇

Théorème 1.5.13 *Soit $w \in A^*$, un mot. Alors w est un mot de Hall si et seulement si w est strictement plus petit que tous ses facteurs droits propres.*

Démonstration. Supposons d'abord que w est un mot de Hall et soit v un facteur droit propre de w. Alors selon la Prop. 1.5.11 (ii), on a $w'' \leq_H v$. Comme $w <_H w''$, par (1.6), on a bien $w <_H v$.

Supposons maintenant que w est strictement plus petit que tous ses facteurs droits propres. On procède par contradiction. Si w n'est pas un mot de Hall, alors il se factorise en:

$$w = h_1 \ldots h_n, \text{ avec } h_1 \geq \ldots \geq h_n, \text{ et } n \geq 2.$$

Or, on doit avoir $h_1 > h_n$. En effet, si au contraire on avait $h_1 = \ldots = h_n$, alors par définition de l'ordre $<_H$ on trouverait:

$$h_i \ldots h_n <_H h_1 \ldots h_n = w, \text{ pour } i = 2, \ldots, n.$$

Mais cela contredirait les hypothèses faites sur w. On a donc $h_1 > h_n$. Et cela implique $h_n <_H h_1 \ldots h_n = w$, ce qui contredit le fait que w est plus petit que tous ses facteurs droits propres. On doit donc avoir $w \in H(A)$. ◇

Proposition 1.5.14 *Soit $w \in A^*$ et $w = h_1 \ldots h_n$ sa factorisation en produit décroissant de mots de Hall. Alors:*

(i) parmi tous les facteurs droits de w qui sont des mots de Hall, h_n est de longueur maximale,

(ii) parmi tous les facteurs droits de w, h_n est minimal pour l'ordre $<_H$.

Démonstration. Observez que lorsque w est un mot de Hall, la partie (i) de l'énoncé est évidente et la partie (ii) est vérifiée, en vertu du Th. 1.5.13. On peut donc supposer que w n'est pas un mot de Hall et que $n \geq 2$. Soit z un facteur droit propre de w.

Si $|z| < |h_n|$, alors $h_n < z$, en vertu du Th. 1.5.13.

Si $|z| > |h_n|$, alors $z = vh_{i+1} \dots h_n$ où v est un facteur droit de h_i, avec $i < n$. Soit $v = h_i$, soit v est un facteur droit propre de h_i, et dans ce cas, selon le Lemme 1.4.7, z se factorise en:

$$z = vh_{i+1} \dots h_n = k_1 \dots k_m h_{i+1} \dots h_n,$$
$$\text{avec } k_1 \geq \dots \geq k_m > h_{i+1} \geq \dots \geq h_n. \tag{1.21}$$

Dans les deux cas, on voit qu'au moins deux facteurs prennent place dans la factorisation de z. Donc, z n'est pas un mot de Hall et la partie (i) de la proposition est montrée.

Pour comparer z à h_n, il suffit de comparer k_1 à h_n. Or, selon (1.21), $k_1 > h_n$; on a donc $z >_H h_n$. ◇

Remarque 1.5.15 Duval [Du 83] a montré la Prop. 1.5.14 pour les mots de Lyndon. Il a aussi montré que la partie (i) de cette proposition est vraie pour les facteurs gauches des mots de Lyndon. Plus précisément, il a montré que *parmi tous les facteurs gauches d'un mot w qui sont des mots de Hall, h_1* (le facteur le plus à gauche de sa factorisation), *est de longueur maximale.* Ce n'est pas le cas en général. Par exemple, prenons un ensemble de Hall dont les mots de Hall de longueur au plus cinq sont ceux de l'Ex. 1.2.1. Alors $w = abbab$ se factorise en $w = h_1 h_2$ avec $h_1 = abb$ et $h_2 = ab, h_1 \geq h_2$. Comme le mot $abba$ est un mot de Hall, on voit que abb n'est pas le facteur gauche de longueur maximale dans w qui est un mot de Hall. ◇

Le prochain résultat est de Viennot [Vi 76]. Il peut être utilisé pour obtenir la factorisation standard d'un mot de Hall, en calculant la factorisation de son plus long facteur gauche propre. On peut le montrer de deux façons en utilisant les parties (i) et (ii) des Prop. 1.5.11 et Prop. 1.5.14.

Corollaire 1.5.16 *Soit $w \in A^*$ un mot de Hall de longueur au moins deux; c'est-à-dire $w = az$ avec $a \in A$ et $z \in A^*, |z| \geq 1$. Supposons que la factorisation en mots de Hall de z est:*

$$z = h_1 \dots h_n, \text{ avec } h_1 \geq \dots \geq h_n.$$

Alors $w'' = h_n$. ◇

Remarque 1.5.17 Les ordres sur A^* qui donnent lieu à des factorisations de Hall du monoïde libre ne sont toujours pas caractérisés. Le problème reste ouvert. ◇

1.6 Réécritures dans l'algèbre de Lie libre.

Soit K un corps de caractéristique nulle. Nous allons maintenant travailler dans la K-algèbre associative libre sur l'aphabet A; on la note $K<A>$. C'est l'algèbre des *polynômes* non commutatifs sur A. C'est aussi le K-module libre sur A^*; les polynômes de $K<A>$ sont des combinaisons linéaires de mots de A^* à coefficients dans K. On désigne le *coefficient d'un mot* w dans un polynôme P par (P,w). On écrira abusivement $w \in P$ lorsque $(P,w) \neq 0$; on dira alors que w *apparaît* dans P. On peut donc définir l'addition et la multiplication de deux polynômes P et Q par les égalités:

$$\begin{aligned}(P+Q,w) &= (P,w)+(Q,w),\\ (PQ,w) &= \sum_{\substack{u\in P, v\in Q\\ uv=w}} (P,u)(Q,v).\end{aligned}$$

Notez que les mots de A^* peuvent être considérés comme des polynômes de $K<A>$. Le *support* d'un polynôme est formé des mots qui y apparaîssent. Le *degré* d'un polynôme P est égal à la longueur du plus long mot de son support: $\deg(P) = \max\{|w| : w \in P\}$. On dira d'un polynôme P qu'il est *homogène de degré* n si tous les mots de son support sont de longueur n. L'algèbre associative libre est *graduée* par le degré, c'est-à-dire que tout polynôme s'écrit de façon unique comme somme de polynômes homogènes.

Une *algèbre de Lie* $\mathcal{L}$ (sur K) est une K-algèbre dont le produit, qui est noté par un crochet, satisfait:

$$[x,x] = 0, \tag{1.22}$$

$$[[x,y]z]] = [x[y,z]] + [[x,z]y]. \tag{1.23}$$

La seconde relation, (1.23), est souvent appelée l'*identité de Jacobi*. On peut munir $K<A>$ du produit:

$$[P,Q] = PQ - QP,$$

pour en faire une algèbre de Lie $\mathcal{L}$. Le produit $[P,Q]$ des polynômes P et Q est appelé le *crochet* de P et de Q. Soit $\mathcal{L}(A)$ la sous-algèbre de Lie de $\mathcal{L}$ engendrée par les lettres de A. C'est l'*algèbre de Lie libre* sur A et son *algèbre enveloppante* est $K<A>$ (voir [Lo 82, Reu]).

Les polynômes de $\mathcal{L}(A)$ sont appelés des *polynômes de Lie* de $\mathcal{L}(A)$ ou des *éléments de Lie de* $K<A>$. On a une application $\lambda : M(A) \to \mathcal{L}(A)$, qui à chaque élément t du magma libre associe un polynôme de Lie. La structure arborescente de t fournit un crochetage de son feuillage qui, interprété comme un crochetage de Lie, donne un polynôme de Lie. Plus précisément, si $t \in M(A)$ alors:

$$\lambda(t) = \begin{cases} t & \text{si } t \text{ est une lettre,}\\ [\lambda(t'),\lambda(t'')] & \text{si } t = [t',t''] \,. \end{cases} \tag{1.24}$$

On a donc $\lambda(t) = \lambda(t')\lambda(t'') - \lambda(t'')\lambda(t')$.

Exemple 1.6.1 Soit $[a,b]$, $[[a,b]b]$ et $[[[a,b]b],a]$ des éléments de l'ensemble de Hall de l'Ex. 1.2.1. Les polynômes de Lie qui leurs sont associés sont:

$$\begin{aligned} [a,b] &= ab - ba \\ [[a,b]b] &= [a,b]b - b[a,b] = abb - 2bab + bba \\ [[[a,b]b]a] &= [[a,b]b]a - a[[a,b]b] \\ &= bbaa - 2baba - aabb + 2abab \end{aligned}$$

Notez que le polynôme de Lie associé à l'arbre de Hall h est homogène de degré $|h|$. $\diamond$

Fixons un ensemble de Hall $H(A)$. La restriction de l'application λ à $H(A)$ nous fournit un ensemble de polynômes de Lie, associés aux arbres de Hall. Nous allons voir que ces polynômes forment une base du K-module $\mathcal{L}(A)$. Plusieurs auteurs ont déjà montré ce résultat pour divers cas d'ensembles de Hall (voir par exemple [HM 50a, Sc 58, Ši 62]). Le prochain résultat est de Schützenberger.

Proposition 1.6.2 (Schützenberger)
Soit $h,k \in H(A)$. Alors $[\lambda(h),\lambda(k)]$ est une combinaison linéaire de polynômes de Lie $\lambda(r)$, $r \in H(A)$, avec $|r| = |h| + |k|$ et $r < \sup(h,k)$.

Démonstration. On procède par récurrence sur les couples $(|h| + |k|, \sup(h,k))$ ordonnés par: $(d_1,r_1) < (d_2,r_2)$ si et seulement si soit $d_1 < d_2$, soit $d_1 = d_2$ et $r_1 > r_2$.

On peut supposer $h < k$, par (1.22). On a donc $\sup(h,k) = k$. Si $h \in A$ ou si $h'' \geq k$ alors hk est un mot de Hall écrit sous forme standard et son polynôme de Lie associé est $\lambda(hk) = [\lambda(h),\lambda(k)]$. On a bien $|hk| = |h| + |k|$; comme par (1.6) $hk < k$, on a aussi $hk < \sup(h,k)$, et le résultat est vérifié.

Sinon, on a:

$$\begin{gathered} h'' < k, \\ \text{et} \quad h, h' < h'' \quad \text{par (1.6) et (1.7)} \end{gathered}$$

On utilise l'identité de Jacobi (1.23), pour obtenir l'égalité:

$$\begin{aligned} & [\lambda(h),\lambda(k)] \\ = \quad & [[\lambda(h'),\lambda(h'')]\lambda(k)] \\ = \quad & [\lambda(h')[\lambda(h''),\lambda(k)]] + [[\lambda(h'),\lambda(k)]\lambda(h'')]. \end{aligned}$$

Par hypothèse de récurrence, on a:

$$\begin{aligned} [\lambda(h'),\lambda(k)] &= \sum_i \alpha_i \lambda(r_i), \\ [\lambda(h''),\lambda(k)] &= \sum_j \beta_j \lambda(p_j), \end{aligned}$$

avec:

$$|r_i| = |h'| + |k|, \quad \text{et} \quad r_i < \sup(h', k) = h',$$
$$|p_j| = |h''| + |k|, \quad \text{et} \quad p_j < \sup(h'', k) = h''.$$

Alors:

$$\begin{aligned}[\lambda(h), \lambda(k)] &= [\sum_i \alpha_i \lambda(r_i), \lambda(h'')] + [\lambda(h'), \sum_j \beta_j \lambda(p_j)] \\ &= \sum_i \alpha_i [\lambda(r_i), \lambda(h'')] + \sum_j \beta_j [\lambda(h'), \lambda(p_j)].\end{aligned}$$

Or, on a $\sup(r_i, h''), \sup(p_j, h') < k$ puisque $r_i < h'$, $p_j < h''$ et $h', h'' < k$. On peut donc conclure par récurrence. ◇

Corollaire 1.6.3 *Les polynômes de Lie associés aux mots de Hall,* $\{\lambda(h) : h \in H(A)\}$, *engendrent l'algèbre de Lie libre* $\mathcal{L}(A)$.

Démonstration. Posons $\mathcal{B} = \{\lambda(h) : h \in H(A)\}$. La sous-algèbre de Lie engendrée par les polynômes de Lie de $\mathcal{B}$ est contenue dans $\mathcal{L}(A)$. En vertu de la Prop. 1.6.2, le crochet de Lie de deux polynômes de Lie de $\mathcal{B}$ est dans le K-module engendré par ces polynômes de Lie. Comme les lettres sont dans $\mathcal{B}$, ce K-module contient $\mathcal{L}(A)$. On peut donc conclure à l'égalité. ◇

Remarque 1.6.4 Dans [Ree 61], Ree introduit ce qu'il appelle les *éléments de Lie généralisés*. Le contexte dans lequel il se place est le suivant. Soit $\mathcal{L}$ une K-algèbre graduée, dont le produit est noté par des crochets. C'est-à-dire qu'on a $\mathcal{L} = \oplus_{n \geq 0} \mathcal{L}_n$ où $\mathcal{L}_n$ est le sous-module des éléments de degré n (Ree considère des graduations sur des semi-groupes quelconques, mais nous nous en tiendrons au semi-groupe N des entiers positifs). Un *bi-caractère gauche* sur la graduation de $\mathcal{L}$ est une application $\chi : N \times N \to K$ qui satisfait:

$$\begin{aligned}\chi(m, n+p) &= \chi(m, n)\chi(m, p), \\ \chi(m+n, p) &= \chi(m, k)\chi(n, p), \\ \chi(m, n)\chi(n, m) &= 1, \end{aligned} \tag{1.25}$$

pour tout $m, n, p \in N$. L'algèbre $\mathcal{L}$ est appelée une *algèbre de Lie généralisée*, et ses éléments sont appelés des éléments de Lie généralisés, si pour $P \in \mathcal{L}_m, Q \in \mathcal{L}_n$ et $R \in \mathcal{L}$ on a:

$$0 = [P, Q] + \chi(m, n)[Q, P], \tag{1.26}$$
$$[[P, Q], R] = [P, [Q, R]] - \chi(m, n)[Q, [P, R]]. \tag{1.27}$$

L'algèbre $\mathcal{L}$ est parfois aussi appelée une *superalgèbre de Lie* (voir [S 79]). Soit $E = \oplus_{n\geq 0} E_n$ une K-algèbre graduée, munie d'un bi-caractère gauche χ sur sa graduation. L'algèbre $\mathcal{L}$ (obtenue de E) munie du produit $[x,y] = xy - \chi(m,n)yx$, pour $x \in E_m, y \in E_n$, est alors une algèbre de Lie généralisée. De la condition (1.25), on voit que χ doit satisfaire $\chi(n,n) = \pm 1$. Lorsque $\chi(n,n) = -1$, les éléments de $\mathcal{L}_n$ sont dits *impairs*, et lorsque $\chi(n,n) = +1$, ils sont dits *pairs*.

L'un des cas intéressant est obtenu en considérant sur l'algèbre associative libre $K<A>$ (graduée par le degré), le bi-caractère gauche donné par:

$$\chi(m,n) = \begin{cases} +1 & \text{si } m \text{ ou } n \text{ est pair,} \\ -1 & \text{si } m \text{ et } n \text{ sont tous les deux impairs,} \end{cases}$$

c'est-à-dire $\chi(m,n) = (-1)^{mn}$. Dans ce cas, on peut considérer la sous-algèbre de Lie généralisée de $\mathcal{L}$ engendrée par A; on la notera aussi $\mathcal{L}(A)$ (cette notation ne débordera pas le cadre de la Rem. 1.6.4). On obtient des bases de $\mathcal{L}(A)$ en adjoignant aux ensembles de Hall $H(A)$, les arbres de la forme $[h,h]$, où h est un arbre de degré impair de $H(A)$. La base de $\mathcal{L}$ est alors obtenue à l'aide de λ, comme dans le cas non-généralisé. On peut aussi reprendre la preuve de la Prop. 1.6.2 pour montrer que ces polynômes de Lie généralisés engendrent bien $\mathcal{L}$, en prenant soin d'exiger $[h,h] < h$ et $[h,h] > k$ pour tout $k < h$. On utilise alors les relations (1.26) et (1.27).

Ree a montré que l'algèbre enveloppante de l'algèbre de Lie généralisée $\mathcal{L}(A)$ a pour base les produits décroissants d'éléments P_i de la base de $\mathcal{L}(A)$:

$$P_1^{n_1} \dots P_q^{n_q}, \qquad P_1 > \dots > P_q,$$

où les exposants n_i satisfont $n_i = 0,1$ si P_i est un élément impair de $\mathcal{L}(A)$. Cela vient du fait que dans l'algèbre enveloppante de $\mathcal{L}(A)$, on a:

$$[P_i, P_i] = 2P_i^2. \tag{1.28}$$

Revenons au cas de l'algèbre associative libre $K<A>$; Ree montre que c'est l'algèbre enveloppante de l'algèbre de Lie généralisée $\mathcal{L}(A)$. Après lecture de ce qui va suivre dans ce paragraphe, le lecteur sera en mesure de constater qu'en le modifiant légèrement (pour tenir compte des coefficients qui apparaîssent en raison de (1.28)), notre système de réécriture peut être utilisé pour calculer dans cette algèbre. On peut faire la réécriture comme dans le cas non généralisé, pour ensuite réduire à 0 ou à 1 les exposants des polynômes associés à des arbres impairs, à l'aide de (1.28). ◇

A partir de maintenant, nous noterons le polynôme de Lie associé à $h \in H(A)$ par $[h]$. Soit $s = (h_1, \dots, h_n)$ une suite standard de mots de Hall. Nous dirons que le polynôme:

$$[h_1] \dots [h_n]$$

est le *polynôme associé* à s dans $K<A>$. Notez que comme $[h]$ est un polynôme homogène de degré $|h|$, le polynôme $[h_1]\ldots[h_n]$ est homogène de degré $|h_1|+\ldots+|h_n|$. Nous allons montrer que l'ensemble des polynômes associés à des suites décroissantes:

$$[h_1]\ldots[h_n] \text{ avec } n \geq 0, h_1 \geq \ldots \geq h_n, \tag{1.29}$$

forment une base de $K<A>$. A l'aide du Th. 1.4.6, on peut mettre les mots de A^* en bijection avec les polynômes (1.29). Les polynômes homogènes de degré n associés à des suites décroissantes sont donc au même nombre que les mots de longueur n, pour chaque $n \geq 0$. Comme les mots forment une base de $K<A>$, notre travail se limite à montrer que tout mot peut s'écrire comme combinaison linéaire de polynômes de la forme (1.29).

Nous noterons le polynôme associé à s simplement par s, s'il n'y a aucune confusion possible. Si s' et s'' sont les suites dérivées de s définies en (1.12) et (1.13) alors on a:

$$s = s' + s'',$$

puisqu'en vertu de la définition du crochet de Lie,

$$[h_i][h_{i+1}] = [[h_i],[h_{i+1}]] + [h_{i+1}][h_i].$$

Partant d'une suite standard s, on peut définir un arbre binaire $\mathcal{A}(s)$, dont la racine est étiquettée par s. Nous dirons que $\mathcal{A}(s)$ est un arbre de dérivations indexarbre de dérivations de s. Un tel arbre est défini récursivement. Si la suite s est décroissante, son arbre est réduit à une feuille étiquettée par s. Sinon, soient s' et s'' les suites dérivées de s par réécriture d'une montée légale de s. La racine de $\mathcal{A}(s)$ est étiquettée par s; le sous-arbre gauche immédiat de $\mathcal{A}(s)$ est un arbre de dérivation $\mathcal{A}' = \mathcal{A}(s')$ de la suite s' et le sous-arbre droit immédiat de $\mathcal{A}(s)$ est un arbre de dérivation $\mathcal{A}'' = \mathcal{A}(s'')$ de la suite s''. Comme il peut y avoir plus d'une montée légale dans la suite s, il existe plusieurs arbres de dérivation associés à s. Les suites qui pendent aux feuilles d'un arbre $\mathcal{A}(s)$ sont des suites décroissantes. La *multiplicité* d'une suite décroissante t dans un arbre $\mathcal{A}(s)$ est égale au nombre de feuilles auxquelles elle est attachée. Convenons de noter le *multi-ensemble* des feuilles d'un arbre de dérivation $\mathcal{A}$ par $\mathcal{F}(\mathcal{A})$. Notez qu'on a:

$$\mathcal{F}(\mathcal{A}) = \mathcal{F}(\mathcal{A}') \cup \mathcal{F}(\mathcal{A}'').$$

Exemple 1.6.5 Soit $H(A)$ un ensemble de Hall dont les éléments de degré au plus cinq sont ceux de l'Ex. 1.2.1. On peut construire l'arbre de dérivations de la suite standard (a,b,b,a) de la Fig. 1.6. Lorsqu'on passe dans $K<A>$, on trouve:

$$\begin{aligned} abba &= [ab]ba + baba \\ &= [abb]a + 2b[ab]a + bbaa \\ &= [abba] + a[aba] + 2b[aba] + 2ba[ab] \end{aligned}$$

Observez que la multiplicité d'une suite décroissante attachée aux feuilles de l'arbre est égale à son coefficient dans l'expression obtenue pour $abba$. ◇

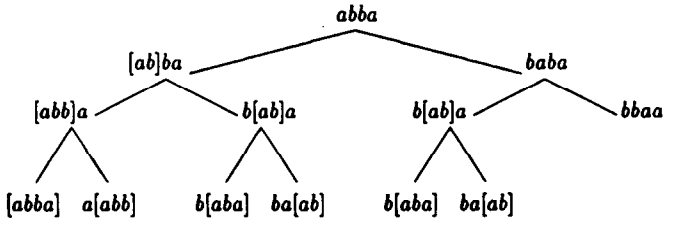

Figure 1.6: Un arbre de dérivation de $s = (a, b, b, a)$.

Nous allons utiliser les arbres de dérivation pour faire les calculs dans $K\langle A\rangle$. Le lemme qui suit est technique. Il montre en quelque sorte la 'confluence' de la réécriture dans $K\langle A\rangle$.

Lemme 1.6.6 *Soit s une suite standard. Alors l'ensemble des suites décroissantes qui pendent aux feuilles d'un arbre de dérivation est le même pour tous les arbres de dérivation de s, et chaque suite décroissante apparait aux feuilles de ces arbres avec la même multiplicité.*

Démonstration. On procède par récurrence sur la longueur et sur le nombre de montées éloignées des suites (voir (1.10)). Soient $\mathcal{A}_1(s)$ et $\mathcal{A}_2(s)$, deux arbres de dérivation de s. Soient s_i' et s_i'' les fils gauche et droit de s dans $\mathcal{A}_i(s)$ $(i = 1, 2)$. Désignons par $\mathcal{A}_i'$ et $\mathcal{A}_i''$ les sous-arbres gauches et droits immédiats de $\mathcal{A}_i(s)$, $(i = 1, 2)$. Les suites s_i' et s_i'' sont à la racine de ces arbres.

Il se peut qu'on ait $s_1' = s_2'$ et $s_1'' = s_2''$, auxquels cas on applique la récurrence. Les suites décroissantes qui apparaîssent aux feuilles de s_1' et s_2' (resp. s_1'' et s_2'') sont les mêmes et elles y apparaîssent avec même multiplicité. Comme l'ensemble des feuilles de $\mathcal{A}_i(s)$ est formé de l'ensemble des feuilles de ses sous-arbres s_i' et s_i'', on a le résultat.

Sinon, c'est que les suites s_1' et s_1'' d'une part, et les suites s_2' et s_2'' d'autre part, sont obtenues de s en réécrivant des montées légales distinctes de s. Soient $s = (h_1, \ldots, h_n)$ et (h_i, h_{i+1}), (h_j, h_{j+1}) les montées légales de s qui sont réécrites. En vertu de Lemme 1.4.9, on sait que les montées légales ne se chevauchent pas, c'est-à-dire $i + 1 < j$. On a donc:

$$\begin{aligned}
s_1' &= (h_1, \ldots, h_{i-1}, h_i h_{i+1}, \ldots, h_j, \ldots, h_n),\\
s_1'' &= (h_1, \ldots, h_{i-1}, h_{i+1}, h_i, \ldots, h_j, \ldots, h_n),\\
s_2' &= (h_1, \ldots, h_{i+1}, \ldots, h_j h_{j+1}, h_{j+2}, \ldots, h_n),\\
s_2'' &= (h_1, \ldots, h_{i+1}, \ldots, h_{j+1}, h_j, h_{j+2}, \ldots, h_n).
\end{aligned}$$

La montée (h_i, h_{i+1}) est une montée légale des suites s_2' et s_2'' et la montée (h_j, h_{j+1}) est une montée légale des suites s_1' et s_1''; on le vérifie aisément (voir la démonstration

du Cor. 1.4.10). Des quatre suites s'_i et $s''_i, (i = 1,2)$, en réécrivant les montées légales $(h_i, h_{i+1}), (h_j, h_{j+1})$, on peut en dériver huit. Or, si on effectue le calcul on voit que:

$$(s'_1)' = (s'_2)' \ , \ (s'_1)'' = (s''_2)' \ , \ (s''_1)' = (s'_2)'' \ , \ (s''_1)'' = (s''_2)'' \ . \tag{1.30}$$

Soient $\overline{\mathcal{A}}'_i$ (respectivement $\overline{\mathcal{A}}''_i$) un arbre de dérivation de s'_i (resp. s''_i), dont les sous-arbres gauches et droits immédiats sont des arbres de dérivation de $(s'_i)'$ et $(s'_i)''$ (resp. $(s''_i)'$ et $(s''_i)''$) $(i = 1,2)$. Par récurrence, on a:

$$\begin{aligned} \mathcal{F}(\mathcal{A}'_i) &= \mathcal{F}(\overline{\mathcal{A}}'_i), \\ \mathcal{F}(\mathcal{A}''_i) &= \mathcal{F}(\overline{\mathcal{A}}''_i). \end{aligned}$$

A cela, les égalités (1.30) nous permettent d'ajouter:

$$\mathcal{F}(\overline{\mathcal{A}}'_1) \cup \mathcal{F}(\overline{\mathcal{A}}''_1) = \mathcal{F}(\overline{\mathcal{A}}'_2) \cup \mathcal{F}(\overline{\mathcal{A}}''_2).$$

Par conséquent:

$$\begin{aligned} \mathcal{F}(\mathcal{A}_1) &= \mathcal{F}(\mathcal{A}'_1) \cup \mathcal{F}(\mathcal{A}''_1) \\ &= \mathcal{F}(\overline{\mathcal{A}}'_1) \cup \mathcal{F}(\overline{\mathcal{A}}''_1) \\ &= \mathcal{F}(\overline{\mathcal{A}}'_2) \cup \mathcal{F}(\overline{\mathcal{A}}''_2) \\ &= \mathcal{F}(\mathcal{A}'_2) \cup \mathcal{F}(\mathcal{A}''_2) \\ &= \mathcal{F}(\mathcal{A}_2) \end{aligned}$$

On en conclut le résultat. ◇

Théorème 1.6.7 *Soit $w \in A^*$ un mot, et $\mathcal{A}$ un arbre de dérivation de la suite de ses lettres. Alors on a:*

$$w = \sum_{t \in \mathcal{F}(\mathcal{A})} t. \tag{1.31}$$

De plus, l'expression (1.31) *ne dépend pas du choix de l'arbre de dérivation $\mathcal{A}$.*

Démonstration. On procède par récurrence sur la longueur et sur le nombre de montées éloignées des suites (voir (1.10)). Soit s une suite standard non décroissante. La Prop. 1.6.6 nous assure que le multi-ensemble $\mathcal{F} = \mathcal{F}(\mathcal{A}(s))$ ne dépend pas du choix de l'arbre $\mathcal{A}(s)$. De plus, la démonstration de cette proposition montre que $\mathcal{F}(\mathcal{A}(s)) = \mathcal{F}(\mathcal{A}(s')) \cup \mathcal{F}(\mathcal{A}(s''))$, où s' et s'' sont obtenues de s par réécriture d'une montée légale de s et où l'union des multi-ensembles est disjointe. Donc, on a:

$$\begin{aligned} s &= s' + s'' \\ &= \sum_{t \in \mathcal{F}(\mathcal{A}(s'))} t + \sum_{\mathcal{F}(\mathcal{A}(s''))} t \\ &= \sum_{t \in \mathcal{F}(\mathcal{A}(s')) \cup \mathcal{F}(\mathcal{A}(s''))} t \\ &= \sum_{t \in \mathcal{F}(\mathcal{A}(s))} t. \end{aligned}$$

Dans le cas où la suite s est décroissante l'expression (1.31) est réduite à un seul terme. Si on applique l'argument à la suite standard formée des lettres du mot w, on obtient le résultat annoncé. ◇

Remarques 1.6.8 (i) Nous avons en fait montré que le Th. 1.6.7 est vérifié pour toute suite standard s:

$$s = \sum_{t \in \mathcal{F}(A(s))} t.$$

(ii) L'énoncé du Th. 1.6.7 est beaucoup plus fort que ce qui nous est nécessaire. Il nous suffisait en fait de montrer que $K<A>$ est *engendrée* par les polynômes associés à des suites standard décroissantes (voir la démonstration du Cor. 1.6.9). ◇

On déduit du Th. 1.6.7 le résultat annoncé plus haut.

Corollaire 1.6.9 *Les polynômes associés aux suites décroissantes de mots de Hall forment une base de* $K<A>$.

Démonstration. En vertu du Th. 1.6.7, les mots de longueur n sont combinaisons linéaires de polynômes homogènes de degré n associés à des suites standard. Ainsi, les polynômes associés à ces suites et les mots de longueur n engendrent le même sous-espace (de $K<A>$), soit celui formé des polynômes homogènes de degré n, qu'on note $K<A>_n$. Comme on le mentionnait précédemment, à l'aide du Th. 1.4.6, on peut mettre les mots de A^* en bijection avec les polynômes (1.29). Les polynômes homogènes de degré n associés à des suites décroissantes sont donc au même nombre que les mots de longueur n, pour chaque $n \geq 0$. Or, les mots de longueur n forment une base de $K<A>_n$; par conséquent, il en est de même pour les polynômes (homogènes de degré n) associés aux suites standard décroissantes. ◇

Corollaire 1.6.10 *Les polynômes de Lie associés aux mots de Hall,* $\{[h] : h \in H(A)\}$, *forment une base du* K*-module* $\mathcal{L}(A)$.

Démonstration. On a vu au Cor. 1.6.3, que les polynômes de Lie associés aux mots de Hall engendrent $\mathcal{L}(A)$. Or, ils forment une sous-famille des polynômes (1.29) et ces derniers forment une famille K-linéairement indépendante (Cor. 1.6.9). Par conséquent, les polynômes de Lie associés aux mots de Hall sont K-linéairement indépendants et forment une base du K-module $\mathcal{L}(A)$. ◇

1.7 Base duale et algèbre de mélange.

La base

$$[h_1]\dots[h_n] \text{ avec } n \geq 0, \quad h_1 \geq \dots \geq h_n,$$

de l'algèbre $K<A>$ est appelée la *base de Poincaré-Birkhoff-Witt associée aux mots de Hall*. On abrégera son nom par 'base PBWH'. On étend la notation $[w]$ au monoïde libre tout entier. Si

$$w = h_1 \dots h_n, \text{ avec } h_1 \geq \dots \geq h_n$$

est la factorisation du mot $w \in A^*$ en produit décroissant de mots de Hall (voir Th. 1.4.6), alors on pose:

$$[w] = [h_1]\dots[h_n].$$

Avec cette notation la base PBWH est simplement:

$$\{[w] : w \in A^*\}.$$

Une *série formelle* S sur A est une somme infinie de mots de A^* à coefficients dans K:

$$S = \sum_{w \in A^*} (S, w)w.$$

Cet espace est noté $K\ll A\gg$ et est naturellement isomorphe à l'espace dual de $K<A>$. La dualité $K\ll A\gg \times K<A> \to K$ s'exprime par:

$$(S, P) \mapsto (S, P) = \sum_{w \in A^*} (S, w)(P, w).$$

Nous introduisons maintenant une base, S_w ($w \in A^*$), duale à la base PBWH. Elle est définie par:

$$u = \sum_{w \in A^*} (S_w, u)[w], \tag{1.32}$$

pour tout mot u.

Remarque 1.7.1 Soit $w \in A^*$ et $w = h_1 \dots h_n$ (avec $h_i \in H(A), h_1 \geq \dots \geq h_n$, sa factorisation en produit décroissant de mots de Hall. On sait, en vertu du Th. 1.6.7, que le coefficient (S_w, u) est égal à la multiplicité de la suite $(h_1, \dots, h_n)$ aux feuilles d'un arbre de dérivation des lettres de w. Par conséquent, S_w est un polynôme à coefficients entiers positifs, homogène de degré $|w|$. ◇

On définit récursivement le *produit de mélange* des mots, et on le note '$\sqcup\!\sqcup$', par:

$$\begin{aligned} 1 \sqcup\!\sqcup u &= u \sqcup\!\sqcup 1 = u, \\ (au) \sqcup\!\sqcup (bv) &= a(u \sqcup\!\sqcup bv) + b(au \sqcup\!\sqcup v). \end{aligned}$$

Ce produit est associatif, commutatif et sans diviseurs de zéro (voir Ree [Ree 58]). Nous dirons qu'un mot w est un *mélange* de u et v si $w \in u \sqcup\!\sqcup v$. Par exemple, on a:

$$ab \sqcup\!\sqcup ab = 2abab + 4aabb.$$

Ce produit s'étend par linéarité à $K\langle A\rangle$ tout entier. Nous dirons que $K\langle A\rangle$ (resp. $K\langle\langle A\rangle\rangle$) est munie de sa structure d'*algèbre de mélange* lorsque le produit considéré sur $K\langle A\rangle$ (resp. $K\langle\langle A\rangle\rangle$) est le produit de mélange. Nous donnons maintenant des identités satisfaites par les polynômes S_w. Ces identités ont été démontrées pour la première fois par Schützenberger [Sc 58] pour les bases de Hall-Shirshov. Melançon et Reutenauer [MR 89] les ont aussi montrées pour les bases de Lyndon. Nous allons voir qu'elles sont aussi vraies pour les bases de Hall générales.

Théorème 1.7.2 *(i) Soit* 1 *le mot vide de* A^*. *Alors:*

$$S_1 = 1.$$

(ii) Soit aw *un mot de Hall commençant par la lettre* a. *Alors:*

$$S_{aw} = aS_w.$$

(iii) Soit w *un mot et:*

$$w = h_1^{i_1} \dots h_n^{i_n}, \text{ avec } i_j \geq 1, \quad h_1 > \dots > h_n,$$

sa factorisation en produit décroissant de mots de Hall. Alors:

$$S_w = \frac{1}{i_1! \dots i_n!} S_{h_1}^{i_1} \sqcup\!\sqcup \dots \sqcup\!\sqcup S_{h_n}^{i_n},$$

où $S_{h_j}^{i_j} = \underbrace{S_{h_j} \sqcup\!\sqcup \dots \sqcup\!\sqcup S_{h_j}}_{i_j \text{ fois}}$.

Démonstration. (i) Le résultat est évident puisque $[1] = 1$.

(ii) Nous utiliserons, pour la démonstration de ce point, les résultats du Lemme 1.5.3. Il nous faut montrer que:

$$(S_{aw}, bu) = \chi(a = b)(S_w, u).$$

où $\chi(*)$ est la fonction de vérité qui vaut 1 si l'énoncé '$*$' est vrai et 0 sinon. On a, en vertu de (1.32),

$$u = \sum_{w \in A^*} (S_w, u)[w].$$

On en tire:

$$bu = \sum_{w \in A^*} (S_w, u) b[w].$$

Maintenant, si $w = h_1 \dots h_n$, avec $h_j \in H(A), h_1 \geq \dots \geq h_n$, est la factorisation de w en produit décroissant de mots de Hall alors la suite $s = (b, h_1, \dots, h_n)$ est standard. Selon la Rem. 1.6.8, on a:

$$b[w] = \sum_{t \in \mathcal{F}(A(s))} t.$$

Selon le point (ii) du Lemme 1.5.3, la seule suite réduite à un seul terme qu'on puisse dériver de s est la suite $([bw])$ si le mot bw est un mot de Hall. Les autres suites qu'on en dérive sont de longueur au moins deux. Donc:

$$b[w] = \chi(bw \in H(A))[bw] + \sum_{\substack{k \geq 2, u_i \in H(A) \\ u_1 \geq \dots \geq u_k}} \alpha_{u_1, \dots, u_k} [u_1] \dots [u_k].$$

Par conséquent,

$$\begin{aligned} bu &= \sum_{w \in A^*} \chi(bw \in H(A))(S_w, u)[bw] + \sum_{\substack{k \geq 2, u_i \in H(A) \\ u_1 \geq \dots \geq u_k}} \beta_{u_1, \dots, u_k} [u_1] \dots [u_k], \\ &= \sum_{bw \in H(A)} (S_w, u)[bw] + \sum_{\substack{k \geq 2, u_i \in H(A) \\ u_1 \geq \dots \geq u_k}} \gamma_{u_1, \dots, u_k} [u_1] \dots [u_k]. \end{aligned} \tag{1.33}$$

D'autre part, on a par définition:

$$\begin{aligned} bu &= \sum_{w \in A^*} (S_w, bu)[w] \\ &= \sum_{aw \in H(A)} (S_a w, bu)[aw] + \sum_{\substack{k \geq 2, u_i \in H(A) \\ u_1 \geq \dots \geq u_k}} \eta_{u_1, \dots, u_k} [u_1] \dots [u_k]. \end{aligned} \tag{1.34}$$

On obtient le résultat en comparant les termes des sommes de gauche de (1.33) et (1.34). ◇

Avant de démontrer le point (iii) du Th. 1.7.2, il nous faut reprendre les Lemmes **3 à 6** de [MR 89].

Soit $p \geq 2$ un entier et soit

$$c_p : K\langle A \rangle \to K\langle A \rangle^{\otimes p}$$

l'homomorphisme (pour le produit de concaténation sur $K\langle A \rangle$) défini sur A par:

$$c_p(a) = a \otimes 1 \dots \otimes 1 + 1 \otimes a \otimes \dots \otimes 1 + \dots + 1 \otimes \dots \otimes 1 \otimes a,$$

où chaque tenseur a p facteurs. Si $w \in A^*$ on a:

$$c_p(w) = \sum_{u_i \in A^*} (w, u_1 \sqcup \ldots \sqcup u_k) u_1 \otimes \ldots \otimes u_k, \tag{1.35}$$

(voir [Reu]). Par exemple, si $p = 2$, on a:

$$c_2(abb) = abb \otimes 1 + 2ab \otimes b + bb \otimes a + a \otimes bb + 2b \otimes ab + 1 \otimes abb.$$

On voit bien dans l'exemple que le coefficient de $u \otimes v$ est égal au coefficient de $w = abb$ dans $u \sqcup v$.

Lemme 1.7.3 *Soient $S_1, \ldots S_p \in K\langle\langle A \rangle\rangle$ et $P \in K\langle A \rangle$. Alors:*

$$(S_1 \sqcup \ldots \sqcup S_p, P) = (S_1 \otimes \ldots \otimes S_p, c_p(P)).$$

Démonstration. Il suffit de montrer le lemme lorsque les séries S_i et les polynômes P sont des mots. Dans ce cas, le résultat découle de (1.35). ◇

Lemme 1.7.4 *Si P est un polynôme de Lie, $P \in \mathcal{L}(A)$, alors:*

$$c_p(P) = P \otimes 1 \otimes \ldots \otimes 1 + 1 \otimes P \otimes \ldots \otimes 1 + \ldots + 1 \otimes \ldots \otimes 1 \otimes P.$$

Démonstration. On montre que l'ensemble des polynômes qui satisfont l'égalité contient les lettres et est fermé par crochet de Lie. Par conséquent, il contient $\mathcal{L}(A)$. ◇

Lemme 1.7.5 *Soient $S_1, \ldots, S_p \in K\langle\langle A \rangle\rangle$ des séries de termes constants nuls, $(S_i, 1) = 0$, et $P_1, \ldots, P_q \in \mathcal{L}(A)$ des polynômes de Lie. Supposons que $p > q$. Alors:*

$$(S_1 \sqcup \ldots \sqcup S_p, P_1 \ldots P_q) = 0.$$

Démonstration. On utilise le Lemme 1.7.3; on obtient:

$$\begin{aligned} & (S_1 \sqcup \ldots \sqcup S_p, P_1 \ldots P_q) \\ = \quad & (S_1 \otimes \ldots \otimes S_p, c_p(P_1 \ldots P_q)) \\ = \quad & (S_1 \otimes \ldots \otimes S_p, c_p(P_1) \ldots c_p(P_q)). \end{aligned}$$

Le lemme est une conséquence du Lemme 1.7.4 et du fait suivant: chaque tenseur du produit $c_p(P_1) \ldots c_p(P_q)$ possède au moins un terme égal à 1 (puisque $p > q$) et chacune des séries S_i est sans terme constant. ◇

Lemme 1.7.6 *Soient $S_1, \ldots, S_p \in K\ll A\gg$ des séries de termes constants nuls, $(S_i, 1) = 0$, et $P_1, \ldots, P_p \in \mathcal{L}(A)$ des polynômes de Lie. Alors:*

$$(S_1 \sqcup \ldots \sqcup S_p, P_1 \ldots P_p) = \sum_{\sigma} (S_1, P_{\sigma(1)}) \ldots (S_p, P_{\sigma(p)}),$$

où la somme s'étend à toutes les permutations σ de l'ensemble $\{1, \ldots, p\}$.

Démonstration. Le lemme est une conséquence directe du Lemme 1.7.3 et du Lemme 1.7.4. ◇

Démonstration du Th. 1.7.2 (iii). Nous allons utiliser les Lemmes précédents dans le cas où les séries $S_i \in K\ll A\gg$ sont nos séries S_w définies en (1.32) et où les polynômes de Lie P_j sont les polynômes $[h], h \in H(A)$, de la base de Hall de $\mathcal{L}(A)$.

Les séries S_w $(w \neq 1)$ sont homogènes de degré $|w|$, donc sans termes constants. Soit $k_1, \ldots k_n \in H(A)$ avec $k_1 \geq \ldots \geq k_n$ et $w \in A^*$. Posons $u = k_1 \ldots k_n$, de sorte que $[u] = [k_1] \ldots [k_n]$. On a, en vertu de la définition (1.32) de la série S_w:

$$(S_w, [u]) = (S_w, [k_1] \ldots [k_n]) = \chi(u = w). \tag{1.36}$$

(Voir aussi Rem. 1.7.1). Donc dans le cas où $w \in H(A)$ et $n \geq 2$ on a:

$$(S_w, [u]) = 0. \tag{1.37}$$

Maintenant, si $h_1, \ldots, h_p, k_1, \ldots, k_n$ sont des mots de Hall et si $p > n$ alors, selon le Lemme 1.7.5, on a:

$$(S_{h_1} \sqcup \ldots \sqcup S_{h_p}, [k_1] \ldots [k_n]) = 0. \tag{1.38}$$

Cette égalité est aussi vraie lorsque $p < n$. En effet, en vertu du Lemme 1.7.3, on a:

$$(S_{h_1} \sqcup \ldots \sqcup S_{h_p}, [k_1] \ldots [k_n]) = (S_{h_1} \otimes \ldots \otimes S_{h_p}, c_p([k_1]) \ldots c_p([k_n])).$$

Or, dans chacun des tenseurs du produit $c_p([k_1]) \ldots c_p([k_n])$, il apparait un terme de la forme $[k_{r_1}] \ldots [k_{r_s}]$ avec $s \geq 2$. On a donc, en vertu de l'observation (1.37), que l'égalité (1.38) est vérifiée lorsque $p < n$.

Le coefficient $(S_{h_1} \sqcup \ldots \sqcup S_{h_p}, [k_1] \ldots [k_n])$ est donc non nul seulement lorsque $p = n$. Dans ce cas, en vertu du Lemme 1.7.6, on a:

$$(S_{h_1} \sqcup \ldots \sqcup S_{h_n}, [k_1] \ldots [k_n]) = \sum_{\sigma} (S_{h_1}, [k_{\sigma(1)}]) \ldots (S_{h_n}, [k_{\sigma(n)}]),$$

où la somme s'étend à toutes les permutations σ de l'ensemble $\{1, \ldots, n\}$.

Posons, comme dans l'énoncé du Théorème:

$$w = h_1^{i_1} \dots h_n^{i_n}, \text{ avec } h_1 > \dots > h_n.$$

Soit $m = \sum_{r=1}^{n} i_r$ et considérons m mots de Hall $k_1, \dots, k_m \in H(A)$ tels que $k_1 \geq \dots \geq k_m$. On a:

$$(S_{h_1}^{i_1} \sqcup\!\sqcup \dots \sqcup\!\sqcup S_{h_n}^{i_n}, [k_1] \dots [k_m])$$
$$= \sum_{\sigma} \underbrace{(S_{h_1}, [k_{\sigma(1)}]) \dots (S_{h_1}, [k_{\sigma(i_1)}])}_{i_1} \dots \underbrace{(S_{h_n}, [k_{\sigma(m-i_n+1)}]) \dots (S_{h_n}, [k_{\sigma(m)}])}_{i_n},$$

où la somme se fait sur toutes les permutations de l'ensemble $\{1, \dots, m\}$. Cette somme est non nulle si et seulement si:

$$h_1 = k_1, \dots, h_{i_1} = k_{i_1}, \dots, h_{m-i_k+1} = k_{m-i_k+1}, \dots, h_m = k_m,$$

en vertu de (1.36). Dans ce cas, les permutations pour lesquelles le produit:

$$(S_{h_1}, [k_{\sigma(1)}]) \dots (S_{h_1}, [k_{\sigma(i_1)}]) \dots (S_{h_n}, [k_{\sigma(m-i_k+1)}]) \dots (S_{h_n}, [k_{\sigma(m)}])$$

est non nul sont celles qui permutent entre eux les i_r facteurs égaux à h_r et elles sont au nombre de $i_1! \dots i_n!$. On en déduit que la série S_w et la série:

$$\frac{1}{i_1! \dots i_n!} S_{h_1}^{i_1} \sqcup\!\sqcup \dots \sqcup\!\sqcup S_{h_n}^{i_n}$$

prennent les mêmes valeurs sur la base PBWH. Elles sont donc égales. La preuve du Th. 1.7.2 est complète. ◇

Le corollaire suivant suit immédiatement des résultats du Th. 1.7.2, comme c'est le cas dans [MR 89].

Corollaire 1.7.7 *Dans le produit tensoriel complété $K\langle\langle A\rangle\rangle \hat{\otimes} K\langle A\rangle$, où le module $K\langle\langle A\rangle\rangle$ est munie de sa structure d'algèbre de mélange et où $K\langle A\rangle$ est munie du produit de concaténation, on a:*

$$\sum_{w \in A^*} w \otimes w = \prod_{h \in H(A)} \exp(S_h \otimes [h]), \tag{1.39}$$

où le produit de droite se fait selon l'ordre décroissant sur $H(A)$.

Démonstration. Le membre droit de (1.39) est égal à:

$$\prod_{h \in H(A)} \sum_{i \geq 0} \frac{1}{i!} S_h^i \otimes [l]^i$$
$$= \sum_{\substack{i_1, \dots, i_n \geq 1 \\ h_1 > \dots > h_n}} \frac{1}{i_1! \dots i_n!} S_{h_1}^{i_1} \sqcup\!\sqcup \dots \sqcup\!\sqcup S_{h_n}^{i_n} \otimes [h_1]^{i_1} \dots [h_n]^{i_n}.$$

En utilisant le Th. 1.7.2, le Th. 1.4.6 sur la factorisation des mots en produit décroissant de mots de Hall et la notation $[w]$ pour décrire la base PBWH, on voit que l'égalité précédente est équivalente à:

$$\sum_{w\in A^*} w\otimes w = \sum_{u\in A^*} S_u \otimes [u]. \tag{1.40}$$

L'identité (1.39) est donc équivalente à $w = \sum_{u\in A^*}(S_u, w)[u]$ qui est vrai par définition. ◇

Dans [MR 89], les résultats du Th. 1.7.2 nous permettait de montrer un résultat de D. E. Radford [Ra 79]. Nous en donnons l'énoncé (voir Rem. 1.5.1 pour les détails sur les mots de Lyndon et l'ordre lexicographique sur les mots).

Théorème 1.7.8 (Radford [Ra 79])
Soit L l'ensemble des mots de Lyndon et $<$ l'ordre lexicographique sur les mots. Soit $w \in A^*$ et

$$w = l_1^{i_1}\dots l_n^{i_n},\ \textit{avec}\ l_1 > \dots > l_n, i_1, \dots, i_n \geq 1$$

sa factorisation en produit décroissant de mots de Lyndon. Alors on a:

$$\frac{1}{i_1!\dots i_n!} l_1^{i_1} \sqcup\!\sqcup \dots \sqcup\!\sqcup l_n^{i_n} = w + \sum_{u<w} \alpha_u u$$

où les coefficients α_u sont des entiers positifs ou nuls et où

$$l_i^{i_k} = \underbrace{l_i \sqcup\!\sqcup \dots \sqcup\!\sqcup l_i}_{i_k}.$$

◇

Remarques 1.7.9 En cours de démonstration, on utilise une propriété importante des polynômes de Lie associés aux mots de Lyndon. Ils sont triangulaires; plus précisément, si $l \in L$ alors:

$$[l] = l + \sum_{u>l} \beta_u u.$$

Or, cette propriété n'est pas vérifiée pour les bases de Hall générales pour l'ordre $<_H$ duquel on aurait pu s'y attendre. En effet, par exemple *abba* est un mot de Hall d'un ensemble de Hall dont les mots de degré au plus cinq sont ceux de l'Ex. 1.2.1. Son polynôme de Lie associé est:

$$[abba] = [[[a,b]b]a] = bbaa - 2baba - aabb + 2abab.$$

Le mot $abba$ n'y apparaît pas. De plus, on a:

$$\begin{aligned} bbaa &= (b)(b)(a)(a) >_H abba, \\ baba &= (b)(aba) >_H abba, \\ aabb &= (a)(abb) >_H abba, \\ abab &= (ab)(ab) <_H abba. \end{aligned}$$

Ainsi, on pouvait s'attendre à ce que les polynômes:

$$\frac{1}{i_1! \dots i_n!} h_1^{i_1} \sqcup \dots \sqcup h_n^{i_n},$$

dans l'algèbre de mélange $K\langle A\rangle$, ne soient pas linéairement indépendants. Et c'est le cas. En effet, sur un alphabet à trois lettres $A = \{a, b, c\}$ avec $a < b < c$ on a $ab, ac, bc \in H(A)$. Il se pourrait que ces mots soient ordonnés par: $ab < bc < a < ac < b < c$. Ainsi, on aurait $acb, bca \in H(A)$. Mais alors on trouve une relation entre les polynômes:

$$b \sqcup ac - a \sqcup bc = acb - bca.$$

Néanmoins, comme on le mentionait dans [MR 89], la base $S_w, w \in A^*$ nous fournit une base de l'algèbre de mélange $K\langle A\rangle$. En effet, par dualité (Eq. (1.40)), tout mot s'écrit:

$$w = \sum_{u \in A^*} (u, [w]) S_u,$$

de sorte qu'en utilisant le Th. 1.7.2, on voit que $K\langle A\rangle$ est linéairement engendrée par les monômes en les séries $S_h, h \in H(A)$:

$$\frac{S_{h_1}^{i_1} \sqcup \dots \sqcup S_{h_n}^{i_n}}{i_1! \dots i_n!}.$$

◇

Chapitre 2

Réécritures dans le groupe libre

2.1 Introduction.

C'est P. Hall [HP 33], qui le premier présentait un système de réécriture de suites de commutateurs dans le groupe libre à deux générateurs. M. Hall [HM 50a] allait reprendre sa méthode et introduire les *commutateurs basiques* dans les groupes libres, ainsi que le '*collecting process*' qui permet de calculer, pour chaque élément du groupe libre, une décomposition unique en produit (décroissant) de commutateurs basiques. Plusieurs auteurs (que nous avons cités au Chap. 1) ont donné des généralisations des travaux de M. Hall. Soulignons entre autres Gorčakov [Go 69], Lyndon [CFL 58] et Meier-Wunderli [MW 52].

Le calcul avec les commutateurs basiques est au groupe libre ce que le calcul avec les 'Bases de Hall' (voir Chap. 1) est à l'algèbre de Lie libre. En effet, Magnus [Ma 37] a donné un isomorphisme entre la suite des quotients de la série centrale descendante du groupe libre et l'algèbre de Lie libre (voir Cor. 2.4.6). Ces familles de commutateurs basiques peuvent toutes être obtenues à l'aide de constructions d'arbres dont les feuilles sont étiquettées par des lettres. Les conditions 'optimales' (1.1), (1.2) et (1.3) (données par Viennot [Vi 76]), qu'il faut imposer à un ensemble d'arbres pour obtenir une base de l'algèbre de Lie libre, doivent aussi être imposées si on veut obtenir une base des quotients de la série centrale descendante. Dans ce sens, les conditions de Viennot (sur les arbres du magma libre) généralisent les constructions (dans le groupe libre) des auteurs que nous avons mentionnés plus haut. Ainsi, on obtiendra d'un ensemble d'arbres de Hall (voir Chap. 1, paragraphe 1.2), un ensemble de commutateurs dans le groupe libre. Ces commutateurs seront appelés des *commutateurs de Hall*.

Ce deuxième chapitre se compose de trois parties. Tout d'abord, nous présentons un

système de réécriture dans le groupe libre, similaire à celui que nous avons développé au Chap. 1, puis nous mettons à jour ses propriétés. Il permet d'effectuer le calcul d'une décomposition en produit de commutateurs de Hall. La convergence de l'algorithme fourni par le système de réécriture n'est pas immédiate puisque les suites peuvent croître en longueur au cours du calcul. A notre connaissance, personne n'a encore donné de démonstration de la *convergence* du calcul. Les bases de P. Hall et de M. Hall sont ordonnées selon le *degré* des commutateurs; la convergence des calculs paraît alors assez évidente. Gorčakov [Go 69], qui semblait avoir constaté que seules les conditions (1.1), (1.2) et (1.3) suffisaient pour arriver à calculer une décomposition en produit de commutateurs basiques, n'en donne pas de démonstration (il ne montre pas non plus l'unicité de la décomposition). Nous donnons une démonstration de la convergence des calculs en codant de façon appropriée les *'montées'* des suites de commutateurs de Hall (Prop. 2.2.8).

Le choix des exposants (positifs ou négatifs) des commutateurs dans une suite donne lieu à cinq règles de réécriture. La simplification possible de deux commutateurs consécutifs d'une suite représente en quelque sorte une perte d'information sur la suite. Il n'est plus possible 'd'inverser' les réécritures pour remonter à la suite de départ. Néanmoins, on peut montrer la *confluence* de la réécriture. C'est ce que nous faisons au paragraphe 2.3.

Les propriétés du système de réécriture ne suffisent pas à montrer que la décomposition en produit de commutateurs de Hall est unique. Nous avons donc élaboré, dans un deuxième temps, un argument algébrique qui permet de montrer l'unicité de la décomposition. En cela nous suivons M. Hall [HM 50a] et Lyndon [CFL 58].

Magnus a donné un isomorphisme du groupe libre $F(A)$, sur un ensemble de générateurs A, dans un groupe de séries formelles à variables non commutatives dans A (voir par exemple [Ma 37, MKS 76]). Cet isomorphisme est appelé la *transformée de Magnus* du groupe libre $F(A)$. Nous avons recours au calcul à l'aide de la transformée de Magnus pour montrer l'unicité de la décomposition des éléments du groupe libre en produit de commutateurs de Hall. On donne, au paragraphe 2.4, une relation qui permet de calculer l'exposant $n_h(g)$ d'un commutateur de Hall h dans la décomposition d'un élément g du groupe libre, à l'aide des coefficients de la série formelle associée à g (Eq. 2.17). Cette relation nous permet de conclure à l'unicité des exposants dans la décomposition en produit de commutateurs de Hall des éléments du groupe libre (Th. 2.4.4). On en déduit facilement un résultat de Magnus [Ma 37] et Witt [Wi 37]: les commutateurs de Hall de degré N forment une base du $N^{\text{ième}}$ groupe quotient de la série centrale descendante du groupe libre (Cor. 2.4.5).

Une identité du même type que la relation (2.17) a été donnée par Thérien [Th 83], pour les bases de M. Hall. Il a montré que l'exposant $n_h(g)$ est une *combinaison linéaire* des coefficients de sa transformée de Magnus lorsque g est un *mot positif* du groupe libre (un produit d'éléments de A, tous avec exposants positifs). Ce résultat lui a permis d'obtenir une description des parties du monoïde libre qui sont reconnues par certains groupes

nilpotents. Au paragraphe 2.5, nous reprenons le résultat de Thérien et montrons qu'il est toujours vérifié pour les bases de Hall générales (Lemme 2.5.3).

Au paragraphe 2.6, nous montrons que l'identité de Thérien (Eq. 2.19) s'étend au groupe libre tout entier, et qu'elle est identique à la relation obtenue des calculs à l'aide de la transformée de Magnus (voir Th. 2.6.1). Nous en tirons de nouvelles démonstrations de deux importants théorèmes de la théorie combinatoire des groupes. Le premier, dû à Magnus [Ma 37], donne une caractérisation des éléments du $n^{\text{ème}}$ groupe de la série centrale descendante de $F(A)$: un élément du groupe libre en fait partie si et seulement si les mots non vides qui apparaîssent dans sa transformée de Magnus sont de longueur au moins n (Cor. 2.6.2). Le second théorème avait permis à P. Hall [HP 33] de montrer plusieurs propriétés des p-groupes réguliers. Il affirme que l'exposant $n_h(g^x)$ est donné par une fonction polynômiale (en x) sans terme constant (Cor. 2.6.4).

C. Reutenauer avait conjecturé que l'identité de Thérien était vérifiée dans le groupe libre tout entier et sa conjecture fut à l'origine des travaux qui sont exposés dans ce chapitre.

2.2 Suites standard dans $F(A)$ et système de réécriture.

On se donne un alphabet A et on considère l'alphabet auxiliaire $A^{-1} = \{a^{-1} : a \in A\}$. Le groupe libre sur A, qu'on note $F(A)$, peut être construit de la façon suivante. On forme le quotient du monoïde libre $(A \cup A^{-1})^*$ par la congruence $\equiv$ engendrée par les relations:

$$aa^{-1} \equiv a^{-1}a \equiv 1, \quad a \in A. \tag{2.1}$$

Par construction, a et a^{-1} sont l'inverse l'un de l'autre. Soit $g = a_1^{\epsilon_1} \dots a_m^{\epsilon_m}$, $a_i \in A, \epsilon_i = \pm 1$, un élément du groupe libre. On dira que g est un *mot réduit* si pour tout $i = 1, \dots, m-1$ on a soit $a_i \neq a_{i+1}$, soit $a_i = a_{i+1}$ et $\epsilon_i = \epsilon_{i+1}$. En d'autre mots, g est un mot réduit si on ne peut pas y simplifier deux lettres successives à l'aide de (2.1). Ce même élément g est appelé un *mot positif* si $\epsilon_i = 1$ pour tout $i = 1, \dots, m$. Evidemment, un mot positif est un mot réduit. A tout élément $g \in F(A)$ il correspond un unique mot réduit $\bar{g}$ tel que $g = \bar{g}$.

Soient $g, h \in F(A)$. On définit leur *commutateur* $[g, h]$ par

$$[g, h] = g^{-1}h^{-1}gh.$$

On étend cette notation aux sous-groupes de $F(A)$. Plus précisément, si H, K sont des sous-groupes de $F(A)$, on pose:

$$[H, K] = < \{[h, k] : h \in H, k \in K\} >,$$

où $< X >$ désigne le sous-groupe engendré par les éléments d'un ensemble $X \subset F(A)$. On définit récursivement une suite $F_1, F_2, \ldots, F_n, \ldots$ de sous-groupes de $F(A)$:

$$F_1 = F(A),$$

et pour $n \geq 1$:

$$F_{n+1} = [F_n, F_1].$$

La suite $F_1, \ldots, F_n, \ldots$ est appelée la *suite centrale descendante* du groupe libre. Ces sous-groupes satisfont la suite d'inclusion:

$$F_1 \supset F_2 \supset \ldots \supset F_n \supset \ldots \tag{2.2}$$

Le sous-groupe F_{n+1} est normal dans F_n et les groupes quotients F_n/F_{n+1} sont des groupes abéliens. Au paragraphe 2.4, nous tirerons avantage de la structure de Z-module de ces groupes abéliens.

Remarque 2.2.1 Soit $m < n$. Si g_1 et g_2 sont deux éléments de $F(A)$ tels que $g_1 \equiv g_2 \mod F_n$ alors $g_1 \equiv g_2 \mod F_m$, en vertu des inclusions (2.2). ◇

Remarque 2.2.2 On dit qu'un arbre t du magma libre $M(A)$ (voir paragraphe 1.2) est un *peigne de degré n* si t' est un peigne de degré $n-1$ et t'' est une lettre; les peignes de degré un sont les lettres de A (voir Fig. 2.1). On peut montrer, à l'aide de relations du type (2.4) et (2.5), que F_n est le sous-groupe engendré par les peignes de degré n (pour plus de détails, voir [HM 59, MKS 76]). ◇

Remarque 2.2.3 Lorsque $n = 1$, F_1/F_2 est le groupe abélien libre sur A. On peut montrer que deux éléments $g = a_1^{\epsilon_1} \ldots a_m^{\epsilon_m}$ et $h = b_1^{\eta_1} \ldots b_n^{\eta_n}$ sont congruents modulo F_2 si et seulement si pour toute lettre $a \in A$, la somme des exposants que porte cette lettre dans g et dans h est la même. C'est-à-dire qu'on doit avoir $\sum_{i=1}^{m} \chi(a_i = a)\epsilon_i = \sum_{j=1}^{n} \chi(b_j = a)\eta_j$, pour tout $a \in A$. Il est donc possible d'associer à tout $g \in F_1 = F(A)$ un unique mot réduit $\bar{g} = a_1^{\alpha_1} \ldots a_p^{\alpha_p}$ avec $\alpha_i \in Z$, tel que $g \equiv \bar{g} \mod F_2$. Si de plus l'alphabet A est totalement ordonné, on peut toujours faire en sorte que $a_1 > \ldots > a_p$. ◇

On définit récursivement une application $\kappa : M(A) \rightarrow F(A)$ par:

$$\kappa(t) = [\kappa(t'), \kappa(t'')], \text{ si } t = [t', t''].$$

L'image d'un arbre t de $M(A)$ est obtenue en interprétant chaque sommet interne de la structure arborescente de t comme le commutateur de ses sous-arbres gauche et droit dans le groupe libre. On a aussi un plongement $A^* \hookrightarrow F(A)$ du monoïde libre dans le groupe libre, dont l'image est l'ensemble des mots positifs de $F(A)$.

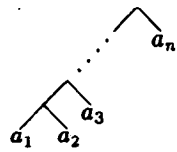

Figure 2.1: Représentation par arbre du peigne $[[[[a_1, a_2]a_3]\ldots]a_n] \in F_n$.

Supposons à partir de maintenant que l'alphabet A est totalement ordonné et choisissons un ensemble de Hall $H(A)$ (voir paragraphe 1.2). On peut, à l'aide de l'application κ considérer les arbres de Hall comme des éléments du groupe libre. Les éléments de l'ensemble: $\{\kappa(h) : h \in H(A)\}$ seront appelés des *commutateurs de Hall.* L'ensemble des commutateurs de Hall est donc totalement ordonné, par l'ordre $\leq$ sur l'ensemble de Hall $H(A)$. On définit le *degré d'un commutateur de Hall* $\kappa(h)$, comme étant le degré de l'arbre de Hall h.

Notations. Le Th. 1.3.3 met en bijection les mots de Hall et les arbres de Hall. La structure arborescente accompagne le mot de Hall et lui est intrinsèque. C'est cette structure arborescente qui permet à κ de calculer le commutateur associé à l'arbre $h \in H(A)$. On pourrait donc définir l'application κ sur l'ensemble des mots de Hall, en invoquant le Th. 1.3.3. C'est pourquoi, dans tout ce chapitre, nous écrirons $[h]$ pour désigner le commutateurs de Hall $\kappa(h)$ associé au *mot de Hall* h. Ainsi, si h et k sont des mots de Hall tels que hk est un mot de Hall, on a $[hk] = [[h], [k]]$. Cette notation a déjà été utilisée au Chap. 1 (voir page 29). Nous levons toute ambiguité possible dans ce chapitre. Nous n'utiliserons cette notation que pour désigner les commutateurs de Hall. Dans le cas où h est une lettre, $h = a \in A$, nous écrirons plus simplement $[a] = a$ (puisque le commutateur d'un seul élément n'est pas défini). $\diamond$

On considère maintenant des suites de commutateurs de Hall de degré au plus N,

$$s = ([h_1]^{\epsilon_1}, \ldots, [h_n]^{\epsilon_n}), \tag{2.3}$$

avec $h_i \in H(A)$, $|h_i| \leq N$ et $\epsilon_i = \pm 1$. Nous dirons que l'élément du groupe libre $\gamma(s) = [h_1]^{\epsilon_1} \ldots [h_n]^{\epsilon_n}$ est *l'élément associé à la suite* s. On dira qu'une *sous-suite* $s' = ([h_{i_1}]^{\epsilon_{i_1}}, \ldots, [h_{i_k}]^{\epsilon_{i_k}})$ de la suite (2.3) est connexe si la suite d'entiers $1 \leq i_1 < \ldots < i_k \leq n$ est une suite d'*entiers consécutifs*. On dira que la suite (2.3) est une *suite standard* si la suite (de mots de Hall) $(h_1, \ldots, h_n)$ est standard au sens du paragraphe 1.4 (c'est-à-dire si elle satisfait la condition (1.9)). Par exemple, si $g = a_1^{\epsilon_1} \ldots a_m^{\epsilon_m}$ alors la suite $s = (a_1^{\epsilon_1}, \ldots, a_m^{\epsilon_m})$ est standard et $\gamma(s) = g$ est l'élément associé à s. Aussi, si $h_1 \geq \ldots \geq h_n$ alors la suite (2.3) est standard. De même, on définit les *montées*, les *montées éloignées* et les *montées légales* de la suite s comme en (1.10) et (1.11) au paragraphe 1.4.

Nous allons montrer que pour tout élément g du groupe libre il existe une unique suite décroissante s telle que g est congru à $\gamma(s)$, modulo le $(N+1)^{\text{ième}}$ groupe de la série

centrale descendante. Nous allons obtenir la factorisation de $g = a_1^{\epsilon_1} \dots a_m^{\epsilon_m}$ à partir de la suite $s = (a_1^{\epsilon_1}, \dots, a_m^{\epsilon_m})$ de ses lettres, en réécrivant les termes consécutifs d'une montée légale, passant ainsi d'une suite standard à une autre suite standard (de commutateurs de Hall), toutes deux associées à des éléments de $F(A)$ congruents modulo F_{N+1}.

Soient $g = a_1^{\epsilon_1} \dots a_m^{\epsilon_m}$ et $s = (a_1^{\epsilon_1}, \dots, a_m^{\epsilon_m})$ la suite standard à partir de laquelle le calcul de la factorisation de g sera fait. En cours de calcul, on pourra être amené à effectuer des réécritures sur des montées légales de l'un des types: $([h_i], [h_{i+1}])$, $([h_i], [h_{i+1}]^{-1})$, $([h_i]^{-1}, [h_{i+1}])$, ou $([h_i]^{-1}, [h_{i+1}]^{-1})$. Un calcul simple montre que pour $x, y, z \in F(A)$ on a les relations:

$$yx = xy[y, x], \tag{2.4}$$

$$[x, yz] = [x, z][x, y][[x, y], z]. \tag{2.5}$$

Nous allons tirer de ces relations, les règles de réécriture qu'il nous faut. Dans un premier temps, nous allons obtenir des congruences (mod F_{N+1}). On a, par (2.5), avec $z = y^{-1}$:

$$1 = [x, yy^{-1}] = [x, y^{-1}][x, y][[x, y], y^{-1}],$$

ou de façon équivalente:

$$[x, y^{-1}] = [[x, y], y^{-1}]^{-1}[x, y]^{-1}. \tag{2.6}$$

De même, par (2.6), encore une fois:

$$[[x, y], y^{-1}] = [[[x, y], y], y^{-1}]^{-1}[[x, y], y]^{-1}.$$

Ainsi, pour m assez grand:

$$[x, y^{-1}] \equiv [xy^2][xy^4] \dots [xy^{2m}][xy^{2m\pm1}]^{-1} \dots [xy^3]^{-1}[xy]^{-1} \pmod{F_{N+1}}.$$

Donc, en utilisant (2.4) on trouve:

$$\begin{aligned} xy^{-1} &= y^{-1}x[x, y^{-1}], \\ &\equiv y^{-1}x[xy^2] \dots [xy^{2m}][xy^{2m\pm1}]^{-1} \dots [xy]^{-1} \\ &\quad \pmod{F_{N+1}}. \end{aligned} \tag{2.7}$$

En développant le commutateur $[x, y]$, on trouve l'égalité:

$$x^{-1}y = y[x, y]^{-1}x^{-1}. \tag{2.8}$$

Finalement, on observe que $x^{-1}y^{-1} = y^{-1}(yxy^{-1})^{-1}$. De (2.7) on obtient:

$$yxy^{-1} \equiv x[xy^2] \dots [xy^{2m}][xy^{2m\pm1}]^{-1} \dots [xy]^{-1} \pmod{F_{N+1}},$$

d'où:

$$\begin{aligned} x^{-1}y^{-1} &= y^{-1}(yxy^{-1})^{-1} \\ &\equiv y^{-1}[xy]\dots[xy^{2m\pm1}][xy^{2m}]^{-1}\dots[xy^2]^{-1}x^{-1} \qquad (2.9) \\ &\quad (\text{mod } F_{N+1}). \qquad (2.10) \end{aligned}$$

Maintenant, on définit des règles de réécriture des suites standard de commutateurs de Hall à partir des congruences ci-haut. Soient $[h]$ et $[k]$ des commutateurs de Hall. Supposons que $([h]^\epsilon, [k]^\delta)$ soit une montée légale d'une suite standard s. Alors on peut *réécrire* s en une nouvelle suite s', en substituant à la montée légale $([h]^\epsilon, [k]^\delta)$ l'un des membres droits des règles de réécritures suivantes, choisi selon les valeurs de ϵ et δ:

(R1) $([h],[k]) \rightarrow ([k],[h],[hk])$ ou simplement $([h],[k]) \rightarrow ([k],[h])$, selon que la longueur du mot hk est $|hk| \leq N$ ou $|hk| > N$.

(R2) $([h],[k]^{-1}) \rightarrow ([k]^{-1},[h],[hk^2],\dots,[hk^{2m}],[hk^{2m\pm1}]^{-1},\dots,[hk]^{-1})$.

(R3) $([h]^{-1},[k]) \rightarrow ([k],[h,k]^{-1},[h]^{-1})$ ou simplement $([h]^{-1},[k]) \rightarrow ([k],[h]^{-1})$, selon que la longueur du mot hk est $|hk| \leq N$ ou $|hk| > N$.

(R4) $([h]^{-1},[k]^{-1}) \rightarrow ([k]^{-1},[hk],\dots,[hk^{2m\pm1}],[hk^{2m}]^{-1},\dots,[hk^2]^{-1},[h]^{-1})$.

Remarque 2.2.4 Il faudra, dans le cas des réécritures (R2) et (R4) choisir l'entier m le plus grand possible, en prenant soin que dans la nouvelle suite tous les commutateurs soient de degré $\leq N$. Dans l'expression $[hk^{2m\pm1}]$ le choix du signe $+$ ou $-$ se fera selon ce critère. ◇

Soient s et s' deux suites standard telles que s' soit obtenue de s par réécriture d'une montée légale. Alors on a $\gamma(s) \equiv \gamma(s')$, en vertu des congruences (2.4), (2.7), (2.8) et (2.9).

Une dernière règle de réécriture nous sera nécessaire. Soit $s = ([h_1]^{\epsilon_1},\dots,[h_n]^{\epsilon_n})$ une suite standard. Si $[h_i] = [h_{i+1}]$ et $\epsilon_i = -\epsilon_{i+1}$ alors on admet la réécriture:

(R5) $s \rightarrow' ([h_1]^{\epsilon_1},\dots,[h_{i-1}]^{\epsilon_{i-1}},[h_{i+2}]^{\epsilon_{i+2}},\dots,[h_n]^{\epsilon_n})$.

On dira dans ce cas qu'on a *effacé* les termes $[h_i]$ et $[h_{i+1}]$. Observez que plusieurs choix de réécritures peuvent se présenter simultanément. Comme nous le verrons, il sera toujours possible de n'effectuer que des réécritures du type (R1), (R2), (R3) ou (R4) jusqu'à l'obtention d'une suite standard décroissante. Puis, on pourra utiliser la règle (R5) pour simplifier la suite. Nous désignons par Γ le système de réécriture qui opère

sur les suites standard et qui n'utilise que les règles (R1), (R2), (R3) ou (R4); et par Γ' le système de réécriture qui opère sur les suites standard et qui utilise toutes les règles: (R1), (R2), (R3), (R4) ou (R5). Dans Γ les effacements ne sont pas permis, alors que dans Γ' ils le sont.

Exemple 2.2.5 Soit $H(A)$ un ensemble de Hall dont les éléments de degré au plus cinq sont ceux de l'Ex. 1.2.1. Posons, pour les besoins de l'exemple, $N = 4$. Soit $g = a^{-1}bab^{-1}$, l'élément du groupe libre que nous allons réécrire:

$$\begin{aligned}
&(\boldsymbol{a^{-1}}, \boldsymbol{b}, a, b^{-1}) \\
(\text{R3})\rightarrow\quad &(b, [ab]^{-1}, a^{-1}, \boldsymbol{a}, \boldsymbol{b^{-1}}) \\
(\text{R2})\rightarrow\quad &(b, [ab]^{-1}, \boldsymbol{a^{-1}}, \boldsymbol{b^{-1}}, a, [ab^2], [ab^3]^{-1}, [ab]^{-1}) \\
(\text{R4})\rightarrow\quad &(b, [ab]^{-1}, b^{-1}, [ab], [ab^3], [ab^2]^{-1}, \boldsymbol{a^{-1}}, \boldsymbol{a}, \\
&\qquad [ab^2], [ab^3]^{-1}, [ab]^{-1})
\end{aligned}$$

Une suite d'applications de (R5) donne:

$$\begin{aligned}
\rightarrow'\quad &(b, [ab]^{-1}, b^{-1}, [ab], [ab^3], [\boldsymbol{ab^2}]^{-1}, [\boldsymbol{ab^2}], [ab^3]^{-1}, [ab]^{-1}) \\
\rightarrow'\quad &(b, [ab]^{-1}, b^{-1}, [ab], [\boldsymbol{ab^3}], [\boldsymbol{ab^3}]^{-1}, [ab]^{-1}) \\
\rightarrow'\quad &(b, [\boldsymbol{ab}]^{-1}, b^{-1}, [ab], [ab]^{-1})
\end{aligned}$$

Puis:

$$\begin{aligned}
(\text{R4})\rightarrow\quad &(\boldsymbol{b}, \boldsymbol{b^{-1}}, [ab^2], [ab^3]^{-1}, [ab]^{-1}, [ab], [ab]^{-1}) \\
(\text{R5})\rightarrow'\quad &([ab^2], [ab^3]^{-1}, [\boldsymbol{ab}]^{-1}, [\boldsymbol{ab}], [ab]^{-1}) \\
(\text{R5})\rightarrow'\quad &([\boldsymbol{ab^2}], [\boldsymbol{ab^3}]^{-1}, [ab]^{-1}) \\
(\text{R2})\rightarrow\quad &([ab^3]^{-1}, [ab^2], [ab]^{-1})
\end{aligned}$$

A chaque fois la montée légale qui est réécrite est en caractère gras et la règle appliquée est indiquée à l'extrême gauche. Une flèche $\rightarrow$ précède les réécritures qui se font à l'aide de Γ. Une flèche 'primée' $\rightarrow'$ précède les effacements (permis dans Γ'). La dernière suite est décroissante, et simplifiée. On a donc:

$$a^{-1}bab^{-1} \equiv [ab^3]^{-1}[ab^2][ab]^{-1} \pmod{F_5},$$

et on peut vérifier que ce produit est décroissant. ◇

Proposition 2.2.6 *Soit $s = ([h_1]^{\epsilon_1}, \ldots, [h_n]^{\epsilon_n})$ une suite standard de commutateurs de Hall. Alors toute suite t obtenue de s, à l'aide d'une réécriture de l'un des systèmes Γ ou Γ', est standard.*

Démonstration. Comme toute sous-suite d'une suite standard est une suite standard, il est clair que si t est obtenue de s à l'aide de (R5), t est standard.

En ce qui concerne les autres règles de réécriture, il faut remarquer les choses suivantes. Soit $([h]^\epsilon, [k]^\delta)$ la montée légale qui fait l'objet de la réécriture. Premièrement, dans le membre droit des règles (R1), (R2), (R3) et (R4), le terme $[k]^\delta$ précède toujours le terme $[h]^\epsilon$. Deuxièmement, dans ce membre droit les termes $[h]^\epsilon$ et $[k]^\delta$ sont toujours suivis (à droite) de termes de la forme $[hk^{2m\pm1}]^{\pm1}$.

Maintenant, soient h, k des mots de Hall tels que $h < k$ et $h'' \geq k$. Si r est un autre mot de Hall tel que $r'' \geq k$ alors on a $r'' \geq hk^p$ pour tout $p \geq 1$, puisque par (1.6), $hk^p < k$. Aussi, si r est un mot de Hall tel que $k \geq r$ alors on a $(hk^p)'' = k \geq r$.

Ces remarques, jumelées à la démonstration de la Prop. 1.4.4, serviront au lecteur à montrer la Prop. 2.2.6. ◇

Dans le cas où t est obtenue à l'aide de Γ ou Γ', on dira qu'elle est *obtenue par réécriture de la montée légale* $([h_i], [h_{i+1}])$, ou encore que t *est dérivée de* s. Notez que la *convergence* du système de réécriture n'est pas immédiate, puisque la longueur de la suite t peut excéder la longueur de la suite s (voir Ex. 2.2.5).

Rappelons qu'une *montée éloignée* de la suite s est un couple $([h], [k])$ dans s tels que: $[h]$ vient avant $[k]$ dans s (en lisant de gauche à droite) et $h < k$. Soit $\leq$, l'ordre donné sur $H(A)$. Soit $\leq_{\text{deg}}$, la relation qui ordonne les éléments de $H(A)$ par degré, puis sur chacun des degrés, par l'ordre induit de $\leq$. On définit un ordre total $\preceq$ sur l'ensemble des couples de mots de Hall de la façon suivante: $(h_1, k_1) \prec (h_2, k_2)$ si et seulement si soit $k_1 > k_2$, soit $k_2 = k_1$ et $h_1 <_{\text{deg}} h_2$ (notez le renversement de l'ordre en deuxième composante).

On associe à une suite standard s, un vecteur d'entiers $v(s)$ dont les entrées sont indicées par les couples (h, k) de mots de Hall de degré au plus N, tels que $h < k$. L'entrée $v_{(h,k)}(s)$ est égale au nombre de montées éloignées $([h]^\epsilon, [k]^\delta)$ (toutes valeurs de ϵ et δ confondues) dans la suite s. On ordonne l'ensemble de ces vecteurs lexicographiquement. C'est-à-dire que deux vecteurs d'entiers v', v'' sont en relation $v' < v''$ si et seulement s'il existe un couple de mots de Hall (h, k) tel que $v'_{(r,p)} = v''_{(r,p)}$ pour tout $(r, p) \prec (h, k)$ et $v'_{(h,k)} < v''_{(h,k)}$.

Lemme 2.2.7 *Soit s et t des suites standard telles que t soit obtenue de s à l'aide de Γ. Alors $v(t) < v(s)$.*

Démonstration. Soit (h, k) la montée légale dans s sur laquelle s'effectue la réécriture. On a alors $v_{(h,k)}(t) = v_{(h,k)}(s) - 1$. En examinant les règles de réécriture (R1), (R2), (R3) et (R4) on voit que les montées éloignées dans t, qui *s'ajoutent* à celle qui viennent de s, sont de l'une des trois formes suivantes (selon qu'elles mettent en jeu un terme de s et

un terme nouvellement créé – pour les deux premiers cas, ou deux termes nouvellement créés).

Soit elles sont de la forme $([r],[hk^m])$, avec $m \geq 1$, où $[r]$ est un élément de la suite qui se trouvait (dans s) à gauche de $[h]$. Dans ce cas, on a $(r, hk^m) \succ (h,k)$, puisque par (1.6), $hk^m < k$.

Soit elles sont de la forme $([hk^m],[r])$, avec $m \geq 1$, où $[r]$ est un élément de la suite qui se trouvait (dans s) à droite de $[k]$. Comme la montée $([h],[k])$ dans s est légale, on a $k \geq r$. Si $k > r$ alors $(h,k) \prec (hk^m, r)$; si, $k = r$ alors comme $|h| < |hk^m|$ on trouve encore une fois $(h,k) \prec (hk^m, r)$.

Soit elles sont de la forme $([p],[r])$, où $[r]$ et $[p]$ sont deux termes qui apparaîssent dans le membre droit de l'une des règles (R1), (R2), (R3) ou (R4). Chacune de ces suites débute par $[k]$, et il en est l'élément maximal. Par conséquent, on a $[r] = [hk^i], [p] = [hk^j]$ avec $i, j \geq 0$ et $i \neq j$. Comme on a $h < k$ par hypothèse, et $hk^i < k$ (pour $i \geq 1$) par (1.6), on en déduit $(h,k) \prec (p,r)$.

On voit donc que $v_{(r,p)}(s) = v_{(r,p)}(t)$, pour tout $(r,p) \prec (h,k)$; comme $v_{(h,k)}(t) = v_{(h,k)}(s) - 1$, on a bien $v(t) < v(s)$. ◇

Théorème 2.2.8 *Les systèmes de réécriture* Γ *et* Γ' *sont convergents.*

Démonstration. Nous allons montrer la proposition par récurrence sur le couple $(v(s), |s|)$, où $|s|$ désigne la longueur de la suite s. Le résultat est vérifié pour les suites qui ont un vecteur $v(s) = \mathbf{0}$. Ces suites sont soit vides, soit réduites à un seul terme, soit décroissantes. La seule réécriture applicable à une suite décroissante est un effacement et dans ce cas on en diminue la longueur. Le système de réécriture converge donc sur les suites décroissantes. Soit s une suite standard qui n'est pas décroissante.

Soit t une suite qui s'obtient par réécriture de la suite s. Si t s'obtient de s à l'aide de (R5), alors on a $|t| < |s|$. Si t s'obtient de s à l'aide de Γ, alors on a $v(t) < v(s)$, selon le Lemme 2.2.7. Par récurrence, le système de réécriture est convergent sur la suite t, par conséquent il l'est sur la suite s. ◇

Exemple 2.2.9 Reprenons l'Ex. 2.2.5, mais cette fois avec $N = 3$. On donne, selon l'ordre $\preceq$, la liste des couples (h,k) (avec $h < k$ et $|h|, |k| \leq 3$):

$$(a,b)\ \ (ab,b)\ \ (aba,b)\ \ (abb,b)\ \ (ab,a)\ \ (aba,a)$$

$$(abb,a)\ \ (ab,abb)\ \ (aba,abb)\ \ (aba,ab).$$

On indique, à droite d'une suite s, son vecteur de montées éloignées et sa longueur $(v(s);|s|)$:

$$\begin{array}{cll}
 & (a^{-1},b,a,b^{-1}) & (3,0,0,0,0,0,0,0,0,0;4)\\
\to & (b,[ab]^{-1},a^{-1},a,b^{-1}) & (2,1,0,0,2,0,0,0,0,0;5)\\
\to & (b,[ab]^{-1},a^{-1},b^{-1},a,[ab^2],[ab]^{-1}) & (1,1,0,0,2,0,0,1,0,0;7)\\
\to & (b,[ab]^{-1},b^{-1},[ab],[ab^2]^{-1},a^{-1},a,[ab^2],[ab]^{-1}) & (0,1,0,0,4,0,2,4,0,0;9)\\
\to' & (b,[ab]^{-1},b^{-1},[ab],[ab^2]^{-1},[ab^2],[ab]^{-1}) & (0,1,0,0,0,0,0,4,0,0;7)\\
\to' & (b,[ab]^{-1},b^{-1},[ab],[ab]^{-1}) & (0,1,0,0,0,0,0,0,0,0;5)\\
\to & (b,b^{-1},[ab^2],[ab]^{-1},[ab],[ab]^{-1}) & (0,0,0,0,0,0,0,0,0,0;6)\\
\to' & ([ab^2],[ab]^{-1},[ab],[ab]^{-1}) & (0,0,0,0,0,0,0,0,0,0;4)\\
\to' & ([ab^2],[ab]^{-1}) & (0,0,0,0,0,0,0,0,0,0;2)
\end{array}$$

◇

2.3 Confluence.

En accord avec les notations précédemment utilisées, on définit deux relations $\to$ et $\to'$ sur l'ensemble des suites standard:

$$s \to t \text{ si et seulement si } t \text{ est dérivée de } s \text{ à l'aide de } \Gamma,$$

et

$$s \to' t \text{ si et seulement si } t \text{ est dérivée de } s \text{ à l'aide de } \Gamma'.$$

On notera par $\overset{*}{\to}$ et $\overset{*}{\to}'$ les fermetures réflexives et transitives des relations $\to$ et $\to'$, respectivement. Comme au paragraphe 1.4, nous dirons que t est dérivée de s si $s\overset{*}{\to}t$ ou si $s\overset{*}{\to}'t$.

Lemme 2.3.1 *Soient $h,k \in H(A)$ des mots de Hall tels que $h < k$ et $\epsilon,\delta = \pm 1$ tels que les suites $s_1 = ([h]^{-\epsilon},[h]^{\epsilon},[k]^{\delta})$ et $s_2 = ([h]^{\epsilon},[k]^{\delta},[k]^{-\delta})$ soient standard. Supposons que dans chacune de ces suites la montée $([h],[k])$ soit légale. Soient t_1 et t_2 les suites obtenues de s_1 et s_2 en réécrivant ces montées:*

$$s_1 \to t_1, \quad s_2 \to t_2,$$

alors il existe des dérivations:

$$t_1 \overset{*}{\to}'([k]^{\delta}), \quad t_2 \overset{*}{\to}'([h]^{\epsilon}) .$$

Démonstration. Dans les calculs qui vont suivre, nous laissons au lecteur le soin de vérifier que les montées auxquelles on applique une réécriture de Γ' sont bien légales. On le voit facilement, en vertu du fait que toutes les montées $([r],[p])$ sujettes à des réécritures, ont comme deuxième composante $[p] = [k]$, et que $k > hk^m$ pour tout $m \geq 0$. Toutes les réécritures qui seront effectuées au cours de la démonstration de ce lemme sont des réécritures de Γ'. Dans le but d'alléger les notations, nous omettrons le $'$ et indiquerons ces réécriture avec une simple flèche $\rightarrow$. Concentrons nous d'abord sur $s_1 = ([h]^{-\epsilon}, [h]^{\epsilon}, [k]^{\delta})$. On considère quatre cas selon les valeurs relatives de ϵ et δ.

Cas 1: $\epsilon = 1, \delta = 1$. On a:

$$\begin{aligned}
& s_1 = ([h]^{-1}, [h], [k]) \\
\text{(R1)}\rightarrow\ & t_1 = ([h]^{-1}, [k], [h], [hk]) \\
\text{(R3)}\rightarrow\ & ([k], [hk]^{-1}, [h]^{-1}, [h], [hk]) \\
\text{(R5)}\rightarrow\ & ([k], [hk]^{-1}, [hk]) \\
\text{(R5)}\rightarrow\ & ([k]) = ([k]^{\delta})
\end{aligned}$$

Cas 2: $\epsilon = 1, \delta = -1$. On a:

$$\begin{aligned}
& s_1 = ([h]^{-1}, [h], [k]^{-1}) \\
\text{(R2)}\rightarrow\ & t_1 = ([h]^{-1}, [k]^{-1}, [h], [hk^2], \ldots, [hk^{2m}], \\
& \qquad [hk^{2m\pm 1}]^{-1}, \ldots, [hk]^{-1}) \\
\text{(R4)}\rightarrow\ & ([k]^{-1}, [hk], \ldots, [hk^{2m\pm 1}], [hk^{2m}]^{-1}, \ldots, [hk^2]^{-1}, [h]^{-1}, \\
& \qquad [h], [hk^2], \ldots, [hk^{2m}], [hk^{2m\pm 1}]^{-1}, \ldots, [hk]^{-1})
\end{aligned}$$

Utilisant une suite d'applications de (R5), on trouve:

$$\ldots \xrightarrow{*} ([k]^{-1}) = ([k]^{\delta})$$

Cas 3: $\epsilon = -1, \delta = 1$. On a:

$$\begin{aligned}
& s_1 = ([h], [h]^{-1}, [k]) \\
\text{(R3)}\rightarrow\ & t_1 = ([h], [k], [hk]^{-1}, [h]^{-1}) \\
\text{(R1)}\rightarrow\ & ([k], [h], [hk], [hk]^{-1}, [h]^{-1}) \\
\text{(R5)}\rightarrow\ & ([k], [h], [h]^{-1}) \\
\text{(R5)}\rightarrow\ & ([k]) = ([k]^{\delta})
\end{aligned}$$

Cas 4: $\epsilon = -1, \delta = -1$. On a:

$$s_1 = ([h], [h]^{-1}, [k]^{-1})$$

$$\begin{aligned}
&\xrightarrow{(R4)} && t_1 = ([h],[k]^{-1},[hk],\ldots,[hk^{2m\pm1}],\\
&&& \quad [hk^{2m}]^{-1},[hk^2]^{-1},[h]^{-1})\\
&\xrightarrow{(R2)} && ([k]^{-1},[h],[hk^2],\ldots,[hk^{2m}],[hk^{2m\pm1}]^{-1},\ldots,[hk]^{-1},\\
&&& \quad [hk],\ldots,[hk^{2m\pm1}],[hk^{2m}]^{-1},\ldots,[hk^2]^{-1},[h]^{-1})
\end{aligned}$$

Utilisant une suite d'applications de (R5), on trouve:

$$\ldots \xrightarrow{*} ([k]^{-1}) = ([k]^{\delta})$$

Concentrons nous maintenant sur $s_2 = ([h]^{\epsilon},[k]^{\delta},[k]^{-\delta})$. Encore une fois, on considère quatre cas selon les valeurs relatives de ϵ et δ.

Cas 1: $\epsilon = 1, \delta = 1$. On a:

$$\begin{aligned}
&&& s_2 = ([h],[k],[k]^{-1})\\
&\xrightarrow{(R1)} && t_2 = ([k],[h],[hk],k^{-1})\\
&\xrightarrow{(R2)} && ([k],[h],[k]^{-1},[hk],[hk^3],\ldots,[hk^{2m\pm1}],\\
&&& \quad [hk^{2m}]^{-1},\ldots,[hk^2]^{-1})\\
&\xrightarrow{(R2)} && ([k],[k]^{-1},[h],[hk^2],\ldots,[hk^{2m}],[hk^{2m\pm1}]^{-1},\ldots,[hk]^{-1},\\
&&& \quad [hk],[hk^3],\ldots,[hk^{2m\pm1}],[hk^{2m}]^{-1},\ldots,[hk^2]^{-1})
\end{aligned}$$

Utilisant une suite d'applications de (R5), on trouve:

$$\begin{aligned}
&\ldots \xrightarrow{*} && ([k],[k]^{-1},[h])\\
&\xrightarrow{(R5)} && ([h]) = ([h]^{\epsilon})
\end{aligned}$$

Cas 2: $\epsilon = 1, \delta = -1$. On a:

$$\begin{aligned}
&&& s_2 = ([h],[k]^{-1},[k])\\
&\xrightarrow{(R2)} && t_2 = ([k]^{-1},[h],[hk^2],\ldots,[hk^{2m}],\\
&&& \quad [hk^{2m\pm1}]^{-1},\ldots,[hk]^{-1},[k])\\
&\xrightarrow{(R3)} && ([k]^{-1},[h],[hk^2],\ldots,[hk^{2m}],\\
&&& \quad [hk^{2m\pm1}]^{-1},\ldots,[k],[hk^2]^{-1},[hk]^{-1})\\
&\xrightarrow{(R3)} && ([k]^{-1},[h],[hk^2],\ldots,[hk^{2m}],\\
&&& \quad [hk^{2m\pm1}]^{-1},\ldots,[k],[hk^4]^{-1},[hk^3]^{-1}[hk^2]^{-1},[hk]^{-1})
\end{aligned}$$

Une suite d'applications de (R3) nous amène à:

$$\begin{aligned}
\ldots \xrightarrow{*} \quad & ([k]^{-1},[h],[hk^2],\ldots,[hk^{2m}],[k]\\
& [hk^{2m+1}]^{-1},[hk^{2m}]^{-1},[hk^{2m-1}]^{-1},\ldots,[hk^3]^{-1},[hk^2]^{-1},[hk]^{-1})
\end{aligned}$$

Le terme $[hk^{2m+1}]^{-1}$ de la suite précédente et le terme $[hk^{2m+1}]$ que fait apparaître la prochaine dérivation pourraient bien être absents. Ils ne seront présents que si $|hk^{2m+1}| \leq N$. Dans le cas où $|hk^{2m+1}| > N$, il faudrait les omettre des formules.

$$\begin{aligned}\xrightarrow{(R1)} \quad & ([k]^{-1},[h],[hk^2],\ldots,[k],[hk^{2m}],[hk^{2m+1}] \\ & [hk^{2m+1}]^{-1},[hk^{2m}]^{-1},[hk^{2m-1}]^{-1},\ldots,[hk^3]^{-1},[hk^2]^{-1},[hk]^{-1})\end{aligned}$$

Une suite d'applications de (R1) nous amène à:

$$\begin{aligned}\ldots \xrightarrow{*} \quad & ([k]^{-1},[k],[h],[hk],[hk^2],[hk^3],\ldots,[hk^{2m}],[hk^{2m+1}] \\ & [hk^{2m+1}]^{-1},[hk^{2m}]^{-1},[hk^{2m-1}]^{-1},\ldots,[hk^3]^{-1},[hk^2]^{-1},[hk]^{-1})\end{aligned}$$

Puis, une suite d'applications de (R5) nous donne:

$$\begin{aligned}\ldots \xrightarrow{*} \quad & ([k]^{-1},[k],[h]) \\ \rightarrow \quad & ([h]) = ([h]^c)\end{aligned}$$

Cas 3: $\epsilon = -1, \delta = 1$. On a:

$$\begin{aligned} & s_2 = ([h]^{-1},[k],[k]^{-1}) \\ \xrightarrow{(R3)} \quad & t_2 = ([k],[hk]^{-1},[h]^{-1},[k]^{-1}) \\ \xrightarrow{(R4)} \quad & ([k],[hk]^{-1},[k]^{-1},[hk],\ldots,[hk^{2m\pm1}], \\ & [hk^{2m}]^{-1},\ldots,[hk^2]^{-1},[h]^{-1}) \\ \xrightarrow{(R4)} \quad & ([k],[k]^{-1},[hk^2],\ldots,[hk^{2m}],[hk^{2m\pm1}]^{-1},\ldots,[hk]^{-1}, \\ & [hk],\ldots,[hk^{2m\pm1}],[hk^{2m}]^{-1},\ldots,[hk^2]^{-1},[h]^{-1}) \\ \xrightarrow{(R5)} \quad & ([hk^2],\ldots,[hk^{2m}],[hk^{2m\pm1}]^{-1},\ldots,[hk]^{-1} \\ & [hk],\ldots,[hk^{2m\pm1}],[hk^{2m}]^{-1},\ldots,[hk^2]^{-1},[h]^{-1})\end{aligned}$$

Utilisant une suite d'applications de (R5), on trouve:

$$\ldots \xrightarrow{*} ([h]^{-1}) = ([h]^c)$$

Cas 4: $\epsilon = -1, \delta = -1$. On a:

$$\begin{aligned} & s_2 = ([h]^{-1},[k]^{-1},[k]) \\ \xrightarrow{(R4)} \quad & t_2 = ([k]^{-1},[hk],\ldots,[hk^{2m\pm1}], \\ & [hk^{2m}]^{-1},\ldots,[hk^2]^{-1},[h]^{-1},[k]) \\ \xrightarrow{(R3)} \quad & ([k]^{-1},[hk],\ldots,[hk^{2m\pm1}], \\ & [hk^{2m}]^{-1},\ldots,[hk^2]^{-1},[k],[hk]^{-1},[h]^{-1})\end{aligned}$$

Une suite d'applications de (R3) nous amène à:

$$\ldots \xrightarrow{*} \quad ([k]^{-1}, [hk], \ldots, [hk^{2m\pm1}], [k], \\ [hk^{2m+1}]^{-1}, [hk^{2m}]^{-1}, \ldots, [hk^2]^{-1}, [hk]^{-1}, [h]^{-1})$$

Encore une fois, le terme $[hk^{2m+1}]^{-1}$ de la suite précédente et le terme $[hk^{2m+1}]$ que fait apparaître la prochaine dérivation pourraient bien être absents. Ils ne seront présents que si $|hk^{2m+1}| \leq N$. Dans le cas où $|hk^{2m+1}| > N$, il faudrait les omettre des formules.

$$\xrightarrow{(R1)} \quad ([k]^{-1}, [hk], \ldots, [k], [hk^{2m+1}], \\ [hk^{2m+1}]^{-1}, [hk^{2m}]^{-1}, \ldots, [hk^2]^{-1}, [hk]^{-1}, [h]^{-1})$$

Une suite d'applications de (R1) nous amène à:

$$\ldots \xrightarrow{*} \quad ([k]^{-1}, [k], [hk], [hk^2], \ldots, [hk^{2m}], [hk^{2m+1}] \\ [hk^{2m+1}]^{-1}, [hk^{2m}]^{-1}, [hk^{2m-1}]^{-1}, \ldots, , [hk^2]^{-1}, [hk]^{-1}, [h]^{-1}) \\ \rightarrow \quad ([hk], [hk^2], \ldots, [hk^{2m}], [hk^{2m+1}], \\ [hk^{2m+1}]^{-1}, [hk^{2m}]^{-1}, [hk^{2m-1}]^{-1}, \ldots, , [hk^2]^{-1}, [hk]^{-1}, [h]^{-1})$$

Puis, une suite d'applications de (R5) nous donne:

$$\ldots \xrightarrow{*} ([h]^{-1}) = ([h]^{\epsilon})$$

◇

Remarque 2.3.2 Comme on le signalait à la fin de la démonstration du Lemme 2.3.1, les montées légales qu'on réécrit ont toutes $[k]$ comme deuxième composante. Cela permet de voir que si s_1 ou s_2 sont des *sous-suites connexes* d'une suite standard s, et que la montée légale $([h]^{\epsilon}, [k]^{\delta})$ de s_1 et s_2 est une montée légale de s, alors les montées sur lesquelles les calculs sont effectués (au Lemme 2.3.1) sont des montées légales de s. ◇

Proposition 2.3.3 *(i) La relation $\rightarrow$ est confluente. Plus précisément, si s, s_1 et s_2 sont des suites standard tels que $s \rightarrow s_1$ et $s \rightarrow s_2$ alors il existe une suite standard t telle que $s_1 \rightarrow t$ et $s_2 \rightarrow t$.*

(ii) La relation $\rightarrow'$ est faiblement confluente. Plus précisément, si s, s_1 et s_2 sont des suites standard tels que $s \rightarrow' s_1$ et $s \rightarrow' s_2$ alors il existe une suite standard t telle que $s_1 \xrightarrow{*}{}' t$ et $s_2 \xrightarrow{*}{}' t$.

Démonstration. (i) On procède comme à la démonstration de la Prop. 1.4.8. Si s_1 et s_2 sont obtenues de s en réécrivant deux montées légales distinctes, alors on est assuré, en vertu du Lemme 1.4.9, que ces montées ne se chevauchent pas. On peut donc effectuer les réécritures de ces deux montées légales dans n'importe quel ordre pour obtenir la même suite t.

(ii) Il nous reste à regarder le cas où l'une des deux suites est obtenues de s en effectuant un effacement, et le cas où les deux suites sont obtenues en effectuant un effacement dans s.

Si on obtient s_1 et s_2 en effaçant deux termes consécutifs de s alors on vérifie aisément l'existence de la suite t. Dans le cas où il y a chevauchement on doit forcément avoir $s_1 = s_2$. Dans le cas où il n'y a pas de chevauchement, les termes consécutifs de s qui ont été effacés pour obtenir s_1 se trouvent dans s_2; les termes consécutifs de s qui ont été effacés pour obtenir s_2 se trouvent dans s_1. On efface ces couples dans s_1 et s_2 et on trouve la même suite t.

Supposons que seulement l'une des deux suites s_1 ou s_2 est obtenue en effectuant un effacement dans s. Dans le cas où la montée légale ne chevauchent pas le couple de termes consécutifs effacés, l'ordre dans lequel sont effectuées ces réécritures ne comptent pas, et elles mènent à la même suite t. Dans le cas où la montée légale et le couple de termes consécutifs effacés se chevauchent, la sous-suite formée de ces trois termes est l'une des sous-suites traitées au Lemme 2.3.1. En vertu de la Rem. 2.3.2, on peut soit effectuer les calculs donnés dans le Lemme 2.3.1, soit effectué l'effacement dans s pour obtenir la même suite t. ◇

On en déduit, par récurrence sur la longueur des dérivations, le corollaire suivant.

Corollaire 2.3.4 *Les relations $\stackrel{*}{\rightarrow}$ et $\stackrel{*}{\rightarrow}'$ sont confluentes.*

Démonstration. On montre que la relation $\stackrel{*}{\rightarrow}$ est confluente par récurrence sur la longueur des dérivations, et en utilisant la confluence de la relation $\rightarrow$ (Prop. 2.3.3 (i)).

En effet, on montre que si s, s_1, s_2 sont des suites standard telles que $s \stackrel{*}{\rightarrow}' s_1$ et $s \stackrel{*}{\rightarrow}' s_2$ alors il existe une suite standard t telle que $s_1 \stackrel{*}{\rightarrow}' t$ et $s_2 \stackrel{*}{\rightarrow}' t$, par récurrence sur le couple $(v(s), |s|)$, en utilisant le Lemme 2.2.7 et la confluence faible de la relation $\rightarrow'$ (Prop. 2.3.3 (ii)). ◇

Donc, partant d'une suite standard $s = ([h_1]^{\epsilon_1}, \ldots, [h_n]^{\epsilon_n})$, il est possible de calculer une suite décroissante $([k_1]^{\delta_1}, \ldots, [k_m]^{\delta_m})$, sur laquelle on ne peut plus effectuer d'effacements et telle que:

$$[h_1]^{\epsilon_1} \ldots [h_n]^{\epsilon_n} \equiv [k_1]^{\delta_1} \ldots [k_m]^{\delta_m} \pmod{F_{N+1}}.$$

En particulier, pour tout $g \in F(A)$, il existe des exposants $n_h(g) \in Z$ tels que:

$$g \equiv \prod_{h \in H(A)} [h]^{n_h(g)} \pmod{F_{N+1}}, \tag{2.11}$$

où le produit se fait selon l'ordre décroissant des commutateurs de Hall. Le membre droit de l'équation (2.11) sera appelé une *décomposition de g en produit décroissant de commutateurs de Hall.*

Remarques 2.3.5 (i) Comme on le signalait plus haut, il est possible de retarder les effacements à la toute fin. En effet, il est possible d'effectuer le calcul en n'utilisant d'abord que les réécritures de Γ, puis de n'effectuer ensuite que des effacements à l'aide de (R5), en vertu du Cor. 2.3.4.

(ii) Les confluences respectives des relations $\xrightarrow{*}$ et $\xrightarrow{*}{}'$ ne nous permettent pas de conclure à l'unicité de la décomposition (2.11) en produit décroissant de commutateurs de Hall, pour les éléments du groupe libre. En effet, le système de réécriture n'est pas inversible comme c'est le cas dans le monoïde libre (Prop. prop:remonte). Cela est dû au fait que les éléments $\gamma(s)$, $\gamma(t)$ associés à deux suites s et t telles que $s \xrightarrow{*} t$ satisfont la congruence $\gamma(s)$ mod $\gamma(t)$, mais ne sont pas nécéssairement égaux. A ce point-ci, nous savons seulement que la suite décroissante de commutateurs de Hall *calculée par le système de réécriture* Γ', à partir d'un élément $g \in F(A)$, est unique.

(iii) Une preuve de l'unicité de la décomposition (2.11), utilisant le système de réécriture, nécessite la possibilité de remonter le long d'une dérivation effectuée sur une suite jusqu'à la suite de départ. Cela est de toute évidence irréalisable si on travaille avec le système Γ', puisqu'on peut alors effacer des termes d'une suite. Le système Γ ne le permet pas non plus puisque les éléments $\gamma(s)$ et $\gamma(s')$ associés à deux suites consécutives d'une même dérivation (i. e. $s \rightarrow s'$) sont seulement congruents mod F_{N+1} (bien que parfois égaux dans le cas des règles (R1) et (R3)).

(iv) Nous allons montrer au paragraphe suivant l'unicité de la décomposition (2.11). La démonstration que nous allons en donner ne repose pas sur les résultats que nous avons jusqu'ici obtenus. Notez que la confluence de la relation $\xrightarrow{*}{}'$ en découle. En effet, soient s, s_1 et s_2 trois suites standard telles que $s \xrightarrow{*}{}' s_1$ et $s \xrightarrow{*}{}' s_2$. Comme Γ' est convergent (Th. 2.2.8), il existe des suites décroissantes (et simplifiées) t_1 et t_2 telles que $s_1 \xrightarrow{*}{}' t_1$, $s_2 \xrightarrow{*}{}' t_2$. On a donc:

$$\gamma(t_1) \equiv \gamma(s_1) \equiv \gamma(s) \equiv \gamma(s_2) \equiv \gamma(t_2).$$

S'il y a unicité de la décomposition (2.11), on conclut à $t_1 = t_2$ et à la confluence de la relation $\xrightarrow{*}{}'$. ◇

Remarque 2.3.6 Le commutateur de deux éléments $g, h \in F(A)$ aurait pu être défini autrement. On aurait pu poser:

$$[g,h] = ghg^{-1}h^{-1} \text{ ou } [g,h] = g^{-1}hgh^{-1}.$$

Les règles de réécriture sont alors différentes, mais analogues à celles que nous avons données. On montre les propriétés des systèmes de réécriture Γ et Γ' de la même façon: invariant de boucle (Prop. 2.2.6), convergence (Th. 2.2.8) et confluence (Prop. 2.3.3 et Cor. 2.3.4). $\diamond$

2.4 Unicité de la décomposition et calcul des exposants de Hall.

On définit un homomorphisme $\mu : F(A) \to K\ll A\gg$ en posant $\mu(a) = 1+a$. Ce polynôme est inversible dans $K\ll A\gg$ et son inverse est égal à:

$$\mu(a^{-1}) = \mu(a)^{-1} = (1+a)^{-1} = 1 - a + a^2 - a^3 + \ldots$$

L'application μ est appelée la *transformée de Magnus* du groupe libre. Par exemple, la transformée de Magnus du mot $w = abb$ est:

$$\mu(abb) = (1+a)(1+b)^2 = 1 + a + 2b + 2ab + bb + abb.$$

La transformée de Magnus du commutateur $[a,b]$, développée jusqu'au degré quatre est:

$$\begin{aligned} \mu([a,b]) &= (1 - a + a^2 - a^3 + \ldots)(1 - b + b^2 - b^3 + \ldots)(1+a)(1+b) \\ &= 1 + ab - ba - aab + aba - bab + bba + \\ &\quad aaab - aaba + abab - abba + bbab - bbba + \ldots \end{aligned} \tag{2.12}$$

L'application μ définit donc un isomorphisme de $F(A)$ dans un groupe (multiplicatif) de séries formelles de terme constant égal à 1. On vérifie que les coefficients de la série $\mu(g)$ sont des entiers, c'est-à-dire $\mu(g) \in Z\ll A\gg$.

Nous énoncons un lemme dû à Magnus [Ma 37] dont nous donnons ici la démonstration. Auparavant, nous introduisons une notation. Soit $T \in K\ll A\gg$ une série formelle non nulle. On définit *l'ordre d'une série* T, et on le note $\omega(T)$, comme étant la longueur du mot le plus court dans le support de T. Plus précisément, on pose $\omega(T) = \inf\{|w| : w \in T\}$. Nous faisons aussi appel, dans la démonstration du lemme, à des notations introduites au paragraphe 1.6 du Chap. 1 et au paragraphe 2.2 de ce chapitre. Rappelons que si t est un arbre du magma libre $M(A)$, alors $\lambda(t)$ est le polynôme de Lie homogène de degré $|t|$ associé à t (voir 1.24).

Lemme 2.4.1 (Magnus [Ma 37])
Soit $g \in F(A), g \neq 1$. Supposons que $g = \kappa(t)$ est l'image par κ d'un arbre t du magma libre $M(A)$. Alors

$$\mu(g) = 1 + \lambda(t) + T,$$

où $T \in K\ll A\gg$ est telle que $T = 0$ si g est une lettre, et $\omega(T) > |t|$, si $|t| \geq 2$.

Le Lemme 2.4.1 est illustré par le calcul effectué en (2.12).

Démonstration. Nous faisons d'abord quelques observations. Soient S et T deux séries formelles. On a:

$$\begin{aligned}
& (1+T)^{-1}(1+S)(1+T) \\
= \quad & \textstyle\sum_{n\geq 0}(-1)^n T^n(1+S+T+ST) \\
= \quad & 1+\textstyle\sum_{n\geq 0}(-1)^n T^n S+\sum_{n\geq 0}(-1)^n T^n ST \\
= \quad & 1+S+\textstyle\sum_{n\geq 1}(-1)^n T^n S+\sum_{n\geq 0}(-1)^n T^n ST \\
= \quad & 1+S+\textstyle\sum_{n\geq 0}(-1)^n T^n(ST-TS).
\end{aligned}$$

De sorte que:

$$\begin{aligned}
& (1+S)^{-1}(1+T)^{-1}(1+S)(1+T) \\
= \quad & (\textstyle\sum_{m\geq 0}(-1)^m S^m)(1+S+\sum_{n\geq 0}(-1)^n T^n(ST-TS) \\
= \quad & 1+\textstyle\sum_{m,n\geq 0}(-1)^n S^m T^n(ST-TS) \qquad (2.13)
\end{aligned}$$

On montre le lemme par récurrence sur le degré de l'arbre t. Dans le cas où t est une lettre, le résultat est évident, puisqu'alors $g = a \in A$ et $\mu(g) = 1 + a$.

Supposons donc que $g = \kappa(t)$ où t est un arbre de degré au moins deux. Il existe alors des arbres t_1 et t_2 (les sous-arbres gauche et droit de t) tels que $g = \kappa(t) = [\kappa(t_1), \kappa(t_2)]$. Posons $g_i = \kappa(t_i)$ $(i = 1, 2)$. On a alors, par récurrence:

$$\mu(g_i) = 1 + \lambda_i + T_i,$$

où $\lambda_i = \lambda(t_i)$ et T_i est une série formelle qui soit est nulle, soit satisfait $\omega(T_i) > |t_i|$ $(i = 1, 2)$. On a:

$$\begin{aligned}
\mu(g) &= \mu(g_1)^{-1}\mu(g_2)^{-1}\mu(g_1)\mu(g_2) \\
&= (1+\lambda_1+T_1)^{-1}(1+\lambda_2+T_2)^{-1}(1+\lambda_1+T_1)(1+\lambda_2+T_2),
\end{aligned}$$

et selon (2.13), le membre droit de la dernière égalité est égal à:

$$1 + \sum_{m,n\geq 0}(-1)^n S^m T^n(ST - TS)$$

où $S = \lambda_1 + T_1$ et $T = \lambda_2 + T_2$. On a $\omega(S) = |t_1|$ et $\omega(T) = |t_2|$. Donc, pour m, n tels que $m + n \geq 1$, la série $S^m T^n (ST - TS)$ est d'ordre au moins $|t| + 1$; pour $m = n = 0$, on calcule:

$$\begin{aligned} & ST - TS \\ = \quad & (\lambda_1 + T_1)(\lambda_2 + T_2) - (\lambda_2 + T_2)(\lambda_1 + T_1) \\ = \quad & (\lambda_1\lambda_2 - \lambda_2\lambda_1) + (\lambda_1 T_2 + T_1\lambda_2 + T_1 T_2 - T_2\lambda_1 - \lambda_2 T_1 - T_2 T_2) \\ = \quad & \lambda(t) + (\lambda_1 T_2 + T_1\lambda_2 + T_1 T_2 - T_2\lambda_1 - \lambda_2 T_1 - T_2 T_2). \end{aligned}$$

Finalement, on vérifie que la série $(\lambda_1 T_2 + T_1\lambda_2 + T_1 T_2 - T_2\lambda_1 - \lambda_2 T_1 - T_2 T_2)$ est d'ordre au moins $|t| + 1$. De sorte que le lemme est montré. ◇

On en déduit facilement le corollaire suivant.

Corollaire 2.4.2 *Si deux éléments du groupe libre sont congruents modulo F_{n+1}, alors leurs transformées de Magnus coïncident jusqu'au degré n.* ◇

Soit $w \in A^*$ un mot, $w = a_1 \dots a_n$. Un *sous-mot* de w est un mot $u = b_1 \dots b_p$ tel qu'il existe une factorisation de w de la forme:

$$w = v_0 b_1 v_1 \dots b_p v_p, \text{ avec } v_i \in A^*. \tag{2.14}$$

Par exemple, $u = abb$ est un sous-mot de $w = ababab$, et ce de quatre façons.

Remarque 2.4.3 Soit $E \subset \{1, \dots, n\}, E = \{i_1, \dots, i_p\}$, avec $i_1 < \dots < i_p$. Alors on désignera par $u = w(E)$ le sous-mot de w, $u = a_{i_1} \dots a_{i_p}$. Cette notation nous sera utile au paragraphe 2.5. ◇

Soit $u \in A^*$; on définit la *fonction sous-mot* $\binom{-}{u} : A^* \to Z$

$$w \mapsto \binom{w}{u}$$

en définissant $\binom{w}{u}$ comme étant le nombre de factorisations (2.14), c'est-à-dire le nombre de sous-ensembles $E \subset \{1, \dots, n\}$ tels que $w(E) = u$. Par exemple, on a $\binom{ababab}{abb} = 4$. La transformée de Magnus est liée aux fonctions sous-mot. En effet, pour tout mot $w = a_1 a_2 \dots a_n \in A^*$, on a:

$$\mu(w) = (1 + a_1)(1 + a_2) \dots (1 + a_n) = \sum_{u \in A^*} \binom{w}{u} u$$

(voir [Lo 82] pour cette identité et plusieurs autres). On étend les fonctions sous-mot au groupe libre tout entier en posant, pour tout $g \in F(A)$,

$$\mu(g) = \sum_{u \in A^*} \binom{g}{u} u.$$

Par exemple, selon les calculs effectués plus haut en (2.12), on a:

$$\binom{a^{-1}b^{-1}ab}{ab} = 1 \text{ et } \binom{a^{-1}b^{-1}ab}{ba} = -1.$$

Maintenant, soit $g \in F(A)$ et

$$\prod_{h \in H(A)} [h]^{n_h(g)} \tag{2.15}$$

une décomposition de g en produit décroissant de commutateurs de Hall.

Donc, en vertu de la Rem. 2.2.1, de la décomposition (2.15) on obtient:

$$g \equiv \prod_{h \in H(A)} [h]^{n_h} \pmod{F_2},$$

c'est-à-dire:

$$g \equiv \prod_{h \in A} [h]^{n_h} \pmod{F_2}, \tag{2.16}$$

où le produit se fait selon l'ordre décroissant des lettres et où on a posé $n_h = n_h(g)$ pour alléger les notations. Le mot (2.16) est réduit et décroissant. Selon la Rem. 2.2.3, cette expression est unique mod F_2. Par conséquent, les exposants $n_h(g)$ sont uniques pour les $h \in H(A), |h| = 1$. De plus, on vérifie en calculant $\mu(g)$ que l'exposant de la lettre a dans (2.16) est égal au coefficient de a dans $\mu(g)$, qui est aussi égal à l'exposant de a dans g (i.e. $\sum \chi(a_i = a)\epsilon_i$, si $g = a_1^{\epsilon_1} \ldots, a_n^{\epsilon_n}$). C'est-à-dire que nous avons:

$$n_a(g) = \binom{g}{a}, \text{ pour tout } a \in A, g \in F(A).$$

Nous allons montrer que les exposants $n_h(g)$ sont uniques, et sont obtenus comme somme de produits de fonctions sous-mot évaluées en g.

Fixons $g \in F(A)$ et posons, comme plus haut, $n_h = n_h(g)$. Supposons que l'unicité soit montrée pour les commutateurs $h \in H(A)$, de degré $|h| < |h_0|$, et que n_h est égal à une somme de produits de fonctions sous-mot (évaluées en g). Posons $N = |h_0|$, de sorte que seuls les commutateurs de degré plus petit que h_0 ou de même degré que h_0 apparaîssent dans la décomposition (2.15). Rappelons encore une fois que le polynôme de Lie associé à un mot de Hall $h \in H(A)$ est noté $\lambda(h)$ (voir 1.24).

On a:

$$\begin{aligned} \mu\Big(\prod_{h \in H(A)} [h]^{n_h}\Big) &= \prod_{h \in H(A)} \mu([h])^{n_h} \\ &= \prod_{h \in H(A)} (1 + \lambda(h) + T_h)^{n_h} \end{aligned}$$

$$= \prod_{h\in H(A)} \left(1 + \sum_{i\geq 1} \binom{n_h}{i} (\lambda(h) + T_h)^i\right)$$

$$= \prod_{h\in H(A)} \left(1 + \sum_{i\geq 1} \binom{n_h}{i} \sum_{W\in\{\lambda(h),T_h\}^i} W\right)$$

$$= \sum_{\substack{i_1,\ldots,i_k\geq 1 \\ h_1,\ldots,h_k\in H(A) \\ W_j\in\{\lambda(h_j),T_{h_j}\}^*,|W_j|=i_j}} \binom{n_{h_1}}{i_1}\ldots\binom{n_{h_k}}{i_k} W_1\ldots W_k$$

Chacun des produits se fait selon l'ordre décroissant des mots de Hall. Il faut expliquer les notations utilisées aux deux dernières lignes. Le calcul du produit $(\lambda(h)+T_h)^i$ se fait en choisissant le terme $\lambda(h)$ ou le terme T_h de chacun des i facteurs $(\lambda(h)+T_h)$. Chacun de ces produits est codé par un mot W à deux lettres ($\lambda(h)$ et T_h), de longueur i, c'est-à-dire $W \in \{\lambda(h), T_h\}^i$. Lorsque toutes les longueurs sont permises, $W \in \{\lambda(h), T_h\}^*$.

Soit $P \in K\langle A\rangle$, homogène de degré $N = |h_0|$, tel que $(\lambda(h), P) = 0$ si $h \neq h_0$ et $(\lambda(h_0), P) = 1$. Un tel polynôme existe puisqu'en vertu du Th. 1.6.7 et du Cor. 1.6.9, la matrice de passage de la base canonique à la base PBWH est inversible.

Remarquez que $(T, P) = 0$ si les mots dans le support de T sont de longueur $\geq N+1$, puisque P est homogène de degré N. La transformée de Magnus de g et la somme de droite de la dernière égalité coïncident jusqu'au degré N. On a donc:

$$\begin{aligned}(\mu(g), P) &= \sum_{\substack{i_j=1 \\ h_j\in H(A) \\ |h_j|=N, W_j=\lambda(h_j)}} n_{h_j}(W_j, P) \\ &\quad + \sum_{\substack{i_1,\ldots,i_k\geq 1 \\ k\geq 1, h_j\in H(A), |h_j|<N \\ W_j\in\{\lambda(h_j),T_{h_j}\}^*,|W_j|=i_j}} \binom{n_{h_1}}{i_1}\ldots\binom{n_{h_k}}{i_k}(W_1\ldots W_k, P) \\ &= n_{h_0} + \sum_{\substack{i_1,\ldots,i_k\geq 1 \\ k\geq 1, h_j\in H(A), |h_j|<N \\ W_j\in\{\lambda(h_j),T_{h_j}\}^*,|W_j|=i_j}} \binom{n_{h_1}}{i_1}\ldots\binom{n_{h_k}}{i_k}(W_1\ldots W_k, P)\end{aligned}$$

D'où:

$$n_{h_0} = (\mu(g), P) - \sum_{\substack{i_1,\ldots,i_k\geq 1 \\ k\geq 1, h_j\in H(A), |h_j|<N \\ W_j\in\{\lambda(h_j),T_{h_j}\}^*,|W_j|=i_j}} \binom{n_{h_1}}{i_1}\ldots\binom{n_{h_k}}{i_k}(W_1\ldots W_k, P) \tag{2.17}$$

Selon l'hypothèse de récurrence, les exposants n_h qui apparaîssent dans la somme de droite sont uniquement déterminés et sont égaux à une somme de produits de fonctions sous-mot. Le coefficient $(\mu(g), P)$ est lui-même égal à une somme de fonctions sous-mot:

$$(\mu(g), P) = \sum_{u \in A^*} (P, u) \binom{g}{u}.$$

Par conséquent, l'exposant n_{h_0} est unique et s'exprime comme une somme de produits de fonctions sous-mot (évaluées en g).

Les résultats de ce paragraphe jumelés à ceux des paragraphes précédents nous donnent le théorème suivant. L'existence de la décomposition en produit décroissant de commutateurs de Hall est assuré par les systèmes de réécriture. L'unicité de cette décomposition vient d'être montrée à l'aide du calcul de la transformée de Magnus.

Théorème 2.4.4 *Soit $g \in F(A)$. Il existe des exposants uniques $n_h(g) \in Z$, tels que:*

$$g \equiv \prod_{h \in H(A)} [h]^{n_h(g)} \pmod{F_{N+1}}.$$

De plus, cette décomposition de g peut être calculée à l'aide du système de réécriture Γ'. ◇

Corollaire 2.4.5 ([Ma 37, Wi 37, HM 50a, CFL 58])
L'ensemble des commutateurs de Hall de poids N forment une base du groupe quotient F_N/F_{N+1}.

Démonstration. Soient $g \in F_N$ et

$$g \equiv \prod_{h \in H(A), |h| \leq N} [h]^{n_h} \pmod{F_{N+1}} \tag{2.18}$$

sa décomposition en produit décroissant de commutateurs de Hall mod F_{N+1}. En vertu de la Rem. 2.2.1, la décomposition de g mod F_N est obtenue de (2.18):

$$g \equiv \prod_{h \in H(A), |h| \leq N-1} [h]^{n_h} \pmod{F_N}.$$

D'autre part, comme $g \in F_N$, on a $g \equiv 1 \bmod F_N$. De sorte que, selon le Th. 2.4.4, $n_h = 0$ pour $|h| < N$ et il n'apparaît dans (2.18) que des commutateurs de poids N. On a donc montré que les commutateurs de Hall de poids N engendrent F_N/F_{N+1}. On déduit facilement du Th. 2.4.4 que ces commutateurs sont libres. ◇

Il est intéressant de noter que M. Hall montre d'abord le Cor. 2.4.5 à l'aide du Lemme 2.4.1. Il utilise ensuite ce résultat pour en déduire l'unicité de la décomposition en produit décroissant de commutateurs de Hall. Le fait que ses bases sont ordonnées selon le degré des commutateurs lui est nécessaire en cours de démonstration (voir par exemple [HM 59, Th. 11. 2. 4]).

Désignons par $\mathcal{L}_n(A)$ le sous-module (sur Z) de $\mathcal{L}(A)$ formé des polynômes de Lie homogènes de degré n.

Corollaire 2.4.6 (Magnus [Ma 37])
Les Z-modules F_N/F_{N+1} et $\mathcal{L}_N(A)$ sont isomorphes.

Démonstration. Le Cor. 1.6.10 montre que les polynômes de Lie $\lambda(h)$ ($h \in H(A)$, $|h| = N$), forment une base du sous-Z-module $\mathcal{L}_N(A)$. Selon le Cor. 2.4.5 qui précède, les commutateurs $\kappa(h)$ forment une base du Z-module F_N/F_{N+1}. Ces Z-modules sont donc isomorphes. ◇

2.5 Les identités de Thérien.

Thérien [Th 83] a montré (pour les bases de Hall classiques) que lorsque g est un mot positif de $F(A)$, $g = w \in A^*$, l'exposant $n_h(w)$ est une *combinaison linéaire à coefficients dans N* de fonctions sous-mot:

$$n_h(w) = \sum_{u \in A^*} k_{h,u} \binom{w}{u}.$$

Nous allons reprendre, dans ce paragraphe, le résultat de Thérien. Nous montrerons, au paragraphe suivant, que les identités qu'il a mises à jour sont aussi vérifiées pour tous les éléments du groupe libre.

Soit $w \in A^*, w = a_1 \dots a_n$. Désignons par $s(w)$ la suite standard formée des lettres de w:

$$s = s(w) = (a_1, \dots, a_n)$$

et soit $s = s_0 \rightarrow \dots \rightarrow s_p = t$ une dérivation de s à une suite décroissante de commutateurs de Hall $t = ([h_1], \dots, [h_n])$. Comme la suite s est la suite des lettres d'un mot positif, nous n'utiliserons que la réécriture (R1) et il n'y aura aucun effacement. La suite décroissante t sera constituée de commutateurs de Hall tous affectés d'un exposant positif. En vertu du Th. 2.4.4, la suite t est unique; nous la désignerons par $\mathcal{T}(w)$.

Suivant Thérien, nous allons associer à chacun des termes de chacune des suites s_i, un ensemble sur $\{1, \dots, n\}$. Au terme a_i de la suite $s_0 = s(w)$ on associe l'ensemble $\mathcal{E}(a_i) = \{i\}$. Maintenant, supposons que tous les termes de la suite s_j ont un ensemble

associé. Un terme $[r]$ de la suite s_{j+1} est peut-être un terme de la suite s_j et alors il garde le même ensemble associé. Sinon il est obtenu par réécriture d'une montée légale $([h],[k])$ de s_j et est égal à $r=[hk]$; dans ce cas on pose $\mathcal{E}([r])=\mathcal{E}([h])\cup\mathcal{E}([k])$.

Exemple 2.5.1 On réécrit le mot positif $w=abab$. On choisit un ensemble de Hall dont les mots de degré au plus cinq sont ceux de l'Ex. 1.2.1. On pose $N=3$. A chaque fois, on réécrit l'inversion la plus à droite de la suite. Sous chacune des lettres d'un commutateur de Hall d'une suite se trouve l'indice de cette lettre dans le mot initial.

				a	b	a	b		
				1	2	3	4		
$\rightarrow$				a	b	b	a	$[ab]$	
				1	2	4	3	34	
$\rightarrow$			b	a	$[ab]$	b	a	$[ab]$	
			2	1	12	4	3	34	
$\rightarrow$		b	a	b	$[ab]$	$[abb]$	a	$[ab]$	
		2	1	4	12	124	3	34	
$\rightarrow$		b	a	b	$[ab]$	a	$[abb]$	$[ab]$	
		2	1	4	12	3	124	34	
$\rightarrow$	b	a	b	a	$[ab]$	$[aba]$	$[abb]$	$[ab]$	
	2	1	4	3	12	123	124	34	
$\rightarrow$	b	a	b	a	$[ab]$	$[abb]$	$[aba]$	$[ab]$	
	2	1	4	3	12	124	123	34	
$\rightarrow$	b	a	b	a	$[ab]$	$[abb]$	$[ab]$	$[aba]$	
	2	1	4	3	12	124	34	123	
$\rightarrow$	b	a	b	a	$[abb]$	$[ab]$	$[ab]$	$[aba]$	
	2	1	4	3	124	12	34	123	
$\rightarrow$	b	b	a	$[ab]$	a	$[abb]$	$[ab]$	$[ab]$	$[aba]$
	2	4	1	14	3	124	12	34	123
$\rightarrow$	b	b	a	a	$[ab]$	$[aba]$	$[abb]$	$[ab]$	$[ab]$	$[aba]$
	2	4	1	3	14	143	124	12	34	123

Les réécritures qui suivent ne font apparaître aucun nouveau terme. Elles réordonnent les termes de la dernière suite. Nous les omettons.

$\stackrel{*}{\rightarrow}$	b	b	a	a	$[abb]$	$[ab]$	$[ab]$	$[ab]$	$[aba]$	$[aba]$
	2	4	1	3	124	14	12	34	143	123

$\diamond$

Soit $s(w) = s_0 \to \ldots \to s_p = \mathcal{T}(w)$ une dérivation qui mène de w à l'unique suite décroissante $\mathcal{T}(w)$. Si $E \subset \{1,\ldots,n\}$ alors on définit la suite standard $s_j|_E$ comme étant la sous-suite de s_j formée des termes $[r]$ de s_j tels que $\mathcal{E}([r]) \subset E$.

Exemple 2.5.2 Posons $E = \{1,3,4\}$. Comme on le verra au Lemme 2.5.3, si on prend les restrictions $s_j|_E$ de chacune des suites de la dérivation de l'exemple précédent, on obtient une dérivation qui va de (a,a,b) à la suite décroissante $\mathcal{T}(abab)\big|_{\{1,3,4\}}$.

$$
\begin{array}{cccccccc}
 & & & a & a & b & & \\
 & & & 1 & 3 & 4 & & \\
\to & & a & b & a & [ab] & & \\
 & & 1 & 4 & 3 & 34 & & \\
\to & b & a & [ab] & a & [ab] & & \\
 & 4 & 1 & 14 & 3 & 34 & & \\
\to & b & a & a & [ab] & [aba] & [ab] & \\
 & 4 & 1 & 3 & 14 & 143 & 34 & \\
\to & b & a & a & [ab] & [ab] & [aba] & \\
 & 4 & 1 & 3 & 14 & 34 & 143 &
\end{array}
$$

◇

Lemme 2.5.3 (Thérien [Th 83])
Soit $w \in A^*, w = a_1 \ldots a_n$, et $E \subset \{1,\ldots,n\}$. Alors:

$$\mathcal{T}(w(E)) = \mathcal{T}(w)|_E.$$

Démonstration. Soit $s(w) = s_0 \to \ldots \to s_p = \mathcal{T}(w)$ une dérivation qui va de w à la suite décroissante $\mathcal{T}(w)$ qui donne sa décomposition en produit décroissant de commutateurs de Hall. Posons $\bar{s}_j = s_j|_E$, pour tout $j = 0,1,\ldots,p$. On a $\bar{s}_0 = s_0|_E = s(w(E)) = s(u)$ (où $u = w(E)$ a été défini à la Rem. 2.4.3). On procède par récurrence sur $j \geq 0$ pour montrer que soit $\bar{s}_{j+1} = \bar{s}_j$, soit $\bar{s}_{j+1}$ se dérive de $\bar{s}_j$ à l'aide de Γ : $\bar{s}_j \to \bar{s}_{j+1}$.

Supposons qu'on ait $\bar{s}_j = s_j|_E$. Soit $([h],[k])$ la montée légale dans s_j qui est réécrite lors de la dérivation $s_j \to s_{j+1}$. On a:

$$\begin{aligned} s_j &= (\ldots,[h],[k],\ldots), \\ s_{j+1} &= (\ldots,[k],[h],[hk],\ldots). \end{aligned}$$

Si $\mathcal{E}([h]) \not\subset E$ ou si $\mathcal{E}([k]) \not\subset E$ alors $\mathcal{E}([hk]) = \mathcal{E}([h]) \cup \mathcal{E}([k]) \not\subset E$ et on a

$$\bar{s}_j = s_j|_E = s_{j+1}|_E = \bar{s}_{j+1}.$$

Sinon, c'est que $\mathcal{E}([h]) \subset E$ et $\mathcal{E}([k]) \subset E$. Donc, $[h]$ et $[k]$ sont des termes de la suite $\bar{s}_j$ et on a $\mathcal{E}([hk]) = \mathcal{E}([h]) \cup \mathcal{E}([k]) \subset E$. Or, la montée $([h],[k])$ est légale dans $\bar{s}_j$, en vertu de la Rem. 1.4.1, de sorte que $\bar{s}_{j+1}$ se dérive bien de $\bar{s}_j$, à l'aide de Γ.

En ne conservant que les suites $\bar{s}_j$ distinctes et en réindiçant ces suites, on obtient une dérivation $s(u) = \bar{s}_0 \xrightarrow{*} \bar{s}_q = \mathcal{T}(w)|_E$. Observez que comme s_p est décroissante il en est de même de toute sous-suite de s_p. Ainsi, $\bar{s}_q = \mathcal{T}(w)|_E$ est décroissante. Or, en vertu du Th. 2.4.4, la suite décroissante que l'on peut dériver de $s(u)$ est unique. On doit donc avoir $\mathcal{T}(w(E)) = \mathcal{T}(w)|_E$. ◇

Remarque 2.5.4 Quelle que soit la dérivation $s(w) \xrightarrow{*} \mathcal{T}(w)$, les sous-ensembles associés aux termes de la suite $\mathcal{T}(w)$ sont toujours les mêmes. On le montre en faisant un raisonnement analogue à celui fait à la démonstration du Cor. 2.3.4. ◇

Maintenant, soit $w = a_1 \dots a_n$ et $E \subset \{1, \dots, n\}$. Désignons par $k_{h,E}$ le nombre de commutateurs de Hall $[h]$ dans $\mathcal{T}(w)$ tels que $\mathcal{E}([h]) = E$. Si $E, F \subset \{1, \dots, n\}$ donnent lieu au même sous-mot $w(E) = u = w(F)$ alors, en vertu du Lemme 2.5.3, on a $k_{h,E} = k_{h,F}$. On dénotera cette valeur commune par $k_{h,u}$.

Remarque 2.5.5 Notez que $k_{h,u}$ est égal au nombre de commutateurs de Hall $[h]$ dans la décompsition de u, tels que $\mathcal{E}([h]) = \{1, \dots, |u|\}$. Par conséquent, on a $k_{h,u} \neq 0$ seulement si $|u| \leq |h|$. ◇

A chaque commutateur $[h]$ de la suite $\mathcal{T}(w)$ est associé un sous-ensemble $E \subset \{1, \dots, n\}$. L'exposant $n_h(w)$ dans la décomposition en produit décroissant de commutateurs de Hall de w est égal au nombre de commutateurs $[h]$ dans la suite $\mathcal{T}(w)$. On a donc l'identité de Thérien:

$$\begin{aligned} n_h(w) &= \sum_{\substack{E \subset \{1,\dots,n\} \\ w(E)=u}} k_{h,E} \\ &= \sum_{E \subset \{1,\dots,n\}} \sum_{u \in A^*} k_{h,u} \\ &= \sum_{u \in A^*, |u| \leq |h|} k_{h,u} \binom{w}{u}. \end{aligned} \tag{2.19}$$

2.6 Généralisation des identités de Thérien.

Nous allons maintenant montrer que l'identité de Thérien (2.19) est valide pour tous les éléments du groupe libre. Nous en donnerons deux démonstrations aux paragraphes 2.6.1 et 2.6.2.

Théorème 2.6.1 *Soit $g \in F(A)$ et $h_0 \in H(A)$. L'exposant du commutateur de Hall h_0 dans la décomposition de g en produit décroissant de commutateurs de Hall est donné par:*

$$n_{h_0}(g) = \sum_{u \in A^*, |u| \leq |h_0|} k_{h_0,u} \binom{g}{u}. \tag{2.20}$$

où les coefficients $k_{h_0,u}$ ont été définis au paragraphe 2.5.

Le Th. 2.6.1 nous permet de donner de nouvelles démonstrations des résultats de Magnus et P. Hall.

Corollaire 2.6.2 (Magnus [Ma 37], Witt [Wi 37])
Un élément $g \in F(A)$ est dans F_{N+1} si et seulement si pour tout mot non vide $u \in A^*$, $|u| \leq N$ implique $(\mu(g), u) = 0$

Démonstration. Montrons d'abord que la condition est suffisante. Supposons que pour tout $u \in A^*$ non vide, $|u| \leq N$, on ait $\binom{g}{u} = 0$. Soit

$$g \equiv \prod_{h \in H(A)} h^{n_h(g)} \pmod{F_{N+1}}.$$

la décomposition de g en produit décroissant de commutateurs de Hall. Tous les commutateurs dans cette décomposition sont de poids au plus N. Or, en vertu de (2.20) et des hypothèses faites sur g, l'exposant $n_h(g)$ dans la décomposition de g est égal à:

$$\begin{aligned} n_h(g) &= \sum_{u \in A^*, |u| \leq |h|} k_{h,u} \binom{g}{u} \\ &= \sum_{u \in A^*, |u| \leq N} k_{h,u} \binom{g}{u} \\ &= 0. \end{aligned}$$

Par conséquent, on a $g \equiv 1 \bmod F_{N+1}$. De sorte que $g \in F_{N+1}$.

Supposons maintenant que $g \in F_{N+1}$; on a donc $g \equiv 1 \bmod F_{N+1}$. En vertu du Cor. 2.4.6, les transformées de Magnus de g et de 1 coïncident jusqu'au degré N. Par conséquent, comme $\mu(1) = 1$, $(\mu(g), u) = 0$ pour tout mot non vide $u \in A^*$ de longueur au plus N. ◇

Remarque 2.6.3 La démonstration de la nécessité de la condition du Cor. 2.6.2 n'est pas nouvelle. Elle repose sur les Lemme 2.4.1 et Cor. 2.4.2, dûs à Magnus [Ma 37]. ◇

Le prochain résultat (Cor. 2.6.4) a d'abord été montré par P. Hall [HP 33], pour le cas $g = ab$. C'est à cette fin qu'il développait le 'collecting process', qui permettait de *réécrire* $(ab)^x$ (x entier) en produit de commutateurs sur $\{a, b\}$. Magnus [Ma 37] et M. Hall [HM 59] ont repris son résultat, et l'ont montré pour tout mot positif (i.e. $g \in A^*$) et $x = p^r$, $p \in N$ premier. Nous allons un peu plus loin en le montrant pour tout $g \in F(A)$ et pour toute valeur entière de x.

Corollaire 2.6.4 (P. Hall [HP 33])
Soit $g \in F(A)$ et x une indéterminée. Pour chaque $h \in H(A)$, il existe un polynôme en x, de degré au plus $|h|$, qui donne l'exposant $n_h(g^x)$ pour les valeurs entières de x.

Démonstration. Nous allons montrer que l'exposant $n_h(g^x)$ est un polynôme de la forme:

$$\alpha_1(g)\binom{x}{1} + \ldots + \alpha_q(g)\binom{x}{q}$$

où $q = |h|$ et les coefficients $\alpha_i(g)$ sont entiers. Cela montrera en effet que $n_h(g^x)$ est un polynôme en x de degré au plus $|h|$. On a, selon (2.20):

$$n_h(g^x) = \sum_{u \in A^*, |u| \leq |h|} k_{h,u}\binom{g^x}{u}.$$

Posons $\mu(g) = 1 + T_g$. Le calcul de la transformée de Magnus de g^x donne:

$$\begin{aligned} \mu(g^x) &= (\mu(g))^x \\ &= (1 + T_g)^x \\ &= \sum_{p \geq 0} \binom{x}{p} T_g{}^p. \end{aligned}$$

Par conséquent, on a:

$$n_h(g^x) = \sum_{p=0}^{|h|} \left(\sum_{u \in A^*, |u| \leq |h|} k_{h,u}(T_g{}^p, u) \right) \binom{x}{p}.$$

◇

2.6.1 Fonctions représentatives de $F(A)$.

Nous considérons l'ensemble de toutes les fonctions $\vartheta : F(A) \to K$. L'ensemble de ces fonctions forme une K-algèbre. En effet, si $\vartheta, \theta : F(A) \to K$ sont deux fonctions de cet ensemble on pose:

$$\begin{aligned} (\alpha\vartheta)(g) &= \alpha(\vartheta(g)), \text{ pour tout } \alpha \in K, \\ (\vartheta + \theta)(g) &= \vartheta(g) + \theta(g), \\ (\vartheta \cdot \theta)(g) &= \vartheta(g)\theta(g). \end{aligned}$$

Dans cette algèbre on peut distinguer la sous-algèbre engendrée par les fonctions sous-mot. Ainsi, on a montré au paragraphe 2.4 que pour $h \in H(A)$ fixé, la fonction $n_h(-) : F(A) \to K$ est dans l'algèbre des fonctions sous-mot (Eq. (2.17)).

Une fonction $\vartheta : F(A) \to K$ est une *fonction représentative* s'il existe un K-espace vectoriel de dimension finie E_ϑ et:

(i) une action (linéaire) à droite de $F(A)$ sur E_ϑ,

$$\begin{aligned} E_\vartheta \times F(A) &\to E_\vartheta \\ (x, g) &\mapsto x.g \end{aligned}$$

(ii) un vecteur $x_\vartheta \in E_\vartheta$ et une fonctionelle linéaire f_ϑ sur E_ϑ tels que pour tout $g \in F(A)$:

$$\vartheta(g) = f_\vartheta(x_\vartheta.g).$$

Le prochain lemme est tiré de [Reu]. L'extension des identités de Thérien au groupe libre en découle directement.

Lemme 2.6.5 *(i) L'ensemble des fonctions représentatives forme une sous-algèbre de la K-algèbre des fonctions sur $F(A)$,*

(ii) Si une fonction représentative s'annule sur A^* alors elle s'annule sur $F(A)$ tout entier,

(iii) Toute fonction sous-mot est représentative.

Démonstration. (i) Soient ϑ et θ deux fonctions représentatives et $\alpha \in K$.

On a $(\alpha\vartheta)(g) = \alpha(\vartheta(g)) = \alpha(f_\vartheta(x_\vartheta.g)) = (\alpha f_\vartheta)(x_\vartheta.g)$. On peut donc laisser intact l'espace vectoriel, l'action de $F(A)$ sur celui-ci et le vecteur qu'on y a choisi. Il suffit de changer la fonctionelle en posant $f_{\alpha\vartheta} = \alpha f_\vartheta$, pour constater que la fonction $(\alpha\vartheta)$ est représentative.

Posons $E = E_\vartheta \oplus E_\theta$. On définit l'action à droite de $F(A)$ sur E, et la fonctionelle linéaire $f : E \to K$ en posant, pour tout $x_1 \in E_\vartheta, x_2 \in E_\theta$:

$$(x_1 + x_2).g = x_1.g + x_2.g,$$

$$f(x_1 + x_2) = f_\vartheta(x_1) + f_\theta(x_2).$$

Alors, si on pose $x = x_\vartheta + x_\theta$, pour tout $g \in F(A)$ on a:

$$\begin{aligned} f(x.g) &= f((x_\vartheta + x_\theta).g) \\ &= f(x_\vartheta.g + x_\theta.g) \\ &= f_\vartheta(x_\vartheta.g) + f_\theta(x_\theta.g) \\ &= \vartheta(g) + \theta(g) = (\vartheta + \theta)(g). \end{aligned}$$

La fonction $(\vartheta + \theta)$ est donc représentative.

Posons $E = E_\vartheta \otimes E_\theta$. On définit l'action à droite de $F(A)$ sur E, et la fonctionelle linéaire $f : E \to K$ en posant, pour tout $x_1 \in E_\vartheta, x_2 \in E_\theta$:

$$(x_1 \otimes x_2).g = x_1.g \otimes x_2.g,$$

$$f(x_1 \otimes x_2) = f_\vartheta(x_1) f_\theta(x_2).$$

Alors, si on pose $x = x_\vartheta \otimes x_\theta$, pour tout $g \in F(A)$ on a:

$$\begin{aligned} f(x.g) &= f((x_\vartheta \otimes x_\theta).g) \\ &= f(x_\vartheta.g \otimes x_\theta.g) \\ &= f_\vartheta(x_\vartheta.g) f_\theta(x_\theta.g) \\ &= \vartheta(g)\theta(g) = (\vartheta \cdot \theta)(g). \end{aligned}$$

La fonction $(\vartheta \cdot \theta)$ est donc représentative. Par conséquent, les fonctions représentatives forment bien une sous-algèbre de la K-algèbre des fonctions sur $F(A)$.

(ii) Soit ϑ une fonction représentative qui s'annule sur A^*.

Tout élément $g \in F(A)$ peut s'écrire $g = u_0 v_1^{-1} u_1 \dots v_k^{-1} u_k$, avec $k \geq 0, u_i, v_j \in A^*$. Nous allons montrer que $\vartheta(g) = 0$ par récurrence sur k. Si $k = 0$ alors l'égalité est vérifiée par hypothèse.

La multiplication à droite par v_1^{-1} : $x \mapsto x.v_1^{-1}$ est un endomorphisme de E_ϑ. Selon le théorème de Cayley-Hamilton il existe un polynôme (commutatif) à coefficients rationnels qui annule cet endomorphisme sur tout l'espace. On a donc:

$$x.v_1^{-n} = r_1 x.v_1^{-n+1} + r_2 x.v_1^{-n+2} + \dots + r_n x,$$

pour tout vecteur $x \in E_\vartheta$, où les r_i sont des nombres rationnels et où $n \geq 1$ est égal à la dimension de E_ϑ. En prenant $x = x_\vartheta.u_0 v_1^{n-1}$ cette relation nous donne:

$$x_\vartheta.u_0 v_1^{-1} = r_1 x_\vartheta.u_0 + r_2 x_\vartheta.u_0 v_1 + \dots + r_n x_\vartheta.u_0 v_1^{n-1}.$$

Multipliant cette dernière égalité par $u_1 v_2^{-1} \dots v_k^{-1} u_k$ à droite et appliquant f_ϑ à chacun des membres, on trouve:

$$\begin{aligned} & \vartheta(u_0 v_1^{-1} u_1 v_2^{-1} \dots v_k^{-1} u_k) \\ = \; & f_\vartheta(x_\vartheta.u_0 v_1^{-1} u_1 v_2^{-1} \dots v_k^{-1} u_k) \\ = \; & r_1 f_\vartheta(x_\vartheta.u_0 u_1 v_2^{-1} \dots v_k^{-1} u_k) + r_2 f_\vartheta(x_\vartheta.u_0 v_1 u_1 v_2^{-1} \dots v_k^{-1} u_k) \\ & + \dots + r_n f_\vartheta(x_\vartheta.u_0 v_1^{n-1} u_1 v_2^{-1} \dots v_k^{-1} u_k) \\ = \; & r_1 \vartheta(u_0 u_1 v_2^{-1} \dots v_k^{-1} u_k) + r_2 \vartheta(u_0 v_1 u_1 v_2^{-1} \dots v_k^{-1} u_k) \\ & + \dots + r_n \vartheta(u_0 v_1^{n-1} u_1 v_2^{-1} \dots v_k^{-1} u_k) \end{aligned}$$

Par récurrence, chacun des termes du membre droit de la dernière égalité est nul. Par conséquent, on trouve $\vartheta(u_0 v_1^{-1} u_1 v_2^{-1} \dots v_k^{-1} u_k) = 0$.

(iii) Soit $u \in A^*$. On désigne par $\mathcal{P}$ l'ensemble des facteurs gauches de u. Soit E le sous-espace vectoriel de $K\ll A\gg$ engendré par $\mathcal{P}$. Soit $\nu : K\ll A\gg \to E$ l'application défini par:

$$\nu(S) = \sum_{v \in \mathcal{P}} (S, v)v.$$

On a, pour $S, T \in K\ll A\gg$, $\nu(ST) = \nu(\nu(S)T)$. En effet,

$$\begin{aligned} \nu(ST) &= \sum_{v \in \mathcal{P}} (ST, v)v \\ &= \sum_{v \in \mathcal{P}} \sum_{v = xy} (S, x)(T, y)v \end{aligned}$$

Comme $v \in \mathcal{P}$ et $v = xy$ impliquent $x \in \mathcal{P}$, la dernière somme est égale à:

$$\begin{aligned} &= \sum_{v \in \mathcal{P}} \sum_{v = xy} (\nu(S), x)(T, y) \\ &= \sum_{v \in \mathcal{P}} (\nu(S)T, v)v, \end{aligned}$$

et cette dernière égalité nous donne bien:

$$\nu(ST) = \nu(\nu(S)T). \tag{2.21}$$

On définit une action (linéaire) à droite de $F(A)$ sur E en posant, pour tout $X \in E$:

$$X.g = \nu(X\mu(g)), \tag{2.22}$$

où μ désigne la transformée de Magnus de $F(A)$ (voir paragraphe 2.4). Il s'agit d'une action du groupe libre sur l'espace E. En effet, soient $g, h \in F(A)$; on utilise la relation (2.21) pour trouver:

$$\begin{aligned} X.(gh) &= \nu(X\mu(gh)) \\ &= \nu(X\mu(g)\mu(h)) \\ &= \nu(\nu(X\mu(g))\mu(h)) \\ &= \nu(X.g\mu(h)) = (X.g).h\ . \end{aligned} \tag{2.23}$$

Nous avons tout ce qu'il faut pour montrer que la fonction sous-mot $(\bar{}_u)$ est représentative. Soit $1 \in E$, le vecteur distingué de E, et la fonctionelle linéaire $f : E \to K$

$$X \mapsto (X, u).$$

On a, par définition, $\binom{g}{u} = (\mu(g), u)$. Comme u est dans E, on a:

$$\begin{aligned}(\mu(g), u) &= (\nu(\mu(g)), u) \\ &= (\nu(1 \cdot \mu(g)), u) \\ &= (1.g, u) = f(1.g).\end{aligned}$$

Ainsi, on a montré que la fonction sous-mot $\binom{-}{u}$ est représentative. ◇

(Première) *Démonstration du Théorème 2.6.1.*

Dans le membre droit de (2.17), considérons les exposants $n_h(-)$ comme des fonctions sur $F(A)$. Ce membre droit est dans l'algèbre des fonctions sous-mot. Le membre droit de la relation de Thérien (2.19) est une combinaison linéaire de fonctions sous-mot. Ces deux expressions définissent donc des fonctions représentatives de $F(A)$, en vertu des points (i) et (iii) du Lemme 2.6.5.

La fonction donnée par le membre droit de (2.17) calcule l'exposant $n_{h_0}(g)$ de h_0 dans la décomposition de g en produit décroissant de mots de Hall, lorsqu'évaluée en g.

Pour $h = h_0$, le membre droit de l'identité de Thérien (2.19) calcule aussi l'exposant $n_{h_0}(g)$ lorsque g est un mot positif de $F(A)$. Ainsi, les deux fonctions représentatives données par les membres droits de (2.17) et (2.19) coïncident sur A^*. Cela implique, selon le point (ii) du Lemme 2.6.5, qu'elles coïncident sur $F(A)$ tout entier. ◇

2.6.2 Topologie de Hall.

Nous allons montrer à nouveau que l'identité de Thérien (2.20) est valide sur $F(A)$ tout entier, par un argument topologique. Pour plus de détails sur ce qui suit le lecteur est renvoyé à [HM 50b]. Nous allons munir le groupe libre $F(A)$ d'une topologie, qu'on appelle la *topologie de Hall*, introduite par M. Hall [HM 50b]. Nous verrons que pour cette topologie, le monoïde libre est *dense* dans $F(A)$ et que les fonctions sous-mot $\binom{-}{u}$ sont *continues*. On en déduira que les fonctions définies par (2.17) et (2.19), qui coïncident sur A^*, coincident sur $F(A)$ tout entier.

Soit $\Phi = \{H_\iota\}_{\iota \in I}$ une famille de sous-groupes d'un groupe G qui satisfait les conditions suivantes:

$$\bigcap_{\iota \in I} H_\iota = \{1\}, \tag{2.24}$$

$$\text{Si } H_\iota, H_{\iota'} \in \Phi \text{ alors } H_\iota \cap H_{\iota'} \in \Phi, \tag{2.25}$$

$$\text{Si } H_\iota \in \Phi \text{ alors } \exists \text{ un sous-groupe normal } H_{\iota'} \text{ tel que } H_{\iota'} \subset H_\iota. \tag{2.26}$$

On peut alors définir sur G une topologie, en prenant comme base d'ouverts de la topologie tous les translatés à gauche et à droite des sous-groupes de la famille Φ. C'est-à-dire que la base d'ouverts de la topologie est formée des $xH_\iota, H_\iota x$ pour $x \in G, \iota \in I$.

Exemple 2.6.6 Soit Z le groupe (additif) des entiers. Pour tout $q \geq 1$, qZ est un sous-groupe (normal) de Z. Soit $\Phi = \{qZ\}_{q\geq 1}$. On vérifie aisément que la famille Φ satisfait aux conditions (2.24), (2.25) et (2.26) ci-haut. La base d'ouverts de la topologie que Φ permet de définir est $\{qZ + b\}_{q\geq 1, 0\leq b\leq q-1}$.

Remarques 2.6.7 Nous discutons ici, quelques notions él'ementaires de la théorie des groupes topologiques, nécessaire pour la suite de notre exposé. Pour plus de détails, le lecteur est renvoyé à [Bo 60].

(i) Pour $q \geq 1$, désignons par π_q la projection canonique $Z \to Z/qZ$. Désignons par $\bar{b}$ la classe de $b \in Z$ dans Z/qZ. Munissons le groupe fini Z/qZ de la topologie discrète. La projection π_q est alors continue puisque $\pi_q^{-1}(\bar{b}) = qZ + b$.

(ii) Soit maintenant un groupe G, muni d'une topologie, et un homomorphisme $\phi : G \to Z$. Alors ϕ est continu si et seulement si $\pi_q \circ \phi$ est continu, pour tout $q \geq 1$. En effet, cela vient de l'égalité $\phi^{-1}(qZ + b) = (\pi_q \circ \phi)^{-1}(\bar{b})$.

(iii) La remarque en (ii) peut être généralisée. Soit $H \subset Z^{m\times m}$ un groupe (multiplicatif) de matrices sur Z. En projetant chacune des entrées d'une matrice sur Z/qZ on obtient un homomorphisme $\bar{\pi}_q : Z^{m\times m} \to (Z/qZ)^{m\times m}$. Munissons $Z^{m\times m}$ et $(Z/qZ)^{m\times m}$ des topologies produits. Alors, à l'aide de (ii), on voit que tout homomorphisme $\phi : G \to H$ est continu si et seulement si $\bar{\pi}_q \circ \phi$ est continu, pour tout $q \geq 1$.

(iv) Soit Ω un espace topologique. La topologie produit sur $\Omega \times \ldots \times \Omega$ peut être obtenue en prenant comme base d'ouverts les $V_i \times \ldots \times V_{i'}$ où les V_i sont pris d'une base d'ouverts de Ω. On montre facilement que la projection sur une composante $\Omega \times \ldots \times \Omega \to \Omega$ est continue, pour cette topologie. Par exemple, pour $\Omega = Z$, comme au point (iii), la projection $Z^{m\times m} \to Z$ qui donne l'entrée d'indices i, j d'une matrice est continue. ◇

La famille $\Phi = \{H_i\}_{i\in I}$ des sous-groupes de $F(A)$ qui sont d'*index fini* satisfait aux conditions (2.24), (2.25) et (2.26) et permet de munir $F(A)$ d'une topologie. Muni de cette topologie, $F(A)$ devient un groupe topologique. Cette topologie a été introduite par M. Hall [HM 50b]; nous la nommerons la *topologie de Hall.*

Remarque 2.6.8 On vérifie aisément que pour la topologie de Hall, tout homomorphisme $F(A) \to G$, de $F(A)$ dans un groupe fini muni de la topologie discrète, est continu. Cela découle du fait que le noyau de l'homomorphisme est d'index fini. ◇

Pour la topologie de Hall de $F(A)$, une suite d'éléments $\{g_n\}_{n\geq 1}, g_n \in F(A)$, converge vers $g \in F(A)$ si et seulement si pour tout homomorphisme $\phi : F(A) \to G$ (où G est un groupe fini muni de la topologie discrète), il existe un entier n_ϕ tel que pour tout $n \geq n_\phi, \phi(g_n) = \phi(g)$. On donne maintenant un exemple important de suite convergente dans $F(A)$.

Proposition 2.6.9 ([Pi 88, Reu 79]) *Pour tout $x, y, g \in F(A)$ on a:*

$$\lim_{n\to\infty} xg^{n!}y = xy.$$

Démonstration. On montre facilement que la multiplication $(g,h) \mapsto gh$ est continue dans $F(A)$. Il suffit donc de montrer que $\lim_{n\to\infty} g^{n!} = 1$, pour tout $g \in F(A)$. Soit G un groupe fini et $\phi : F(A) \to G$ un homomorphisme. Alors pour tout $n \geq |G|$, $|G|$ divise $n!$ de sorte que $\phi(g^{n!}) = (\phi(g))^{n!} = 1$. ◇

Corollaire 2.6.10 *Le monoïde libre A^* est dense dans le groupe libre $F(A)$, pour la topologie de Hall.*

Démonstration. Soit $g \in F(A)$. Il nous faut construire une suite de mots positifs, $(w_n)_{n\geq 1}, w_n \in A^*$, qui converge vers g. Tout $g \in F(A)$ peut s'écrire $g = u_0 v_1^{-1} u_1 \dots v_k^{-1} u_k$, avec $k \geq 0, u_i, v_j \in A^*$. Posons $x_i = u_{i-1} v_i^{-1}$, pour $i = 1, \dots, k$, et $y = u_k$. On a donc $g = x_1 \dots x_k y$. Comme la multiplication est continue, on peut utiliser la Prop. 2.6.9 pour obtenir:

$$\begin{aligned} & \lim_{n\to\infty} x_1 v_1^{n!} \dots x_k v_k^{n!} y \\ = & \left(\prod_{i=1}^{k} \lim_{n\to\infty} x_i v_i^{n!} \right) y \\ = & \left(\prod_{i=1}^{k} x_i \right) y \quad = \quad g. \end{aligned}$$

Or, pour $n \geq 1$ on a $x_i v_i^{n!} \in A^*$. La suite $(x_1 v_1^{n!} \dots x_k v_k^{n!} y)_{n\geq 1}$ est donc une suite de mots positifs qui converge vers g. ◇

Nous allons maintenant montrer que la fonction sous-mot $\binom{-}{u}$, $u \in A^*$, est continue pour la topologie de Hall. Nous reprenons la construction de la démonstration du point (iii) du Lemme 2.6.5.

Soit $u \in A^*, u = a_1 \dots a_n$. Considérons la base ordonnée

$$\mathcal{B} = (1, a_1, a_1 a_2, \dots, a_1 \dots a_n)$$

du sous-espace vectoriel $E \subset K\langle\langle A \rangle\rangle$ engendré par l'ensemble $\mathcal{P}$ des facteurs gauches de u. On définit, à l'aide de l'application (2.22), un endomorphisme $\varphi(g)$ de E, en posant: $\varphi(g)(X) = X.g$, pour chaque $g \in F(A)$. On a, pour $x \in \mathcal{B}$:

$$\varphi(g)(x) = x.g = \nu(x\mu(g)) = \sum_{v\in\mathcal{P}, v=xy} (\mu(g), y)xy. \tag{2.27}$$

Ainsi, l'application:

$$\begin{aligned} \varphi : F(A) &\to \mathrm{End}(E) \\ g &\mapsto \varphi(g) \end{aligned}$$

définit un homomorphisme de groupes, en vertu de (2.23). Comme la transformée de Magnus est à coefficients dans Z, l'endomorphisme $\varphi(g)$ est codé par une matrice dans $Z^{m\times m}$, où on a posé $m = n+1$. Nous identifierons $\varphi(g)$ à sa matrice. Faisant suivre l'homomorphisme φ de la projection $Z^{m\times m}\to(Z/qZ)^{m\times m}$ on obtient un homomorphisme $\varphi_q : F(A)\to(Z/qZ)^{m\times m}$, dont l'image est un groupe fini. Or, la topologie de Hall est telle que cet homomorphisme est continu, pour tout $q \geq 1$ (Rem. 2.6.8). Selon la Rem. 2.6.7 (iii), $\varphi : F(A)\to Z^{m\times m}$ est continu.

La valeur de la fonction sous-mot $\binom{g}{u}$ est inscrite à l'entrée de la matrice $\varphi(g)$ indicée par $(1,u)$. En effet, si on reprend (2.27) avec $x = 1$, on trouve:

$$\varphi(g)(1) = \nu(\mu(g)) = \sum_{v\in P} (\mu(g), v).$$

Or, la projection sur la composante d'indice $(1,u)$, $Z^{m\times m}\to Z$, est continue (Rem. 2.6.7 (iv)). Par conséquent, $\binom{-}{u} : F(A) \xrightarrow{\varphi} Z^{m\times m}\to Z$ est continue. On obtient ainsi la nouvelle démonstration, ci-dessous, du Th. 2.6.1

(Deuxième) *Démonstration du Théorème* 2.6.1.

Les membres droits des égalités (2.17) et (2.19) sont dans l'algèbre des fonctions sous-mot. Par conséquent, ils définissent des fonctions continues $F(A)\to Z$. Or, ces fonctions coïncident sur A^* puisque leurs valeurs en $w \in A^*$ donnent l'exposant du commutateur de Hall h_0 dans la décomposition de w en produit décroissant de commutateurs de Hall. Comme A^* est un sous-ensemble dense de $F(A)$, la continuité des fonctions implique qu'elles coïncident sur $F(A)$ tout entier. On a donc, pour $h_0 \in H(A)$ et pour tout $g \in F(A)$:

$$n_{h_0}(g) = \sum_{u\in A^*, |u|\leq|h_0|} k_{h_0,u}\binom{g}{u}.$$

◇

Chapitre 3

Constructions des bases standard des $K<A>$-modules à droite

3.1 Introduction.

On sait depuis P. M. Cohn [Co 69] que tout idéal à droite de $K<A>$ est libre (comme $K<A>$-module à droite). Berstel et Reutenauer en ont donné une nouvelle preuve qui utilise les codes préfixes ([BR 88, Chap. II, Th. 3.2]). La présence des codes préfixes dans ce contexte est liée aux résultats de Schützenberger [Sc 58] concernant les représentations minimales des séries rationelles (en variables non commutatives) en rapport avec les récurrences linéaires que satisfont ces séries.

Nous présentons ici des bases pour les sous-$K<A>$-modules à droite de $K<A>^q$, que nous appelons *bases standard* (paragraphes 3.4, 3.5). Dans le cas où $q = 1$, ces sous-modules (sous-$K<A>$-modules à droite) sont des idéaux à droite de $K<A>$ et la construction des bases standard est très proche de la construction de Schreier d'une base d'un sous-groupe du groupe libre (voir [LS 77, MKS 76]).

Dans le but de donner une construction effective de la base standard d'un sous-module, on munit l'ensemble des mots du monoïde libre A^* d'un ordre $\leq$, satisfaisant certaines conditions de compatibilité (voir paragraphe 3.2). Cet ordre est un analogue non commutatif de celui imposé sur l'ensemble des monômes de $K[z_1, \ldots, z_n]$ pour le calcul des *bases de Gröbner* (ou *bases standard*) des idéaux de cet anneau (voir Rem. 3.2.1). Les algorithmes que nous donnons, qui permettent le calcul de la base standard d'un sous-module, sont analogues à ceux déjà existant dans le cas des bases de Gröbner des idéaux de $K[z_1, \ldots, z_n]$ (voir [Bu 85]). Les calculs effectués sur les systèmes de générateurs se font tous à l'aide de *réécritures élémentaires*. Ces réécritures élémentaires sont inspirées

des transformations de Nielsen (voir [LS 77, MKS 76]) utilisées pour le calcul d'une *base réduite* d'un sous-groupe de type fini du groupe libre.

Une des principales applications de nos résultats est de rendre effectif le travail avec les sous-modules $\mathcal{M}$ de $K<A>^q$ et les quotients $K<A>^q/\mathcal{M}$. L'ordre $\leq$ étant fixé, on montre l'*unicité* de la base standard d'un sous-module (Th. 3.4.8, Th. 3.5.11). L'algorithme de calcul de la base standard d'un sous-module de type fini (Th. 3.4.9, Th. 3.5.17) permet de tester si deux sous-modules de type fini sont égaux (Cor. 3.4.11, Cor. 3.5.20). On est aussi en mesure de tester si un élément de $K<A>^q$ appartient à un sous-module $\mathcal{M}$ et on peut résoudre le "problème des mots" dans le quotient $K<A>^q/\mathcal{M}$ (Cor. 3.4.12, Cor. 3.5.21).

Dans [Mo 85], Mora construit des bases de Gröbner des *idéaux bilatères de* $K<A>$. Notre approche est sensiblement différente et nous livre des résultats d'une autre nature. D'une part, nous considérons les idéaux à droite de $K<A>$. D'autre part, nous nous inspirons de Cohn [Co 61, Co 69] pour introduire la notion de $\leq$-dépendance à droite d'une famille de polynômes; ce faisant, nous obtenons une version adaptée à notre contexte de l'*Algorithme faible (transfini)* de Cohn (voir Rem. 3.2.8). Nos méthodes permettent aussi de réaliser l'algorithme faible de Cohn (pour le degré des polynômes) dans l'algèbre des polynômes non commutatifs (voir Prop. 3.3.7). Nous développons d'abord, aux paragraphes 3.2, 3.3 et 3.4, la théorie pour les idéaux (le cas $q = 1$). Nous généralisons ensuite aux dimensions supérieures ($q \geq 1$) (paragraphe 3.5). Nous tenons à remercier A. Joyal qui s'est intéressé à notre travail; la définition des bases standard, pour le cas $q > 1$, nous a été suggérée par lui.

3.2 Recteurs des polynômes et $\leq$-dépendance à droite.

Nous allons maintenant travailler dans l'algèbre des polynômes non commutatifs sur un alphabet A. Nous l'avons introduite au paragraphe 1.6; nous reprenons dans ce chapitre les mêmes notations (voir page 29).

Un ensemble de mots $X \subset A^*$ est un *code préfixe* si aucun mot de X n'est préfixe d'un autre mot de X. Par exemple, $\{abc, ac, b\}$ et $\{a^n b : n \geq 0\}$ sont des codes préfixes. Notez que cette définition fait de l'ensemble vide et de l'ensemble $\{1\}$, réduit au mot vide, des codes préfixes. L'ensemble $\{1\}$ est le seul code préfixe dont le mot vide fait partie. On se donne un *bon ordre* $\leq$ sur l'ensemble des mots. On suppose que cet ordre est *compatible avec la multiplication à droite* et qu'il est *préfixiel*, c'est-à-dire qu'il satisfait:

$$\text{Pour tous mots } u, v, w \in A^*, u \leq v \text{ implique } uw \leq vw, \tag{3.1}$$

$$\text{Si } u, v, w \in A^*, v \text{ est non vide et } w = uv \text{ alors } u < w. \tag{3.2}$$

De la deuxième condition on déduit que $1 \leq w$ pour tout $w \in A^*$.

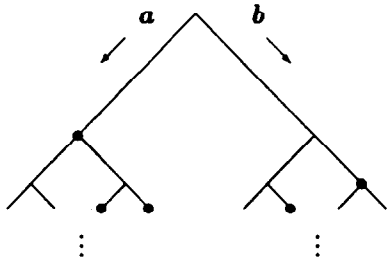

Figure 3.1: Représentation par arbre du monoïde libre sur $\{a, b\}$.

Remarque 3.2.1 Soit $Z = \{z_1, \ldots, z_n\}$ un ensemble d'*indéterminées* qui commutent deux à deux; désignons par $K[Z]$ l'anneau de *polynômes commutatifs* sur Z à coefficient dans K. Dans la théorie des *Bases de Gröbner* (ou *Bases standard*) des idéaux de $K[Z]$ (voir [Bu 85]), dans le but de formuler des algorithmes qui calculent les bases standard des idéaux, on impose un *bon ordre* $\leq$ sur l'ensemble des monômes $z_1^{\alpha_1} \ldots z_n^{\alpha_n}$ de $K[Z]$. Ce bon ordre doit être *compatible* avec la *multiplication* et doit satisfaire:

$$1 \leq z_1^{\alpha_1} \ldots z_n^{\alpha_n} \tag{3.3}$$

où 1 est l'élément unité de l'anneau et où $z_1^{\alpha_1} \ldots z_n^{\alpha_n}$ est un monôme quelconque de $K[Z]$.

On voit que les conditions (3.1) et (3.2) nous donnent un analogue non commutatif (à droite) des conditions imposées sur l'ensemble des monômes dans le cas commutatif. En effet, dans les deux cas l'ordre doit être compatible avec la multiplication. Si dans $K[Z]$ on a:

$$z_1^{\alpha_1} \ldots z_n^{\alpha_n} = z_1^{\beta_1} \ldots z_n^{\beta_n}\ z_1^{\gamma_1} \ldots z_n^{\gamma_n},$$

alors de la condition (3.3), et à l'aide de la commutativité de la multiplication, on déduit que: $z_1^{\beta_1} \ldots z_n^{\beta_n} < z_1^{\alpha_1} \ldots z_n^{\alpha_n}$. En définissant de façon appropriée les préfixes d'un monôme de $K[Z]$, on voit que la condition (3.3) est équivalente à exiger qu'un monôme soit précédé par tous ses préfixes. $\diamond$

On peut se représenter le monoïde libre sous la forme d'un arbre infini. A la racine de l'arbre se trouve le mot vide et à chaque sommet de l'arbre est placé un mot de A^*. L'ensemble des fils d'un mot w est: $\{wa : a \in A\}$. Notez que l'idéal à droite wA^* dans A^*, engendré par un mot w est obtenu en détachant de A^* le sous-arbre qui a w pour racine. Par exemple, si $A = \{a, b\}$ l'arbre est binaire. On peut convenir qu'une arête vers la gauche correspond à la lettre a et qu'une arête vers la droite correspond à la lettre b. Ainsi, à la Fig. 3.1, les sommets marqués d'un point sont a, aba, abb, bab, bb.

Remarque 3.2.2 On vérifie facilement avec cette représentation si un ensemble X de mots est un code préfixe. Il suffit de s'assurer que jamais deux mots de X ne se trouvent le long d'une même branche de l'arbre. ◇

Exemple 3.2.3 L'ordre du dictionnaire des mots croisés est un ordre qui satisfait nos conditions. Cet ordre est construit en ordonnant d'abord les mots par longueur, puis lexicographiquement sur chacune des longueurs. Plus précisément, $u < v$ si et seulement si soit $|u| < |v|$, soit $|u| = |v|$ et $u <_{lex} v$. C'est l'ordre que nous utiliserons toujours dans les exemples.

Maintenant, ordonnons les lettres de l'alphabet A et convenons de placer les fils d'un sommet de l'arbre de A^* de gauche à droite selon l'ordre des lettres de A. Alors, on voit que pour parcourir les mots selon l'ordre du dictionnaire de mots croisés dans l'arbre, il faut faire comme suit: on commence d'abord par la racine (le mot vide), puis on visite, en allant de gauche à droite, les sommets qui se trouvent à distance 1 du mot vide, puis ceux qui se trouvent à distance 2, etc... Par exemple, si on parcourt l'arbre de la Fig. 3.1 selon cet ordre on rencontre les sommets marqués d'un point dans l'ordre a, bb, aba, abb, bab. ◇

Soit $P \in K\langle A\rangle$; le *recteur* [1] de P est le mot le plus grand qui y apparaît: $r(P) = \max\{w : w \in P\}$. Par exemple, $r(abc + 4b) = abc$ et $r(ab - 2a) = ab$. On conviendra que $r(0) < r(P), \forall P \in K\langle A\rangle$. Nous dirons d'un polynôme qu'il est *unitaire* si le coefficient de son recteur est égal à 1. En d'autres mots, un polynôme P est unitaire s'il s'écrit sous la forme: $P = u + \sum_{v<u}(P,v)v$.

Lemme 3.2.4 *Soient* $P, Q et P_i, Q_i \in K\langle A\rangle (i = 1, \ldots, N)$.

(i) Pour tout $w \in A^*$, *on a* $r(Pw) = r(P)w$,

(ii) $r(PQ) = \max\{r(Pw) : w \in Q\} = \max\{r(P)w : w \in Q\}$,

(iii) $r(\sum_{n=1}^{N} P_nQ_n) \leq \max_{n=1,\ldots,N} r(P_nQ_n)$.

Démonstration. (i) Soit $w' \in Pw$. Alors $w' = uw$ pour un certain $u \in P$. Comme $u \leq r(P)$, la condition (3.1) entraîne $uw \leq r(P)w$, d'où l'assertion, puisque $r(P)w \in Pw$.

(ii) D'une part, on a $PQ = \sum_{w\in Q}(Q,w)Pw$. D'autre part, $r(Pw) = r(P)w$ pour tout $w \in Q$, en vertu du point (i) de la démonstration. Par conséquent, si le mot $\max\{r(Pw) : w \in Q\} = \max\{r(P)w : w \in Q\}$ a un coefficient non nul dans PQ, alors c'est le recteur de PQ. Soient $u = r(P)$ et $w_1 \in A^*$ tels que $uw_1 = \max\{r(Pw) : w \in Q\}$. Il

[1] En grammaire française, le mot qui tient le rôle central dans un groupe de mots s'appelle le *recteur* de ce groupe de mots. Par exemple, dans *'Le célèbre algorithme faible de Cohn'*, le recteur est *'algorithme'*.

nous faut montrer que $(PQ, uw_1) \neq 0$. Supposons qu'au contraire on ait $(PQ, uw_1) = 0$. Alors c'est qu'il existe des mots $v \in P, w_2 \in Q$ tels que $u \neq v$ et $w_1 \neq w_2$, et tels que $uw_1 = vw_2$. Comme $u = r(P)$, on a $u > v$, de sorte que la condition (3.1) entraîne $uw_2 > vw_2 = uw_1$, ce qui contredit la maximalité de uw_1. On a donc $(PQ, uw_1) \neq 0$ et par conséquent $r(PQ) = uw_1 = \max\{r(Pw) : w \in Q\}$.

(iii) Il suffit de voir que si $w \in \sum_{n=1}^{N} P_nQ_n$ alors $w \leq \max_{n=1,\ldots,N} r(P_nQ_n)$. Mais si $u \in P_n, v \in Q_n$ alors, en vertu des points (i) et (ii) on a $uv \leq r(P)v = r(Pv) \leq \max\{r(Pv) : v \in Q_n\} = r(P_nQ_n)$; comme $r(P_nQ_n) \leq \max_{n=1,\ldots,N} r(P_nQ_n)$, le résultat est montré. ◇

Lemme 3.2.5 *Soient P et Q des polynômes unitaires de recteurs respectifs u et v. S'il existe $w \in A^*$ tel que $u = vw$, alors $r(P - Qw) < r(P)$.*

Démonstration. On a, selon le Lemme 3.2.4 (i), $u = vw = r(Qw)$. Comme ce mot apparaît dans Qw avec coefficient 1, l'inégalité $r(P - Qw) < r(P)$ est vérifiée. ◇

Soient maintenant N un ensemble d'indices et $\{Q_\nu\}_{\nu \in N}$ une famille de polynômes de $K\langle A\rangle$. Nous ne considérerons que les cas où N est l'ensemble des entiers non nuls ou $N = \{1, \ldots, n\}$. Dans les deux cas nous noterons les familles par $\{Q_n\}_{n \geq 1}$ en précisant de quel cas il s'agit lorsque cela s'avère nécessaire; les familles finies seront parfois notées simplement $Q_1, \ldots, Q_n$. On dira que les polynômes Q_n sont *presque tous nuls* si l'ensemble $\{n : Q_n \neq 0\}$ est fini; c'est toujours le cas lorsque la famille est finie.

Soient $\{P_n\}_{n \geq 1}$ et $\{Q_n\}_{n \geq 1}$ deux familles de polynômes et supposons que les polynômes Q_n sont presque tous nuls. Alors les polynômes P_nQ_n sont presque tous nuls et la somme $\sum_{n \geq 1} P_nQ_n$ est définie.

Remarque 3.2.6 Le résultat (iii) du Lemme 3.2.4 reste vrai si on multiplie une famille $\{P_n\}_{n \geq 1}$ et une famille de polynômes presque tous nuls $\{Q_n\}_{n \geq 1}$, à savoir:

$$r(\sum_{n \geq 1} P_nQ_n) \leq \max_{n \geq 1} r(P_nQ_n). \tag{3.4}$$

◇

Nous nous inspirons de Cohn [Co 61, Co 69] pour introduire la notion de $\leq$-dépendance à droite dans l'algèbre $K\langle A\rangle$. On dira qu'une famille de polynômes $\{P_n\}_{n \geq 1}$ est $\leq$-*dépendante à droite* si soit l'un des P_n est nul, soit il existe une famille de polynômes $\{Q_n\}_{n \geq 1}$ presque tous nuls, mais non tous nuls, tels que:

$$r(\sum_{n \geq 1} P_nQ_n) < \max_{n \geq 1} r(P_nQ_n).$$

On dira qu'un polynôme P est $\leq$-*dépendant à droite de la famille* $\{P_n\}_{n\geq 1}$ si soit il est nul, soit il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls tels que:

$$r(P - \sum_{n\geq 1} P_n Q_n) < r(P),$$

et tels que $r(P_n Q_n) \leq r(P)$, pour tout n.

Remarque 3.2.7 Notez que selon cette définition la famille vide est une famille indépendante. ◇

Remarque 3.2.8 Dans [Co 85], Cohn définit l'*Algorithme faible*. Soit R un anneau muni d'une fonction $v : R \to N$, appelée *pseudo-valuation*. Pour $r \in R$, l'entier $v(r)$ est appelé le *degré* de r. La fonction v satisfait des conditions de compatibilité avec les opérations de l'anneau - similaires aux propriétés de la fonction de degré dans les anneaux de polynômes en variables commutatives (voir [Co 85, Chap. 2]). On peut définir la dépendance (à droite) d'une famille $\{r_i\}_{i\in I}$ (avec $r_i \in R$), et la dépendance d'un élément r sur une famille $\{r_i\}_{i\in I}$, par rapport à cette fonction v. On dit que l'anneau R *satisfait* l'algorithme faible si dans toute famille dépendante $r_1, \ldots, r_n$ d'éléments de R, ordonnés de façon croissante (i.e. $v(r_1) \leq \ldots v(r_n)$), il existe un élément r_i qui dépend des précédents $r_1, \ldots, r_{i-1}$.

Dans $K\langle A\rangle$, on peut définir la pseudo-valuation $d : K\langle A\rangle \to N$ qui donne le degré d'un polynôme, $d(P) = \max\{|w| : w \in P\}$. On peut montrer que s'il y a une relation de dépendance entre des polynômes $P_1, \ldots, P_n$, ordonnés selon le degré, cela implique que l'un des P_i est dépendant de ses prédécesseurs (cf. [Co 61]). L'algèbre associative libre satisfait donc l'algorithme faible pour la fonction *'degré'*.

Cohn [Co 85] définit aussi l'*Algorithme faible transfini*. Etant donné une fonction ω définie sur un anneau R à valeur dans un *ensemble bien ordonné*, on peut aussi définir la dépendance (à droite) d'une famille $\{r_i\}_{i\in I}$ ($r_i \in R$), et la dépendance d'un élément r sur une famille $\{r_i\}_{i\in I}$, par rapport à ω (en imposant à ω certaines conditions de compatibilité avec les opérations de l'anneau; voir [Co 85, Chap. 2]). On dit que l'anneau R *satisfait* l'algorithme faible transfini si dans toute famille dépendante d'éléments de R, il existe un élément qui dépend des autres éléments de la famille.

La fonction $r : K\langle A\rangle \to A^*$ qui donne le recteur d'un polynôme est une fonction à valeur dans un ensemble bien ordonné, en vertu des hypothèses que nous avons faites sur l'ordre $\leq$ imposé aux mots du monoïde libre A^*. Le Cor. 3.2.12 (plus loin) montre que $K\langle A\rangle$ satisfait l'algorithme faible transfini pour cette fonction. La notion de $\leq$-dépendance (à droite) est plus 'serrée' que la notion de dépendance (à droite) par rapport au degré. En effet, s'il y a une relation de $\leq$-dépendance à droite dans une famille de polynômes, elle a toujours lieu entre deux polynômes de la famille (voir Cor. 3.2.12). ◇

Remarques 3.2.9 (i) Si une sous-famille de la famille $\{P_n\}_{n\geq 1}$ est $\leq$-dépendante à droite alors la famille $\{P_n\}_{n\geq 1}$ est $\leq$-dépendante à droite.

(ii) Si un polynôme P est $\leq$-dépendant à droite d'une famille de polynômes $\{P_n\}_{n\geq 1}$ alors la famille $\{P\} \cup \{P_n\}_{n\geq 1}$ est $\leq$-dépendante à droite.

(iii) Si un polynôme P est $\leq$-dépendant à droite d'une sous-famille de la famille $\{P_n\}_{n\geq 1}$ alors la famille $\{P\} \cup \{P_n\}_{n\geq 1}$ est aussi $\leq$-dépendante à droite. ◇

Remarque 3.2.10 Utilisant le (iii) du Lemme 3.2.4 on voit qu'une famille de polynômes $\{P_n\}_{n\geq 1}$ est *indépendante à droite* si quelle que soit la famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls on a:

$$r(\sum_{n\geq 1} P_n Q_n) = \max_{n\geq 1} r(P_n Q_n).$$

Et dans ce cas, selon les résultats du même Lemme, il existe un indice i et des mots $u_i \in P_i, v_i \in Q_i$ tels que $r(\sum_{n\geq 1} P_n Q_n) = u_i v_i$. ◇

Par la suite, nous abrégerons l'expression '*$\leq$-dépendant à droite*' par *dépendant*.

Théorème 3.2.11 *Soit $\{P_n\}_{n\geq 1}$ une famille de polynômes non nuls et soit $u_n = r(P_n)$. La famille $\{P_n\}_{n\geq 1}$ est indépendante si et seulement si les u_n sont distincts deux à deux et forment un code préfixe.*

Démonstration. On peut supposer P_n unitaire, pour tout n.

Supposons d'abord que les mots u_n ne soient pas distincts deux à deux ou ne forment pas un code préfixe. Alors il existe $i \neq j$ et un mot $w \in A^*$ tels que $u_i = u_j w$. Selon le Lemme 3.2.4 (i), on a $r(P_i) = r(P_j w)$. Selon le Lemme 3.2.5 on a $r(P_i - P_j w) < r(P_i)$. Par conséquent, P_i est dépendant de P_j. En vertu de la Rem. 3.2.9 (iii), cela implique que la famille $\{P_n\}_{n\geq 1}$ est dépendante.

Supposons maintenant que les mots u_n sont distincts deux à deux et forment un code préfixe. Soit $\{Q_n\}_{n\geq 1}$ une famille de polynômes presque tous nuls. Selon les points (i) et (ii) du Lemme 3.2.4, pour tout i tel que $Q_i \neq 0$, il existe un mot $v_i \in Q_i$ tel que $r(P_i Q_i) = r(P_i)v_i$. Soient $u_k = r(P_k)$ et $v_k \in Q_k$ tels que $u_k v_k = \max_{n\geq 1} r(P_n Q_n)$. Ce mot est bien défini puisque les polynômes $P_n Q_n$ sont presque tous nuls. Montrons que $u_k v_k$ apparaît dans $\sum_{n\geq 1} P_n Q_n$. Sinon, c'est qu'il existe un indice j et des mots $u' \in P_j, v' \in Q_j$ tels que $u_k v_k = u'v'$, et:

(i) soit $j = k, u' \in P_k$ et $u' < u_k$,

(ii) soit $j \neq k, u' \in P_j$ et $u' \leq u_j$.

Observons d'abord que dans le cas (ii), on ne peut avoir $u' = u_j$ puisqu'alors $u_k v = u_j v'$ et que les u_i sont distincts deux à deux et forment un code préfixe. On a donc dans tous les cas, $u_j > u'$. Mais alors, en utilisant la condition (3.1), on trouve que: $u_j v' > u'v' = u_k v_k$, ce qui contredit la maximalité de $u_k v_k$.

Comme le mot $u_k v_k$ apparaît dans $\sum_{n\geq 1} P_n Q_n$, on a, selon la Rem. 3.2.10, $r(\sum_{n\geq 1} P_n Q_n) = u_k v_k$; c'est-à-dire $r(\sum_{n\geq 1} P_n Q_n) = \max_{n\geq 1} r(P_n Q_n)$. La famille $\{Q_n\}_{n\geq 1}$ étant arbitraire, on en conclut que la famille de polynômes $\{P_n\}_{n\geq 1}$ est indépendante. ◇

Soit $\{P_n\}_{n\geq 1}$ une famille indépendante de polynômes. Nous dirons que le code préfixe $\{u_n\}_{n\geq 1}$, où $u_n = r(P_n)$, est le *code préfixe associé* à la famille $\{P_n\}_{n\geq 1}$. La démonstration du Th. 3.2.11 montre aussi le corollaire suivant.

Corollaire 3.2.12 *Si la famille $\{P_n\}_{n\geq 1}$ est dépendante alors il existe des indices $i \neq j$ tels que P_i est dépendant de P_j. Plus précisément, il existe des indices $i \neq j$ et un mot $w \in A^*$ tels que $r(P_i - P_j w) < r(P_i)$.* ◇

Remarque 3.2.13 Du Th. 3.2.11 on déduit un algorithme simple pour vérifier si une famille finie de polynômes forment une base de l'idéal qu'elle engendre. Cet algorithme devrait trouver, dans le cas où les générateurs sont liés par une relation de dépendance, une relation $u_i = u_j v$ entre les recteurs u_i et u_j de deux générateurs P_i et P_j. On trouve donc du même coup, selon le Cor. 3.2.12, la relation de dépendance qui lie P_i et P_j. ◇

Remarque 3.2.14 Dans [Mo 85], Mora suit de très près les concepts et les définitions utilisés dans le cas commutatif, pour construire des bases de Grõbner des idéaux bilatères de $K\langle A\rangle$. L'ordre qu'il utilise sur les mots de A^* diffère du nôtre. Il annonce que ses résultats restent vrais pour les idéaux à droite. Il mentionne, sans le montrer, que si les générateurs d'un idéal ont tous des recteurs distincts qui forment un code préfixe alors ces générateurs forment une base de Grõbner de l'idéal. ◇

3.3 Idéaux à droite dans $K\langle A\rangle$.

Soient $\{P_n\}_{n\geq 1}$ une famille de polynômes; on désigne par $I = < \{P_n\}_{n\geq 1} >$, ou $I = < P_1, \ldots, P_n >$ si la famille est finie, l'*idéal à droite* de $K\langle A\rangle$ engendré par la famille $\{P_n\}_{n\geq 1}$. Les polynômes qui sont dans I sont tous de la forme $\sum_{n\geq 1} P_n Q_n$ où les Q_n sont des polynômes arbitraires de $K\langle A\rangle$, presque tous nuls. On dit aussi que la famille $\{P_n\}_{n\geq 1}$ forme un *système de générateurs* pour l'idéal I. Dans le cas où il existe une famille finie qui engendre I on dit qu'il est de *type fini*, ou *finiment engendré*. On désignera par $\varphi : K\langle A\rangle \to K\langle A\rangle/I$ le morphisme de K-module canonique.

Soit $P_1, \ldots, P_n$ un système de générateurs d'un idéal à droite. On définit trois types de 'réécritures élémentaires' d'un tel système :

(R1) si $P_i = 0$, on permet la réécriture:

$$P_1, \ldots, P_n \rightarrow P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n$$

(R2) pour $\alpha \in K, \alpha \neq 0$, on permet la réécriture:

$$P_1, \ldots, P_n \rightarrow P_1, \ldots, P_{i-1}, \alpha P_i, P_{i+1}, \ldots, P_n$$

(R3) si $i \neq j$ et $r(P_j w) = r(P_j)w \leq r(P_i)$, on permet la réécriture:

$$P_1, \ldots, P_n \rightarrow P_1, \ldots, P_{i-1}, P_i', P_{i+1}, \ldots, P_n$$

où $P_i' = P_i - P_j w$.

Remarques 3.3.1 (i) Ces trois règles de réécritures élémentaires permettent de remplacer, dans un système de générateurs, un polynôme P_i par le polynôme $P_i - \sum_{i \neq j} P_j Q_j$, avec $r(P_j Q_j) \leq r(P_i)$.

(ii) Bien que les réécritures élémentaires puissent être appliquées à des systèmes de générateurs infinis, nous ne le ferons pas. Nous utiliserons les règles de réécritures pour formuler des algorithmes de calculs effectifs des bases des idéaux engendrés par des familles finies. ◇

Lemme 3.3.2 *Soient $P_1, \ldots, P_n$ et $Q_1, \ldots, Q_m$ deux familles de polynômes. Si la famille $Q_1, \ldots, Q_m$ peut être obtenue de la famille $P_1, \ldots, P_n$ par une suite finie de réécritures élémentaires alors elles engendrent le même idéal:*

$$< P_1, \ldots, P_n > \; = \; < Q_1, \ldots, Q_m > .$$

◇

Remarque 3.3.3 Tout idéal à droite de $K<A>$ peut être considéré comme un $K<A>$-module à droite. Il est connu depuis Cohn [Co 69] qu'un tel $K<A>$-module à droite est toujours libre. Notez que si une famille de polynômes $P_1, \ldots, P_n$ est indépendante alors elle est a *fortiori* $K<A>$-linéairement indépendante. Ainsi, tout idéal à droite engendré par une famille indépendante est librement engendré par elle, comme $K<A>$-module. ◇

Soit $P_1, \ldots, P_n$ une famille finie de polynômes. Posons $\vartheta_w = |\{i : r(P_i) = w\}|$; l'entier ϑ_w compte donc le nombre de fois que w apparaît comme recteur d'un polynôme de la famille. Il n'existe qu'un nombre fini de mots w pour lesquels ϑ_w est non nul, c'est-à-dire que les entiers ϑ_w sont presque tous nuls. Le *multi-indice des recteurs* de la famille $P_1, \ldots, P_n$ est le vecteur infini d'entiers positifs ϑ_w, presque tous nuls, indicés par les

mots de A^*. On le notera $\mathcal{V} = \mathcal{V}(P_1, \ldots, P_n) = (\vartheta_w)_{w \in A^*}$. Notez que si la famille compte des polynômes nuls, ils ne contribuent en rien aux multi-indice des recteurs. On ordonne l'ensemble des multi-indices des recteurs selon *l'ordre lexicographique inverse*. Plus précisément, pour $\mathcal{V}' = (\vartheta'_w)_{w \in A^*}$ et $\mathcal{V} = (\vartheta_w)_{w \in A^*}$, on aura $\mathcal{V}' < \mathcal{V}$ si et seulement s'il existe un mot $w \in A^*$ tel que $\vartheta'_w < \vartheta_w$ et $\vartheta'_u = \vartheta_u$ pour tout $u > w$.

Lemme 3.3.4 *Soit $P_1, \ldots, P_n$ une famille de polynômes. Supposons qu'on ait, pour $i \neq j$, $r(P_j w) = r(P_j)w = r(P_i)$. Alors, si on pose $P'_i = P_i - P_j w$, on a $\mathcal{V}(P_1, \ldots, P_n) < \mathcal{V}(P_1, \ldots, P_{i-1}, P'_i, P_{i+1}, \ldots, P_n)$.*

Démonstration. On a, selon le Lemme 3.2.5, $r(P'_i) = r(P_i - P_j w) < r(P_i)$. Comme les recteurs des autres polynômes restent inchangés, on a bien

$$\mathcal{V}(P_1, \ldots, P_n) < \mathcal{V}(P_1, \ldots, P_{i-1}, P'_i, P_{i+1}, \ldots, P_n). \diamond$$

Théorème 3.3.5 *Soit I un idéal de $K<A>$ engendré par une famille finie de polynômes $P_1, \ldots, P_n$. Il est possible de calculer une base $\leq$-indépendante à droite de I en effectuant une suite finie de réécritures élémentaires sur la famille $P_1, \ldots, P_n$.*

Démonstration. On peut toujours faire en sorte que tous les polynômes de la famille $P_1, \ldots, P_n$ soient non nuls et unitaires, à l'aide d'un nombre fini de réécritures du type (R1) et (R2). On suppose donc les P_i non nuls et unitaires et on pose $u_i = r(P_i)$ pour $i = 1, \ldots, n$.

On procède par récurrence sur le multi-indice des recteurs. Si le multi-indice est nul, i.e. $\vartheta_w = 0$ pour tout $w \in A^*$, alors c'est que la famille est vide et elle est $\leq$-indépendante, en vertu de la Rem. 3.2.7. Sinon, il y a deux cas. Soit la famille est $\leq$-indépendante et il n'y a rien à faire. Soit la famille est $\leq$-dépendante et alors, en vertu du Cor. 3.2.12, il existe deux polynômes P_i et P_j $(i \neq j)$ et un mot $w \in A^*$ tels que $r(P_j w) = r(P_j)w = r(P_i)$. Posons $P'_i = P_i - P_j w$, de sorte que la famille $P_1, \ldots, P_{i-1}, P'_i, P_{i+1}, \ldots, P_n$ est obtenue à l'aide d'une réécriture du type (R3) appliquée à $P_1, \ldots, P_n$.

Selon le Lemme 3.3.2, la famille $P_1, \ldots, P_{i-1}, P'_i, P_{i+1}, \ldots, P_n$, engendre le même idéal que la famille initiale. Selon le Lemme 3.3.4, on a $\mathcal{V}(P_1, \ldots, P_n) < \mathcal{V}(P_1, \ldots, P_{i-1}, P'_i, P_{i+1}, \ldots, P_n)$. On obtient ainsi le résultat, puisque par récurrence, on peut calculer une base $\leq$-indépendante de l'idéal à l'aide d'une suite finie de réécritures élémentaires appliquées à la famille $P_1, \ldots, P_{i-1}, P'_i, P_{i+1}, \ldots, P_n$. $\diamond$

Remarque 3.3.6 Nous allons montrer comment nos méthodes permettent de réaliser, dans $K<A>$, l'algorithme faible de Cohn (pour le degré) sur une famille finie de polynômes. Rappelons d'abord quelques propriétés sur le degré. Quels que soient $P, Q \in$

$K\langle A\rangle$, on a:

$$\begin{aligned} \deg(0) &= -\infty \\ \deg(P+Q) &\leq \max(\deg(P),\deg(Q)) && (3.5)\\ \deg(P+Q) &= \deg(Q), \qquad \text{si } \deg(P) < \deg(Q) && (3.6)\\ \deg(PQ) &= \deg(P)+\deg(Q) && (3.7) \end{aligned}$$

Suivant Cohn [Co 69], nous dirons qu'une famille de polynômes $\{P_n\}_{n\geq 1}$ est d-dépendante (à droite), si soit l'un des P_n est nul, soit il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$, presque tous nuls et non tous nuls, tels que:

$$\deg(\sum_{n\geq 1} P_nQ_n) < \max_{n\geq 1} \deg(P_nQ_n).$$

De même, nous dirons qu'un polynôme P est d-dépendant (à droite) d'une famille $\{P_n\}_{n\geq 1}$ si soit il est nul, soit il existe des polynômes $\{Q_n\}_{n\geq 1}$, presque tous nuls, tels que:

$$\deg(P - \sum_{n\geq 1} P_nQ_n) < \deg(P), \tag{3.8}$$

et tels que $\deg(P_nQ_n) \leq \deg(P)$.

Tout au long de la présente remarque, nous supposerons que l'ordre $\leq$ est compatible avec le degré, dans le sens où $\deg(P) < \deg(Q)$ implique $r(P) < r(Q)$ (autrement dit, les mots sont ordonnés selon la longueur). L'ordre du dictionnaire des mots croisés (voir Ex. 3.2.3) est un ordre qui satisfait cette hypothèse.

Proposition 3.3.7 *Soit $P_1, \ldots, P_n$ une famille d-dépendante de polynômes non nuls. Il est possible de trouver, à l'aide d'un nombre fini de réécritures sur la famille $P_1, \ldots, P_n$ une relation de d-dépendance de l'un des P_m sur les autres membres de la famille qui sont de degré n'excédant pas celui de P_m.*

Démonstration. Si $P_1, \ldots, P_n$ est d-dépendante c'est qu'il existe une famille de polynômes $Q_1, \ldots, Q_n$, tels que:

$$\deg(\sum_{m=1}^{n} P_mQ_m) < \max_{m\geq 1} \deg(P_mQ_m).$$

Comme l'ordre $\leq$ est compatible avec le degré, on en tire une relation de $\leq$-dépendance de la famille. Par conséquent, selon le Cor. 3.2.12, il existe $i \neq j$ et un mot $w \in A^*$ tels que $r(P_i - P_jw) < r(P_i)$. Notez qu'on a $\deg(P_j) \leq \deg(P_i)$, de sorte que P_i est $\leq$-dépendant d'un polynôme de degré au plus égal à $\deg(P_i)$. Notez aussi que $\deg(P_jw) \leq \deg(P_i)$. Si

on a $\deg(P_i - P_j w) < \deg(P_i)$, alors on tient là la relation de d-dépendance du polynôme P_i sur le reste de la famille.

Sinon, on pose $P'_m = P_m$ pour $m \neq i$, et $P'_i = P_i - P_j w$. Nous allons montrer que la famille $P'_1, \ldots, P'_n$ est une famille d-dépendante. Posons aussi, $Q'_m = Q_m$, pour $m \neq j$, et $Q'_j = (wQ_i + Q_j)$. Alors, on vérifie facilement que:

$$\sum_{m=1}^{n} P_m Q_m = \sum_{m=1}^{n} P'_m Q'_m. \tag{3.9}$$

De plus, $P_m Q_m = P'_m Q'_m$, pour $m \neq i, j$; de sorte que $\deg(P'_m Q'_m) = \deg(P_m Q_m)$, pour $m \neq i, j$. Comme $\deg(P_i - P_j w) = \deg(P_i)$, on a en vertu de (3.7), $\deg(P'_i Q'_i) = \deg(P'_i Q_i) = \deg(P_i Q_i)$. Finalement, selon (3.5), on a

$$\deg(P'_j Q'_j) \leq \max(\deg(P_j w Q_i), \deg(P_j Q_j)),$$

de sorte que

$$\deg(P'_j Q'_j) \leq \max(\deg(P_i Q_i), \deg(P_j Q_j)),$$

puisqu'en vertu de (3.7), $\deg(P_j w Q_i) = \deg(P_j w) + \deg(Q_i) = \deg(P_i) + \deg(Q_i) = \deg(P_i Q_i)$.

Maintenant, soit k l'indice tel que $\max_{m \geq 1} \deg(P_m Q_m) = \deg(P_k Q_k)$. Si $k \neq j$ alors on trouve $\deg(P'_k Q'_k) = \deg(P_k Q_k) \geq \deg(P_m Q_m)$, pour tout $m = 1, \ldots, n$. Par conséquent, $\deg(P'_k Q'_k) \geq \deg(P'_m Q'_m)$, pour tout $m = 1, \ldots, n$; on a donc:

$$\max_{m \geq 1} \deg(P'_m Q'_m) = \deg(P'_k Q'_k) = \deg(P_k Q_k) = \max_{m \geq 1} \deg(P_m Q_m).$$

Si $k = j$ alors on peut supposer $\deg(P_j Q_j) > \deg(P_i Q_i)$ (sinon on prend $k = i$ et on s'en remet au raisonnement précédent). Donc, de (3.6) on obtient $\deg(P'_j Q'_j) = \deg(P_j w Q_i + P_j Q_j) = \deg(P_j Q_j)$, puisque $\deg(P_j w Q_i) = \deg(P_i Q_i) < \deg(P_j Q_j)$. On a donc encore une fois $\deg(P'_j Q'_j) = \deg(P_j Q_j) \geq \deg(P_m Q_m)$, pour tout $m = 1, \ldots, n$, d'où $\deg(P'_j Q'_j) \geq \deg(P'_m Q'_m)$, pour tout $m = 1, \ldots, n$. Ainsi:

$$\max_{m \geq 1} \deg(P'_n Q'_n) = \deg(P'_j Q'_j) = \deg(P_j Q_j) = \max_{m \geq 1} \deg(P_n Q_n).$$

Par conséquent,

$$\begin{aligned}
& \deg\left(\textstyle\sum_{m=1}^{n} P'_m Q'_m\right) \\
= \; & \deg\left(\textstyle\sum_{m=1}^{n} P_m Q_m\right) \qquad \text{(en vertu de (3.9))} \\
< \; & \max_{m \geq 1} \deg(P_m Q_m) \\
= \; & \max_{m \geq 1} \deg(P'_m Q'_m).
\end{aligned}$$

La famille de polynômes $P'_1, \ldots, P'_n$ est donc d-dépendante. En vertu du Lemme 3.3.4, on a $\mathcal{V}(P'_1, \ldots, P'_n) < \mathcal{V}(P_1, \ldots, P_n)$. Par récurrence, il est possible de trouver, à l'aide d'un nombre fini de réécritures, une relation de d-dépendance de l'un des P'_m sur les autres membres de la famille de degré n'excédant pas celui de P'_m. On peut ensuite remonter cette relation de dépendance au niveau de la famille initiale $P_1, \ldots, P_n$. ◇

De la Prop. 3.3.7 se dégage un algorithme pour tester si une famille est d-dépendante. Etant donnée une famille $P_1, \ldots, P_n$ de polynômes non nuls, on entreprend le calcul d'une base $\leq$-indépendante de l'idéal qu'elle engendre. A chaque fois qu'une réécriture du type (R3) $P_i \rightarrow P_i - P_j w$ est appliquée, on teste pour savoir si on a abaissé le degré du polynôme P_i. Dans l'affirmative, on peut remonter le long des réécritures pour obtenir la relation de d-dépendance d'un polynôme sur les autres polynômes de la famille. Si le calcul de la base se fait sans que jamais le degré ne soit abaissé, alors on sait que la famille de départ est d-indépendante, puisque l'ordre $\leq$ est compatible avec le degré. ◇

Exemple 3.3.8 Nous allons calculer une base $\leq$-indépendante de l'idéal I, engendré par les polynômes $P_1 = acb + 4b$, $P_2 = ac - 2ab$, $P_3 = abb + 2aa$ et $P_4 = aa - b$.

Le mot $ac = r(P_2)$ est préfixe de $acb = r(P_1)$. On effectue les réécritures:

$$\begin{aligned} P_1 &\rightarrow P_1 - P_2 b = acb + 4b - acb + 2abb = 2abb + 4b, \\ P_1 &\rightarrow \frac{1}{2} P_1 = abb + 2b. \end{aligned}$$

Le nouveau système de générateurs est $P'_1 = abb + 2b$, $P'_2 = P_2 = ac - 2ab$, $P'_3 = P_3 = abb + 2aa$ et $P'_4 = P_4 = aa - b$. P'_1 et P'_3 ont même recteur, abb. On effectue la réécriture:

$$P'_3 \rightarrow P'_3 - P'_1 = abb + 2aa - abb - 2b = 2aa - 2b.$$

Cette fois, on a abaissé le degré, puisque $\deg(P'_3 - P'_1) < \deg(P'_3)$. La famille de départ est donc d-dépendante. La relation de d-dépendance que nous avons calculée, écrite sous la forme (3.8), est:

$$\deg(P_3 - P_1(\frac{1}{2}) - P_2(-\frac{1}{2}b)) < \deg(P_3).$$

Poursuivons le calcul d'une base $\leq$-indépendante de I. On rend le polynôme P'_3 unitaire:

$$P'_3 \rightarrow \frac{1}{2} P'_3 = aa - b,$$

de sorte que le nouveau système de générateurs est $P''_1 = P'_1 = abb + 2b$, $P''_2 = P'_2 = ac - 2ab$, $P''_3 = aa - b$ et $P''_4 = P'_4 = aa - b$. P''_3 et P''_4 ont même recteur aa. On effectue la réécriture:

$$P''_3 \rightarrow P''_3 - P''_4 = 0.$$

On éjecte le polynôme P_3'', puisqu'il est nul. Les recteurs $\{abb, ac, aa\}$ des trois polynômes non nuls P_1'', P_2'', P_4'' forment un code préfixe. Ces polynômes forment donc une base de l'idéal $I = < P_1, P_2, P_3, P_4 >$. ◇

Le prochain corollaire se trouve implicitement démontré chez Cohn [Co 61, Co 69] puisqu'il est aussi une conséquence de l'algorithme faible (pour le degré des polynômes).

Corollaire 3.3.9 *(Théorème du défaut pour les idéaux à droite de type fini.)*
Si n polynômes sont $K<A>$-linéairement dépendants à droite, alors l'idéal à droite qu'ils engendrent est libre de rang $\leq n-1$.

Démonstration. On vérifie facilement que si $P_1, \ldots, P_n$ sont linéairement dépendants alors il en est de même de toute famille obtenue de $P_1, \ldots, P_n$ à l'aide d'une réécriture élémentaire de type (R2) ou (R3). Par conséquent, en appliquant l'algorithme du Th. 3.3.5, à une certaine étape on éjectera un générateur nul à l'aide d'une réécriture du type (R1). ◇

3.4 Bases standards des idéaux à droite.

Soit maintenant un idéal à droite I, quelconque. Nous dirons qu'une famille de mots $\{w_i\}_{i\geq 1}$, finie ou infinie, est *linéairement indépendante* mod I si leurs images $\{\varphi(w_i)\}_{i\geq 1}$ sont linéairement indépendantes dans $K<A>/I$. De façon équivalente, $\{w_i\}_{i\geq 1}$ est linéairement indépendante mod I s'il est impossible de trouver des scalaires $\alpha_i \in K$, presque tous nuls (mais non tous nuls), tels que $\sum_{i\geq 1} \alpha_i w_i \in I$.

Désignons par $[u, v]$ l'*intervalle* des mots compris entre u et v. Plus précisément, $[u, v] = \{w \in A^* : u \leq w \leq v\}$. On définit une suite (finie ou infinie) de mots u_n comme suit:

$$u_1 = \inf\{w \in A^* : [1, w] \text{ est linéairement dépendant mod } I\},$$

et pour $n \geq 2$:

$$u_n = \inf\{w \in A^* - \{u_1, \ldots, u_{n-1}\}A^* : [1, w] \cap (A^* - \{u_1, \ldots, u_{n-1}\}A^*)$$
$$\text{est linéairement dépendant mod } I\}.$$

Il se peut qu'à un certain moment, la famille $\{v\}_{v \in A^* - \{u_1, \ldots, u_{n-1}\}A^*}$ soit linéairement indépendante mod I. Le mot u_n, et les suivants, ne sont alors pas définis.

Remarque 3.4.1 Ainsi, pour obtenir les mots u_n, il faut parcourir l'arbre du monoïde libre selon l'ordre $\leq$. Au début, à chaque mot rencontré, on cherche s'il y a une dépendance K-linéaire parmi ses prédécesseurs. On trouve un premier mot lié à ses prédécesseurs; on détache de l'arbre du monoïde libre le sous-arbre dont il est la racine. On dira que les mots de ce sous-arbre ne sont plus dans l'arbre de départ. On continue le parcours de l'arbre dans l'ordre, en s'arrêtant à chaque mot qui est encore dans l'arbre de départ. A chaque fois, on cherche une dépendance K-linéaire qui lie un mot à ses prédécesseurs qui sont encore dans l'arbre. Cette description géométrique de la définition des mots u_n, illustre le fait que la famille de mots $\{u_n\}$ forme un code préfixe, puisque jamais deux mots u_i ne se trouveront le long d'une même branche de l'arbre (voir Rem. 3.2.2). C'est ce que montre le lemme qui suit. ◇

Lemme 3.4.2 *La famille de mots $\{u_n\}_{n\geq 1}$ est un code préfixe qui satisfait $u_i < u_j$ si $i < j$.*

Démonstration. Nous montrons par récurrence sur n, que les mots $u_1, \ldots, u_n$ forment un code préfixe et que $u_1 < \ldots < u_n$. Il n'y a rien à montrer pour $n = 1$.

Soit $n \geq 1$. Supposons que les mots $u_1, \ldots, u_n$ forment un code préfixe satisfaisant $u_1 < \ldots < u_n$. Comme $u_{n+1} \in (A^* - \{u_1, \ldots, u_n\}A^*)$, aucun des mots $u_1, \ldots, u_n$ n'est préfixe de u_{n+1}; en particulier, $u_n \neq u_{n+1}$.

Nous allons montrer que $u_n < u_{n+1}$. On saura alors, en vertu de (3.2), que u_{n+1} n'est pas préfixe de $u_1, \ldots, u_n$. Supposons qu'au contraire $u_{n+1} < u_n$. On sait alors, par (3.2), que $[1, u_{n+1}] \cap u_n A^* = \emptyset$. Par conséquent,

$$[1, u_{n+1}] \cap (A^* - \{u_1, \ldots, u_n\}A^*) = [1, u_{n+1}] \cap (A^* - \{u_1, \ldots, u_{n-1}\}A^*).$$

Or, par définition de u_{n+1}, le membre gauche de cette égalité est linéairement dépendant mod I. Un coup d'oeil au membre droit nous permet de constater que l'on contredit la minimalité du mot u_n. On a donc $u_n < u_{n+1}$ et le lemme est montré. ◇

Posons pour la suite $X_n = \{u_1, \ldots, u_{n-1}\}$ et $X = \{u_n\}_{n\geq 1}$. Par définition, pour chaque n il existe une relation, qui définit un polynôme de l'idéal I:

$$P_n = u_n + \sum_{\substack{v < u_n \\ v \in A^* - X_n A^*}} (P_n, v)v \quad \in I.$$

En vertu du Lemme 3.4.2, les recteurs des polynômes P_n sont distincts deux à deux et forment un code préfixe. Par conséquent, selon le Th. 3.2.11, la famille $\{P_n\}_{n\geq 1}$ est indépendante; elle est une base du $K\langle A\rangle$-module (ou de façon équivalente de l'idéal) qu'elle engendre.

Remarques 3.4.3 (i) L'ensemble de mots $A^* - XA^*$ est l'*ensemble préfixiel* qui correspond à X. C'est l'ensemble formé des mots qu'ils restent dans l'arbre de A^* une fois qu'on y a détaché les sous-arbres dont la racine est un mot du code X.

(ii) Soit $v < u_n$. Si $v \in A^* - XA^*$ alors on a $v \in A^* - X_nA^*$ en vertu de l'inclusion $X_n \subset X$. Inversement, si $v \in A^* - X_nA^*$ alors on a $v \in A^* - XA^*$. En effet, supposons qu'au contraire on ait $v = u_m w$ pour $m \geq n$ et $w \in A^*$. On trouve (en utilisant les conditions (3.1) et (3.2)), $u_n \leq u_n w \leq u_m w = v$, puisque $u_n \leq u_m$, selon le Lemme 3.4.2. On contredit ainsi l'inégalité $v < u_n$.

(iii) Ainsi, les polynômes P_n sont aussi égaux à:

$$P_n = u_n + \sum_{\substack{v<u_n \\ v\in A^*-XA^*}} (P_n, v)v.$$

◇

Lemme 3.4.4 *Supposons que soit donné l'idéal à droite I, et le code préfixe X. Soit $R \in K<A>$. Alors il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls, et une famille de scalaires $\{\alpha_v\}_{v\in A^*-XA^*}$ presque tous nuls, tels que R puisse s'écrire sous la forme:*

$$R = \sum_{n\geq 1} P_nQ_n + \sum_{v\in A^*-XA^*} \alpha_v v.$$

Démonstration. Il suffit de montrer le lemme dans le cas où R est un mot $w \notin A^* - XA^*$. On a alors $w = u_k w'$ et on procède par récurrence sur la longueur du mot w'. Le cas $|w'| = 0$ est donné par la relation qui définit P_k. Sinon, on a:

$$u_k w' = P_k w' - \sum_{\substack{v<u_k \\ v\in A^*-X_kA^*}} (P_k, v)vw'.$$

Les mots vw' qui apparaîssent dans la somme de droite sont soit des mots de $A^* - XA^*$, soit ils sont de la forme $vw' = u_j w''$ avec $|w''| < |w'|$, car $v < u_k$ et $v \in A^* - X_kA^*$ impliquent $v \in A^* - XA^*$, comme on a vu à la Rem. 3.4.3 (i). On conclut par récurrence. ◇

Lemme 3.4.5 *La famille de mots $\{v\}_{v\in A^*-XA^*}$ est linéairement indépendante mod I.*

Démonstration. Dans le cas où $X = \{u_1, \ldots, u_n\}$ est fini, le résultat est évident: le mot u_{n+1} n'est pas défini précisément parce que la famille $\{v\}_{v\in A^*-XA^*}$ est linéairement indépendante mod I.

Il reste donc à considérer le cas où X est infini. Supposons qu'au contraire il existe des scalaires α_v, presque tous nuls, tels que $\sum_v \alpha_v v = 0 \bmod I$. Soit:

$$u_i = \inf\{u_n : u_n > v \text{ pour tout } v \text{ tel que } \alpha_v \neq 0\}.$$

On voit donc, en s'aidant de la Rem. 3.4.3 (i), que les mots $v \in \sum_v \alpha_v v$ sont des mots de $A^* - X_i A^*$, plus petit que u_i, de sorte que la relation $\sum_v \alpha_v v = 0 \bmod I$ contredit la minimalité de u_i. ◇

Proposition 3.4.6 *La famille de polynômes $\{P_n\}_{n\geq 1}$ engendre l'idéal I.*

Démonstration. Soit R un polynôme de I. Selon le Lemme 3.4.4, il existe une famille de polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls, et une famille de scalaires $\{\alpha_v\}_{v\in A^*-XA^*}$ presque tous nuls, tels que

$$R = \sum_{n\geq 1} P_n Q_n + \sum_{v\in A^*-XA^*} \alpha_v v.$$

Par conséquent,

$$0 = \varphi(R) = \sum_{v\in A^*-XA^*} \alpha_v \varphi(v).$$

On en déduit que $\alpha_v = 0$ pour tout v, en vertu du Lemme 3.4.5. Donc, $R = \sum_{n\geq 1} P_n Q_n$ et la famille $\{P_n\}_{n\geq 1}$ engendre l'idéal I. ◇

Corollaire 3.4.7 *L'idéal I est de type fini si et seulement si le code préfixe X est fini. De plus, l'idéal I est de codimension finie si et seulement si le code préfixe X est fini et complet.*

Démonstration. La proposition montre que si l'ensemble X est fini alors I est finiment engendré. Nous serons en mesure de montrer la réciproque plus loin (Th. 3.4.9). Pour la deuxième partie de l'énoncé, il faut remarquer que si le code est fini et complet alors la famille de mots $A^* - XA^*$ est finie. Le corollaire découle aussi des théorèmes de Cohn [Co 69]. ◇

Nous allons maintenant montrer que la famille $\{P_n\}_{n\geq 1}$ est unique.

Théorème 3.4.8 *Soit $\{P'_n\}_{n\geq 1}$ une famille indépendante de polynômes, de recteurs respectifs $\{u'_n\}_{n\geq 1}$, satisfaisant $u'_i < u'_j$ si $i < j$. Posons $X'_n = \{u'_1, \ldots, u'_{n-1}\}$ et supposons que:*

$$P'_n = u'_n + \sum_{\substack{v<u'_n \\ v\in A^*-X'_nA^*}} (P'_n, v)v.$$

Si la famille $\{P'_n\}_{n\geq 1}$ engendre le même idéal I que la famille $\{P_n\}_{n\geq 1}$ alors $P_n = P'_n$, pour tout n.

Démonstration. On procède par récurrence sur k pour montrer que $u_k = u'_k$ et que $P_k = P'_k$.

Le polynôme P'_1 nous donne une relation K-linéaire (mod I) dans l'intervalle de mots $[1, u'_1]$. On doit donc avoir $u_1 \leq u'_1$ en vertu de la définition de u_1. Comme $\{P'_n\}_{n\geq 1}$ engendre I, il existe des polynômes Q'_n, presque tous nuls, tels que $P_1 = \sum_{n\geq 1} P'_n Q'_n$. Selon la remarque 3.2.10, $r(\sum_{n\geq 1} P'_n Q'_n) = u'_i v'_i$ pour un certain i et un certain $v'_i \in Q'_i$. On a donc $u_1 = r(P_1) = u'_i v'_i$. On en tire $u'_i \leq u_1$. Par suite, on a $u_1 \leq u'_1 \leq u'_i \leq u_1$; donc $u_1 = u'_1$. On peut en conclure que $P'_1 = P_1$ puisque la famille de mots $[1, u_1] - \{u_1\}$ est linéairement indépendante mod I.

Supposons qu'on ait montré que $u_1 = u'_1, \ldots, u_{k-1} = u'_{k-1}$ et que $P_1 = P'_1, \ldots, P_{k-1} = P'_{k-1}$. On a donc $X_k = X'_k$ et le même argument que dans le cas $k = 1$ montre qu'on doit avoir $u_k \leq u'_k$. Comme $P_k \in I$ il existe des polynômes Q'_n, presque tous nuls, tels que $P_k = \sum_{n\geq 1} P'_n Q'_n$. Mais alors $u_k = r(P_k) = r(\sum_{n\geq 1} P'_n Q'_n)$. Selon la Rem. 3.2.10, $r(\sum_{n\geq 1} P'_n Q'_n) = u'_i v'_i$ pour un certain i et un certain $v'_i \in Q'_i$. On a donc $u_k = u'_i v'_i$ et on en tire $u'_i \leq u_k \leq u'_k$. Maintenant, regardons comment se comparent les indices i et k. Le cas $i > k$ est exclu car, par hypothèse, $u_i \leq u_k$ implique $i \leq k$. Donc, on a soit $i = k$ et alors $u_k = u'_k$; soit $i < k$ de sorte que, par récurrence, $u'_i = u_i$. Mais alors c'est que $u_k = u_i v'_i$ ce qui contredit le fait que $\{u_n\}_{n\geq 1}$ est un code préfixe. On doit donc avoir $u_k = u'_k$.

On conclut à l'égalité $P'_k = P_k$ en vertu du fait que les mots de $A^* - X_k A^*$ sont linéairement indépendants mod I. ◇

La base $\{P_n\}_{n\geq 1}$ de l'idéal I sera appelée *la base standard de* I. On dira aussi qu'une famille est standard si elle est la base standard de l'idéal qu'elle engendre. Remarquez que la famille vide est la base standard de l'idéal nul et la famille $\{1\}$ est la base standard de l'algèbre toute entière.

Théorème 3.4.9 *Soit $P_1, \ldots, P_n$ une famille indépendante. Il est possible de calculer, à l'aide d'une suite finie de réécritures élémentaires, la base standard de l'idéal $I = < P_1, \ldots, P_n >$. De plus, le code préfixe associé à la base standard de I est égal au code préfixe associé à $P_1, \ldots, P_n$.*

Démonstration. Supposons les polynômes P_m unitaires. Soient $u_i = r(P_i)$ et $X = \{u_1, \ldots, u_n\}$. On construit d'abord un outil de récurrence pour la démonstration du théorème. On définit le multi-indice $\overline{\mathcal{V}} = \overline{\mathcal{V}}(P_1, \ldots, P_n) = (\varrho_w)_{w\in XA^*}$, en posant $\varrho_w = |\{i : w \in P_i, w \neq r(P_i)\}|$, pour tout $w \in XA^*$. L'entier ϱ_w compte donc le nombre de polynômes dans lesquels le mot $w \in XA^*$ apparaît, sans en être le recteur. On ordonne ces multi-indices selon l'ordre lexicographique inverse (comme on l'a fait plus haut pour les multi-indices des recteurs). Nous allons montrer le théorème par récurrence sur $\overline{\mathcal{V}}(P_1, \ldots, P_n)$.

Si $\overline{V}(P_1, \ldots, P_n)$ est nul alors la base est standard. Sinon, il existe $w \in XA^*$ et i tels que $w \in P_i$ et $w \neq r(P_i)$. Comme $w < u_i$, la condition (3.2) nous assure que $w = u_j v$ pour un $j \neq i$. Posons $P_i' = P_i - (P_i, w)P_j v$, et $P_m' = P_m$, pour $m \neq i$. On a $(P_i', w) = 0$. De plus, si $w' \in P_j v$ et $w' \neq w$, alors $w' < w$. En effet, tous ces mots sont de la forme sv avec $s < u_j$. Donc, par (3.1), $w' = sv < u_i v = w$.

D'une part cela montre que $r(P_m') = r(P_m)$ pour tout $m \geq 1$. De sorte que la famille P_1', $\ldots$, P_n' est indépendante et X est son code préfixe associé. Nous sommes donc en mesure de comparer $\overline{V}(P_1', \ldots, P_n')$ et $\overline{V}(P_1, \ldots, P_n)$. D'autre part, notre raisonnement montre aussi que $\overline{V}(P_1', \ldots, P_n') < \overline{V}(P_1, \ldots, P_n)$. Par récurrence il est possible, à l'aide d'une suite finie de réécritures élémentaires, de calculer la base standard de l'idéal engendré par la famille $P_1', \ldots, P_n'$. Cette base standard aura aussi X comme code préfixe associé. Le théorème est montré, puisque selon le Lemme 3.3.2, les deux familles $P_1, \ldots, P_n$ et $P_1', \ldots, P_n'$ engendrent le même idéal. ◇

Exemple 3.4.10 Nous allons calculer la base standard de l'idéal engendré par les polynômes (indépendants) $P_1 = aab - 2bc$, $P_2 = ac + 2ab$ et $P_3 = b - 2a$. On a $bc \in P_1$ et $bc = r(P_3)c$. On applique la réécriture:

$$P_1 \to P_1 + 2P_3c = aab - 2bc + 2bc - 4ac = aab - 4ac.$$

La nouvelle base de l'idéal est formée des polynômes $Q_1 = aab - 4ac$, $Q_2 = ac + 2ab$ et $Q_3 = b - 2a$. On a $ac \in Q_1$ et $ac = r(Q_2)$. On applique la réécriture:

$$Q_1 \to Q_1 + 4Q_2 = aab - 4ac + 4ac + 8ab = aab + 8ab.$$

La nouvelle base $R_1 = aab + 8ab$, $R_2 = ac + 2ab$, $R_3 = b - 2a$ est standard. ◇

Le Th. 3.4.8 et le Th. 3.4.9 s'unissent pour nous donner le corollaire suivant.

Corollaire 3.4.11 *Il est possible de tester si deux ensembles finis de polynômes engendrent le même idéal.*

Démonstration. En effet, on a montré au Th. 3.4.9, qu'il est possible de calculer la base standard d'un idéal. Il est donc possible, étant donné deux familles finies de polynômes, de calculer les bases standard des idéaux qu'elles engendrent et de les comparer. On conclut à l'égalité des idéaux seulement dans le cas où ces bases standard sont identiques, en vertu de l'unicité de la base standard (Th. 3.4.8). ◇

Corollaire 3.4.12 *Soient Q et $P_1, \ldots, P_n \in K\langle A\rangle$ tels que $P_1, \ldots, P_n$ est la base standard de l'idéal I qu'ils engendrent. Il est possible de calculer l'image de Q dans la base $A^* - XA^*$ du K-module $K\langle A\rangle/I$. En particulier, il est possible de tester si $Q \in < P_1, \ldots, P_n >$.*

Démonstration. On a montré au Lemme 3.4.5, que la famille de mots $A^* - XA^*$ est linéairement indépendante mod I. C'est bien dire que ces mots forment une base du K-module $K<A>/I$.

Le polynôme P_i est unitaire, pour tout i. On pose, comme plus haut, $u_i = r(P_i)$, $X = \{u_1, \ldots, u_n\}$ et on désigne par $\varphi : K<A> \to K<A>/I$ le morphisme canonique. On procède par récurrence sur le recteur de Q.

Cas 1. Si $Q = 0$, alors $\varphi(Q) = 0$ et $Q \in I$.

Sinon, soit $w = r(Q)$.
Cas 2. Si $w \in (A^* - XA^*)$, on a:

$$\varphi(Q) = (Q, w)w + \varphi(Q - (Q, w)w).$$

Par récurrence, on peut calculer l'image de $Q - (Q, w)w$ et terminer le calcul de l'image de Q.
Cas 3. Si $w \in XA^*$,
il existe $u_i \in X$ et $v \in A^*$ tels que $w = u_i v$. On a, d'après le Lemme 3.2.5, $r(Q - (Q, w)P_i v) < r(Q)$. Comme:

$$\begin{aligned} \varphi(Q) &= \varphi(Q - (Q, w)P_i v) + \varphi((Q, w)P_i v)) \\ &= \varphi(Q - (Q, w)P_i v) + 0 \\ &= \varphi(Q - (Q, w)P_i v), \end{aligned}$$

on peut calculer l'image de $Q - (Q, w)P_i v$ et terminer le calcul.

Comme la famille de mots $A^* - XA^*$ est linéairement indépendante mod I, on saura que le polynôme Q est dans I si et seulement si après un certain moment, on trouve le polynôme nul. ◇

3.5 $K<A>$-modules à droite et $\leq$-dépendance à droite.

Nous considérons maintenant le $K<A>$-module à droite $K<A>^q$, où q est un entier positif, $q \geq 1$. Les éléments de $K<A>^q$ sont des *vecteurs colonnes* V formés de q polynômes de $K<A>$:

$$V = \begin{pmatrix} P_1 \\ \vdots \\ P_q \end{pmatrix}.$$

Pour cette raison, nous appellerons les éléments de $K<A>^q$ des *vecteurs de polynômes*, ou simplement des *vecteurs*. Nous allons nous intéresser aux *sous-$K<A>$-modules à droite* de $K<A>^q$. Par la suite, nous abrégerons l'expression '*sous-$K<A>$-module à*

droite' simplement par *sous-module*. Dans le cas où $q = 1$, un sous-module de $K\langle A\rangle^q$ n'est rien d'autre qu'un idéal à droite de $K\langle A\rangle$. Nous serons donc en mesure d'utiliser une récurrence sur q afin d'étendre les résultats des paragraphes précédents.

Nous désignons par π_i, pour $i = 1, \ldots, q$, la projection canonique des vecteurs sur leur $i^{\text{ème}}$ composante:

$$\begin{aligned} \pi_i : K\langle A\rangle^q &\to K\langle A\rangle \\ V &\mapsto P_i \end{aligned}$$

Nous introduisons aussi les projections π (resp. $\overline{\pi}$) : $K\langle A\rangle^q \to K\langle A\rangle^{q-1}$ qui oublient la première (resp. dernière) composante des vecteurs:

$$\pi(V) = \begin{pmatrix} P_2 \\ \vdots \\ P_q \end{pmatrix}, \qquad \overline{\pi}(V) = \begin{pmatrix} P_1 \\ \vdots \\ P_{q-1} \end{pmatrix}.$$

La multiplication à droite d'un vecteur V par un polynôme $Q \in K\langle A\rangle$ s'exprime donc par $\pi_i(VQ) = \pi_i(V)Q$. Nous désignerons par ι le plongement:

$$\begin{aligned} \iota : K\langle A\rangle^{q-1} &\to K\langle A\rangle^q \\ V = \begin{pmatrix} P_1 \\ \vdots \\ P_{q-1} \end{pmatrix} &\mapsto \begin{pmatrix} 0 \\ P_1 \\ \vdots \\ P_{q-1} \end{pmatrix}, \end{aligned}$$

qui ajoute une première composante nulle; i.e. $\pi_1(\iota(V)) = 0$, $\pi_{k+1}(\iota(V)) = \pi_k(V)$, pour $k = 1, \ldots, q-1$. On a donc, d'une part $\pi \circ \iota = id$, et d'autre part, $\iota \circ \pi(V) = V$ si $\pi_1(V) = 0$. Ces applications sont toutes $K\langle A\rangle$-linéaires.

Soient $\{V_n\}_{n\geq 1}$ une famille de vecteurs et $\{Q_n\}_{n\geq 1}$ une famille de *polynômes* presque tous nuls. Alors les vecteurs V_nQ_n sont presque tous nuls et on peut former la somme $\sum_{n\geq 1} V_nQ_n$. Soit N un ensemble d'indices. Nous dirons qu'une famille $E_1, \ldots, E_q$ de q sous-ensembles de N est une *partition en q blocs* de la famille $\{V_n\}_{n\in N}$ si pour tout $i \in N$, il existe un unique k tel que $i \in E_k$; c'est-à-dire:

$$E_{k_1} \cap E_{k_2} = \emptyset \quad \text{pour } (k_1 \neq k_2) \quad \text{et} \quad \bigcup_{k=1}^{q} E_k = N.$$

Par la suite, nous abrégerons l'expression '*partition en q blocs*' à *partition*. Notez que certains blocs de la partition peuvent être vides. Etant donné une famille de vecteurs *non nuls* $\{V_n\}_{n\geq 1}$ il existe une unique partition $E_1, \ldots, E_q$ telle que $V_i \in E_k$ implique:

$$\pi_j(V_i) = 0 \quad \text{pour } j = 1, \ldots, k-1 \quad \text{et} \quad \pi_k(V_i) \neq 0.$$

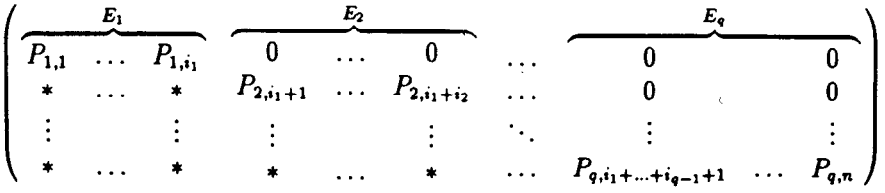

Figure 3.2: Partition associée à une famille finie de vecteurs.

Cette partition sera appelée *la partition associée à la famille* $\{V_n\}_{n\geq 1}$. Dans le cas où la famille $V_1, \ldots, V_n$ est finie, ces conditions se visualisent facilement. Après avoir réindicé la famille on peut placer les vecteurs côte-à-côte pour former une matrice $q \times n$, réduite-échelonnée. On fait apparaître la partition associée à la famille de vecteurs en localisant les blocs rectangulaires d'entrées nulles dans la matrice (voir Fig. 3.2).

Remarques 3.5.1 Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs non nuls de $K\langle A\rangle^q$ et E_1, $\ldots$, E_q sa partition associée.

(i) Alors $E'_k = E_{k+1}$ $(k = 1, \ldots, q-1)$, est la partition associée à la famille de vecteurs $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$.

(ii) La partition $E_1, \ldots, E_{q-1}$ est la partition associée à la famille $\{\overline{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$.

(iii) La famille $\{\iota(V_n)\}_{n\geq 1}$, a pour partition associée $E'_1 = \emptyset$, $E'_k = E_{k-1}$ $(k = 2, \ldots, q+1)$.

(iv) Supposons que, de plus, on ait $\pi_1(V_n) \neq 0$ pour tout $n \geq 1$. La partition associée à la famille $\{V_n\}_{n\geq 1}$ est donc réduite à un seul bloc E_1. Si $\{U_n\}_{n\geq 1}$ est une famille de $K\langle A\rangle^{q-1}$ de partition associée $E'_1, \ldots, E'_{q-1}$, alors la partition associée à la famille $\{\iota(U_n)\}_{n\geq 1} \cup \{V_n\}_{n\geq 1}$ est $E''_1 = E_1$, $E''_k = E'_{k-1}$ $(k = 2, \ldots, q)$. ◇

Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs non nuls et $E_1, \ldots, E_q$ la partition qui lui est associée. Nous dirons que cette famille est *$\leq$-indépendante à droite* si pour tout $k = 1, \ldots, q$, la famille de *polynômes* $\{\pi_k(V_i)\}_{i\in E_k}$ est $\leq$-indépendante à droite. Notez que certains des blocs peuvent être vide, puisqu'une famille vide (de polynômes) est indépendante (Rem. 3.2.7). Dans le cas où la famille de vecteurs n'est pas vide, les blocs E_k de la partition ne peuvent être tous vides puisque les vecteurs sont non nuls. Par la suite, nous abrégerons l'expression '*$\leq$-indépendante à droite*' simplement par *indépendante*.

Remarque 3.5.2 Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs de $K\langle A\rangle^q$, telle que la famille de polynômes $\{\pi_1(V_n)\}_{n\geq 1}$ est indépendante. Alors la famille de vecteurs $\{V_n\}_{n\geq 1}$ est elle-même indépendante. ◇

Remarques 3.5.3 Soit $\{V_n\}_{n\geq 1}$ une famille indépendante de vecteurs de $K\langle A\rangle^q$.

(i) Alors on constate facilement, à l'aide des Rem. 3.5.1 (i), (ii) et (iii), que les familles de vecteurs $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$, $\{\overline{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$ et $\{\iota(V_n)\}_{n\geq 1}$ sont indépendantes.

(ii) Supposons que, de plus, on ait $\pi_1(V_n)\neq 0$ pour tout $n\geq 1$. Si $\{U_n\}_{n\geq 1}$ est une famille indépendante de $K\langle A\rangle^{q-1}$, alors on vérifie, à l'aide de la Rem. 3.5.1 (iv), que la famille de vecteurs $\{\iota(U_n)\}_{n\geq 1}\cup\{V_n\}_{n\geq 1}$ est indépendante. ◇

Théorème 3.5.4 *Soit $\{V_n\}_{n\geq 1}$ une famille indépendante de vecteurs. Alors elle est $K\langle A\rangle$-linéairement indépendante.*

Démonstration. On procède par récurrence sur q. On a vu à la Rem. 3.3.3 qu'une famille indépendante de *polynômes* est une famille $K\langle A\rangle$-linéairement indépendante de $K\langle A\rangle$. Par conséquent, le résultat est vrai pour $q=1$. On suppose donc $q\geq 2$.

Imaginons qu'au contraire les vecteurs V_n ne soient pas $K\langle A\rangle$-linéairement indépendants. Il existe alors des polynômes $\{Q_n\}_{n\geq 1}$ presque tous nuls (mais non tous nuls) tels que:

$$\sum_{n\geq 1} V_n Q_n = 0.$$

On déduit de la relation précédente, par application de π, la relation:

$$\pi(\sum_{n\geq 1} V_n Q_n) = \sum_{n\geq 1}\pi(V_n)Q_n = 0.$$

Soit $E_1, \ldots, E_q$ la partition associée à la famille de vecteurs $\{V_n\}_{n\geq 1}$. Les vecteurs de $K\langle A\rangle^{q-1}$, $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$, sont indépendants, en vertu de la Rem. 3.5.3 (i). Par récurrence, ils sont aussi $K\langle A\rangle$-linéairement indépendants. Si E_1 est vide alors on a $\iota\circ\pi(V_n)=V_n$ (pour tout n) et on conclut à l'indépendance $K\langle A\rangle$-linéaire de la famille. Sinon, c'est que les polynômes $\{Q_n\}_{n\geq 1, n\in E_1}$ ne peuvent être tous nuls. Mais alors on obtient, par application de π_1, une relation de dépendance $K\langle A\rangle$-linéaire en première composante:

$$\pi_1(\sum_{n\geq 1} V_n Q_n) = \sum_{n\in E_1}\pi_1(V_n)Q_n = 0.$$

On contredit là l'indépendance des polynômes $\{\pi_1(V_n)\}_{n\geq 1, n\in E_1}$. La famille de vecteurs $\{V_n\}_{n\geq 1}$ est donc $K\langle A\rangle$-linéairement indépendante. ◇

On peut définir, comme au paragraphe 3.3, des *réécritures élémentaires* de systèmes de vecteurs. Soient $V_1, \ldots, V_n$ une famille de vecteurs. On définit trois types de 'réécritures élémentaires':

(R_q1) si $V_i = 0$, on permet la réécriture:

$$V_1, \ldots, V_n \to V_1, \ldots, V_{i-1}, V_{i+1}, \ldots, V_n,$$

(R_q2) pour $\alpha \in K, \alpha \neq 0$, on permet la réécriture:

$$V_1, \ldots, V_n \rightarrow V_1, \ldots, V_{i-1}, \alpha V_i, V_{i+1}, \ldots, V_n$$

(R_q3) s'il existe k $(1 \leq k \leq q)$, $i \neq j$, et $r(\pi_k(V_j w)) = r(\pi_k(V_j))w \leq r(\pi_k(V_i))$, on permet la réécriture:

$$V_1, \ldots, V_n \rightarrow V_1, \ldots, V_{i-1}, V_i', V_{i+1}, \ldots, V_n$$

où $V_i' = V_i - V_j w$.

Remarque 3.5.5 Les règles ($R_q i$) et ($R_{q-1} i$) sont liées (les règles ($R_1 i$) ne sont autres que celles introduites au paragraphe 3.3). En effet, soient $V_1, \ldots, V_n$ des vecteurs de $K\langle A\rangle^{q-1}$. Alors on peut, de façon équivalente, soit appliquer une règle ($R_{q-1} i$) à ce système, soit plonger les vecteurs dans $K\langle A\rangle^q$: $\iota(V_1), \ldots, \iota(V_n)$, appliquer la règle correspondante ($R_q i$), et revenir à $K\langle A\rangle^{q-1}$ à l'aide de π, puisqu'on a $\pi \circ \iota = id$.

De même, soient V_k des vecteurs de $K\langle A\rangle^q$ qui satisfont $\pi_1(V_k) = 0$, pour tout k. Alors on peut passer dans $K\langle A\rangle^{q-1}$ (à l'aide de π), appliquer une règle ($R_{q-1} i$) à ce système et revenir dans $K\langle A\rangle^q$ à l'aide de ι, en vertu du fait que $\iota \circ \pi(V_k) = V_k$, pour tout k.◇

On obtient évidemment un analogue du Lemme 3.3.2.

Lemme 3.5.6 *Soient $U_1, \ldots, U_n$ et $V_1, \ldots, V_m$ deux familles de vecteurs. Si la famille $V_1, \ldots, V_m$ peut être obtenue de la famille $U_1, \ldots, U_n$ par une suite finie de réécritures élémentaires alors elles engendrent le même sous-module de $K\langle A\rangle^q$.* ◇

Théorème 3.5.7 *Soit $\mathcal{M}$ un sous-module de $K\langle A\rangle^q$ engendré par les vecteurs $V_1, \ldots, V_n$. Il est possible de calculer une base indépendante de $\mathcal{M}$ en effectuant une suite finie de réécritures élémentaires sur la famille $V_1, \ldots, V_n$.*

Le lecteur tirera avantage à imaginer les vecteurs $V_1, \ldots, V_n$ disposés dans une matrice, comme nous l'avons fait plus haut (voir Fig. 3.2). La démonstration s'inspire de l'algorithme de Gauss-Jordan pour mettre une matrice sous la forme réduite-échelonnée.

Démonstration. On peut, à l'aide de réécritures du type (R_q1), éjecter les vecteurs nuls. On supposera donc que les vecteurs V_i sont tous non nuls. Soit $E_1, \ldots, E_q$ la partition associée aux générateurs de $\mathcal{M}$. On procède par récurrence sur q, le cas $q = 1$ ayant été traité au Th. 3.3.5.

Supposons d'abord que $E_1 = \emptyset$. Alors on a $\pi_1(V_n) = 0$, pour tout $n \geq 1$, de sorte que

$$\iota \circ \pi(\mathcal{M}) = \mathcal{M}. \tag{3.10}$$

Par récurrence, il est possible de calculer, à l'aide de réécritures élémentaires ($R_{q-1}i$), une base indépendante du sous-module (de $K<A>^{q-1}$) engendré par les vecteurs $\{\pi(V_n)\}_{n\geq 1}$. On peut remonter cette base à l'aide de ι, pour obtenir une base indépendante de $\mathcal{M}$, en vertu de (3.10) et de la Rem. 3.5.3 (i). De plus, cette base peut être calculée par une suite finie de réécritures élémentaires ($R_q i$), en vertu de la Rem. 3.5.5.

Supposons maintenant que $E_1 \neq \emptyset$. Par récurrence, il est possible de calculer, à l'aide de réécritures ($R_1 i$), une base indépendante du sous-module engendré par la famille de polynômes $\{\pi_1(V_i)\}_{i\in E_1}$. Ces règles de réécritures peuvent être simulées sur les vecteurs $\{V_i\}_{i\in E_1}$, en appliquant les règles de réécritures ($R_q i$) correspondantes. Ces réécritures donnent lieu, en vertu de la Rem. 3.5.2, à une famille indépendante de vecteurs $\{V'_i\}_{i\in E'_1}$, ($E'_1 \subset E_1$), tels que $\pi_1(V'_i) \neq 0$, et à d'autres vecteurs $\{U_j\}_{j\in E_1\setminus E'_1}$ tels que $\pi_1(U_i) = 0$.

Soient $\mathcal{M}_1$ le sous-module de $\mathcal{M}$ de base $\{V'_i\}_{i\in E'_1}$ et $\mathcal{M}_2$ le sous-module de $\mathcal{M}$ engendré par la famille $\{U_j\}_{j\in E_1\setminus E'_1} \cup \{V_i\}_{i\notin E_1}$. Chacun des vecteurs V de cette famille satisfait $\pi_1(V) = 0$ et par conséquent, on a:

$$\iota \circ \pi(\mathcal{M}_2) = \mathcal{M}_2. \tag{3.11}$$

De plus, $\mathcal{M}_1$ et $\mathcal{M}_2$ sont supplémentaires:

$$\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2. \tag{3.12}$$

Par récurrence, on peut calculer une base indépendante $\{U'_j\}_{j\in E'}$ du sous-module $\pi(\mathcal{M}_2)$ engendré par la famille de vecteurs $\{\pi(U_j\}_{j\in E_1\setminus E'_1} \cup \{\pi(V_i)\}_{i\notin E_1}$, à l'aide de réécritures élémentaires ($R_{q-1}i$).

Par application de ι on obtient une base indépendante de $\mathcal{M}_2$, $V'_j = \iota(U'_j)$ ($j \in E'$), en vertu de (3.11) et de la Rem. 3.5.3 (i). De plus, cette base de $\mathcal{M}$ peut être calculée par une suite finie de réécritures élémentaires ($R_q i$), en vertu de la Rem. 3.5.5. La réunion des bases indépendantes des sous-modules $\mathcal{M}_1$ et $\mathcal{M}_2$ nous donne une base de $\mathcal{M}$, en vertu de (3.12). Cette base est indépendante, en vertu de la Rem. 3.5.3 (ii). ◇

Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs indépendants de $K<A>^q$, de partition associée $E_1, \ldots, E_q$. Posons, pour $k = 1, \ldots, q$, $X_k = \emptyset$ si $E_k = \emptyset$ et $X_k = \{r(\pi_k(V_i))\}_{i\in E_k}$, sinon. Dans le deuxième cas, X_k est *le code préfixe associé* à la famille de polynômes $\{\pi_k(V_i)\}_{i\in E_k}$. Nous dirons que les parties $X_k \subset A^*$ sont *les codes préfixes associés* à la famille $\{V_n\}_{n\geq 1}$. Une fois le calcul d'une base indépendante terminé, on peut poursuivre le travail sur chaque composante, et utiliser le calcul des bases standard des idéaux (Th. 3.4.9) pour montrer le corollaire suivant.

Corollaire 3.5.8 *Soit $V_1, \ldots, V_n$ une famille de vecteurs indépendants, $E_1, \ldots, E_q$ sa partition associée et $X_1, \ldots, X_q$ ses codes préfixes associés. Il est possible de calculer, à l'aide de réécritures élémentaires, une base indépendante $V'_1, \ldots, V'_n$ avec partition associée $E_1, \ldots, E_q$ et codes préfixes associés $X_1, \ldots, X_q$ et telle que chacune des familles de polynômes $\{\pi_k(V'_i)\}_{i\in E_k}$ soit standard.* ◇

Exemple 3.5.9 Ainsi, pour calculer la base indépendante d'un sous-module, on travaille sur les générateurs composante par composante. On construit pour les vecteurs du $k^{\text{ème}}$ bloc, une base indépendante de l'idéal de polynômes engendrés par les polynômes en composante k de ces vecteurs. Soient les vecteurs:

$$V_1 = \begin{pmatrix} abc+2b \\ abbc+2bc+2ac \\ 0 \end{pmatrix}, V_2 = \begin{pmatrix} ab-2a \\ abb+4a \\ cba \end{pmatrix}, V_3 = \begin{pmatrix} ac+b \\ 6abc+bc+1 \\ a+b \end{pmatrix},$$

$$V_4 = \begin{pmatrix} 0 \\ 3abc+2bc-1 \\ c+2a \end{pmatrix}, V_5 = \begin{pmatrix} 0 \\ 0 \\ c+2a \end{pmatrix}.$$

Nous allons calculer une base indépendante du sous-module qu'ils engendrent. La partition associée à notre famille de vecteurs est $E_1 = \{1,2,3\}$, $E_2 = \{4\}$ et $E_3 = \{5\}$. On dispose les vecteurs dans une matrice; les réécritures élémentaires correspondront à effectuer des opérations élémentaires sur les colonnes de la matrice. On désignera la colonne i de la matrice par C_i et on écrira les réécritures élémentaires ($R_5 2$) et ($R_5 3$) sous la forme: $C_i \to \alpha C_i$ ($\alpha \neq 0$) et $C_i \to C_i - C_j w$ $(i \neq j,\ w \in A^*)$.

$$\begin{pmatrix} abc+2b & ab-2a & ac+b & 0 & 0 \\ abbc+2bc+2ac & abb+4a & 6abc+bc+1 & 3abc+2bc-1 & 0 \\ 0 & cba & a+b & c+2a & c+2a \end{pmatrix}$$

On calcule d'abord une base indépendante de l'idéal engendré par les polynômes en première composante des vecteurs du blocs E_1. On effectue les réécritures $C_1 \to C_1 - C_2 c$, $C_1 \to \frac{1}{2} C_1$, $C_3 \to C_3 - C_1$.

$$\begin{pmatrix} ac+b & ab-2a & 0 & 0 & 0 \\ bc-ac & abb+4a & 6abc+ac+1 & 3abc+2bc-1 & 0 \\ -\frac{1}{2}cbac & cba & \frac{1}{2}cbac+a+b & c+2a & c+2a \end{pmatrix}$$

La partition associée à cette famille est $E_1 = \{1,2\}$, $E_2 = \{3,4\}$ et $E_3 = \{5\}$. On cherche à calculer une base indépendante de l'idéal engendré par les polynômes en deuxième composante des vecteurs du blocs E_2. On effectue les réécritures $C_4 \to 2C_4$, $C_4 \to C_4 - C_3$, $C_3 \to \frac{1}{6} C_3$, $C_4 \to \frac{1}{4} C_4$.

$$\begin{pmatrix} ac+b & ab-2a & 0 & 0 & 0 \\ bc-ac & abb+4a & abc+\frac{1}{6}(ac+1) & bc-\frac{1}{4}(ac+3) & 0 \\ -\frac{1}{2}cbac & cba & \frac{1}{12}(cbac+a+b) & -\frac{1}{8}(cbac-4c+2b-6a) & c+2a \end{pmatrix}$$

Cette fois, la partition associée à la famille est restée inchangée: $E_1 = \{1,2\}$, $E_2 = \{3,4\}$ et $E_3 = \{5\}$. Il n'y a pas de travail à faire sur le bloc E_3 puisqu'il est réduit à un seul vecteur. La famille de vecteurs est maintenant indépendante. Les codes préfixes associés à cette famille sont $X_1 = \{ac, ab\}$, $X_2 = \{abc, bc\}$ et $X_3 = \{c\}$. De plus, on vérifie que les polynômes en $k^{\text{ème}}$ composante des vecteurs du bloc E_k ($k = 1, 2, 3$) forment une base standard de l'idéal qu'ils engendrent.

Les vecteurs:

$$V_1' = \begin{pmatrix} ac+b \\ bc-ac \\ -\frac{1}{2}cbac \end{pmatrix}, V_2' = \begin{pmatrix} ab-2a \\ abb+4a \\ cba \end{pmatrix}, V_3' = \begin{pmatrix} 0 \\ abc+\frac{1}{6}(ac+1) \\ \frac{1}{12}(cbac+a+b) \end{pmatrix},$$

$$V_4' = \begin{pmatrix} 0 \\ bc-\frac{1}{4}(ac+3) \\ -\frac{1}{8}(cbac-4c+2b-6a) \end{pmatrix}, V_5' = \begin{pmatrix} 0 \\ 0 \\ c+2a \end{pmatrix}$$

forment une base indépendante du sous-module engendré par les vecteurs V_1, V_2, V_3, V_4 et V_5. ◇

Comme dans le cas $q = 1$, bien que les bases indépendantes d'un sous-module (de type fini) aient toutes les mêmes codes préfixes associés (Cor. 3.5.8), il n'y a pas unicité de la base. On ne gagne pas l'unicité en exigeant que chacune des familles de polynômes associées à chacun des blocs de la partition soit standard. Il faut demander un peu plus. La définition suivante nous a été suggérée par A. Joyal.

Soit $\{V_n\}_{n\geq 1}$ une famille de vecteurs indépendants de partition associée $E_1, \ldots, E_q$ et de codes préfixes associés $X_1, \ldots, X_q$. On dira que cette famille est *standard* si de plus, pour tout $k = 1, \ldots, q$:

(i) la famille de polynômes $\{\pi_k(V_i)\}_{i\in E_k}$ est une base standard de l'idéal qu'elle engendre,

(ii) si $i \in E_k$ et $j > k$ alors la condition suivante est satisfaite: pour tout $w \in A^*$, $w \in \pi_j(V_i)$ implique $w \in A^* - X_jA^*$.

Remarque 3.5.10 Soit $\{V_n\}_{n\geq 1}$ une famille standard de vecteurs de $K\langle A\rangle^q$. Alors on vérifie (comme à la Rem. 3.5.3 (i)) que les familles $\{\pi(V_n)\}_{n\geq 1, n\notin E_1}$, $\{\bar{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$ et $\{\iota(V_n)\}_{n\geq 1}$ sont standard. ◇

Théorème 3.5.11 *Soit $\mathcal{M}$ un sous-module de $K\langle A\rangle^q$. S'il existe une base standard de $\mathcal{M}$ alors elle est unique.*

Démonstration. On procède par récurrence sur q. Le théorème a déjà été montré pour $q = 1$ (Th. 3.4.8). Supposons qu'il existe deux bases standard de $\mathcal{M}$, $\mathcal{F} = \{V_n\}_{n\geq 1}$ et $\mathcal{F}' = \{V'_n\}_{n\geq 1}$ avec partition associée et codes préfixes associés respectifs $E_1, \ldots, E_q$, $X_1, \ldots, X_q$, et $E'_1, \ldots, E'_q$, $X'_1, \ldots, X'_q$. Les familles de vecteurs $\{\bar{\pi}(V_n)\}_{n\geq 1, n\notin E_q}$ et $\{\bar{\pi}(V'_n)\}_{n\geq 1, n\notin E'_q}$ sont deux bases du même sous-module de $K\langle A\rangle^{q-1}$. De plus, selon la Rem. 3.5.10 elles sont toutes deux standard. Par récurrence, elles sont égales. On peut donc supposer pour la suite, que $E_k = E'_k$, $X_k = X'_k$ $(k = 1, \ldots, q-1)$ et $\bar{\pi}(V_n) = \bar{\pi}(V'_n)$ (pour $n \geq 1$, $n \notin E_q$).

Nous montrons maintenant que les sous-familles $\{V_n\}_{n\in E_q}$ et $\{V'_n\}_{n\in E'_q}$ sont égales. Les idéaux I et I' (de $K\langle A\rangle$), respectivement engendrés par les familles de polynômes $\{\pi_q(V_n)\}_{n\in E_q}$ et $\{\pi_q(V'_n)\}_{n\in E'_q}$ sont égaux. En effet, soit $\{Q_n\}_{n\in E_q}$ une famille de polynômes presque tous nuls. Alors, puisque $\mathcal{F}$ et $\mathcal{F}'$ sont toutes deux des bases de $\mathcal{M}$, il existe une famille $\{Q'_n\}_{n\geq 1}$ de polynômes presque tous nuls tels que:

$$\sum_{n\in E_q} V_n Q_n = \sum_{n\geq 1} V'_n Q'_n.$$

On en tire, par application de $\bar{\pi}$, la relation

$$0 = \sum_{n\notin E'_q} \bar{\pi}(V'_n) Q'_n,$$

d'où $Q'_n = 0$ pour tout $n \notin E'_q$, puisque selon le Th. 3.5.4 la famille $\{\bar{\pi}(V'_n)\}_{n\geq 1}$ est $K\langle A\rangle$-linéairement indépendante. Par conséquent,

$$\sum_{n\in E_q} V_n Q_n = \sum_{n\in E'_q} V'_n Q'_n.$$

Par application de π_q on obtient:

$$\sum_{n\in E_q} \pi_q(V_n) Q_n = \sum_{n\in E'_q} \pi_q(V'_n) Q'_n,$$

ce qui montre que les deux familles de polynômes $\{\pi_q(V_n)\}_{n\in E_q}$ et $\{\pi_q(V'_n)\}_{n\in E'_q}$ engendrent le même idéal (puisque le raisonnement est symétrique en $\mathcal{F}$ et $\mathcal{F}'$); on a donc $I = I'$. Soit les blocs E_q, E'_q sont tous deux vides, et alors on a $I = I' = \{0\}$. Soit ils sont tous deux non vides; mais alors, par hypothèse, les familles $\{\pi_q(V_n)\}_{n\in E_q}$ et $\{\pi_q(V'_n)\}_{n\in E'_q}$ sont toutes deux des bases standard de l'idéal qu'elles engendrent. Selon le Th. 3.4.8, elles sont égales. On peut donc supposer que $E_q = E'_q$, $X_q = X'_q$ et $\pi_q(V_n) = \pi_q(V'_n)$ $(n \in E_q)$, d'où $V_n = V'_n$ pour $n \in E_q$.

Il reste à montrer que $\pi_q(V_i) = \pi_q(V'_i)$ pour $i \notin E_q$. Soit $i \geq 1$, $i \notin E_q$. Alors, comme $\mathcal{F}$ et $\mathcal{F}'$ sont toutes deux des bases de $\mathcal{M}$, il existe des polynômes $\{Q'_n\}_{n\geq 1}$ presque tous nuls, tels que:

$$V_i = \sum_{n\geq 1} V'_n Q'_n.$$

A l'aide de $\bar{\pi}$ on trouve:

$$\bar{\pi}(V_i) = \sum_{n \notin E'_q} \bar{\pi}(V'_n) Q'_n.$$

On a montré plus haut que $\bar{\pi}(V_n) = \bar{\pi}(V'_n)$ $(n \geq 1, n \notin E_q)$ et que la famille $\{\bar{\pi}(V_n)\}_{n \notin E_q}$ est la base standard du sous-module qu'elle engendre. Par conséquent, on a $Q'_n = 0$ pour $n \notin E'_q$ et $n \neq i$, et $Q'_i = 1$. La relation initiale est donc

$$V_i = V'_i + \sum_{n \in E'_q} V'_n Q'_n.$$

Par application de π_q on trouve:

$$\pi_q(V_i) = \pi_q(V'_i) + \sum_{n \in E'_q} \pi_q(V'_n) Q'_n.$$

On fait passer cette dernière égalité au quotient en appliquant la projection canonique $\varphi : K\langle A\rangle \to K\langle A\rangle/I$, pour obtenir $\pi_q(V_i) \equiv \pi_q(V'_i) \bmod I$ (car $I = I'$ est engendré par les polynômes $\{\pi_q(V'_n)\}_{n \in E'_q}$). Dans le cas où $E_q = E'_q = \emptyset$, on a $I = \{0\}$, et la congruence est en fait une égalité. Si $E_q = E'_q$ est non vide, on conclut aussi à l'égalité $\pi_q(V_i) = \pi_q(V'_i)$ puisque ces polynômes sont des sommes de mots de $A^* - X_q A^*$ et que cette famille de mots est indépendante mod I (Lemme 3.4.5). ◇

Pour montrer l'existence de la base standard d'un sous-module, on peut faire un raisonnement analogue en tout point à celui fait au paragraphe 3.4. On dira qu'un vecteur $U \in K\langle A\rangle^q$ est un *vecteur simple* si seulement l'une des composantes de U est non nulle et qu'elle se réduit à un mot. En d'autres mots, U est un vecteur simple si, pour un indice $k \in \{1, \ldots, q\}$, $\pi_k(U) = u \in A^*$ et $\pi_j(U) = 0$ pour $j \neq k$. Nous dirons alors que U est de *niveau* k.

Remarque 3.5.12 Tout vecteur $V \in K\langle A\rangle^q$ peut être écrit de façon unique comme combinaison K-linéaire de vecteurs simples. L'ensemble des vecteurs simples forme la K-base canonique de $K\langle A\rangle^q$ vu comme K-module. On notera par (V, W) le *coefficient du vecteur simple* W dans le vecteur V. ◇

Désignons par $\mathcal{S}$ l'ensemble des vecteurs simples. On ordonne totalement $\mathcal{S}$ d'abord selon le niveau, les vecteurs de niveau q devant être les plus petits; puis sur chaque niveau selon l'ordre $\leq$ sur le monoïde libre. Plus précisément, pour $U, U' \in \mathcal{S}$, respectivement de niveau k_1 et k_2, on aura $U < U'$ si et seulement si soit $k_1 > k_2$, soit $k_1 = k = k_2$ et $\pi_k(U) < \pi_k(U')$ (notez le renversement de l'ordre sur le niveau). Cet ordre total sur $\mathcal{S}$ est un bon ordre. Le vecteur $\mathbf{0}$ dont toutes les composantes sont nulles n'est pas un vecteur simple. Le vecteur de niveau q dont la $q^{\text{ème}}$ composante est le mot vide est le vecteur le plus petit de $\mathcal{S}$; nous le désignerons par $\mathbf{1}$. On définit aussi l'*intervalle*

$[U', U''] = \{U \in \mathcal{S} : U' \leq U \leq U''\}$. Etant donné une partie $P \subset A^*$ du monoïde libre, on désigne par $\mathcal{S}_{k,P}$ l'ensemble des vecteurs simples U de niveau k tels que $\pi_k(U) \in P$.

Soit $\mathcal{M}$ un sous-module de $K<A>$. Nous allons définir une suite croissante de vecteurs simples, qui donnera lieu à la base standard de $\mathcal{M}$. Nous abrégerons l'expression 'linéairement dépendant' par 'lin. dép.' On dira (comme on l'a fait pour les mots au paragraphe 3.4) qu'une famille de vecteurs simples $\{W_n\}_{n\geq 1}$ est lin. dép. mod $\mathcal{M}$ s'il est possible de trouver des scalaires $\{\alpha_n\}_{n\geq 1}$ ($\alpha_i \in K$), presque tous nuls (mais non tous nuls), tels que $\sum_{i\geq 1} \alpha_i W_i \in \mathcal{M}$.

Nous allons définir, pour $k = 1, \ldots, q$, une suite de vecteurs simples $\{U_n^{(k)}\}_{n\geq 1}$, de niveau k. On désignera la $k^{\text{ème}}$ composante du vecteur $U_n^{(k)}$ par $u_n^{(k)} = \pi_k(U_n^{(k)})$. Prenons $k = q$. On pose d'abord:

$$U_1^{(q)} = \inf\{W \in \mathcal{S}_{q,A^*} : [1, W] \cap \mathcal{S}_{q,A^*} \text{ est lin. dép. mod } \mathcal{M}\},$$

et pour $n \geq 2$:

$$U_n^{(q)} = \inf\{W \in \mathcal{S}_{q,A^*-\{u_1^{(q)},\ldots,u_{n-1}^{(q)}\}A^*} :$$

$$[1, W] \cap \mathcal{S}_{q,A^*-\{u_1^{(q)},\ldots,u_{n-1}^{(q)}\}A^*} \text{ est lin. dép. mod } \mathcal{M}\}.$$

Il se peut que pour un certain indice $n \geq 1$, la famille $\mathcal{S}_{q,A^*-\{u_1^{(q)},\ldots,u_{n-1}^{(q)}\}A^*}$ soit linéairement indépendante (mod $\mathcal{M}$). Le vecteur simple $U_n^{(q)}$ et les suivants ne sont alors pas définis.

Soit maintenant $k < q$. Supposons que les familles de vecteurs simples:

$$\{U_n^{(k+1)}\}_{n\geq 1}, \ldots, \{U_n^{(q)}\}_{n\geq 1}$$

ont toutes été définies. Posons, $X_i = \{u_n^{(i)}\}_{n\geq 1}$ et $\overline{X}_i = A^* - X_i A^*$, pour $i = k+1, \ldots, q$. On définit la suite $\{U_n^{(k)}\}_{n\geq 1}$ de la façon suivante:

$$U_1^{(k)} = \inf\{W \in \mathcal{S}_{k,A^*} : [1, W] \cap \left(\mathcal{S}_{k,A^*} \cup \bigcup_{i=k+1}^{q} \mathcal{S}_{i,\overline{X}_i}\right) \text{ est lin. dép. mod } \mathcal{M}\}.$$

et pour $n \geq 2$:

$$U_n^{(k)} = \inf\{W \in \mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*} :$$

$$[1, W] \cap \left(\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*} \cup \bigcup_{i=k+1}^{q} \mathcal{S}_{i,\overline{X}_i}\right) \text{ est lin. dép. mod } \mathcal{M}\}.$$

Encore une fois, il se peut que pour un certain indice $n \geq 1$, la famille

$$\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*} \cup \bigcup_{i=k+1}^{q} \mathcal{S}_{i,\overline{X}_i}$$

soit linéairement indépendante (mod $\mathcal{M}$). Le vecteur simple $U_n^{(k)}$ et les suivants ne sont alors pas définis.

Dans le cas où $q = 1$, cette construction est la même que celle que nous avons donnée au paragraphe 3.4.

Lemme 3.5.13 *Les mots de la famille $\{u_n^{(k)}\}_{n\geq 1}$, si elle n'est pas vide, sont distincts deux à deux et forment un code préfixe qui satisfait $u_i^{(k)} < u_j^{(k)}$, si $i < j$.*

Démonstration. On procède comme au Lemme 3.4.2. Supposons que les mots $u_1^{(k)}, \ldots, u_n^{(k)}$ forment un code préfixe et satisfont $u_1^{(k)} < \ldots < u_n^{(k)}$. Comme le vecteur simple $U_{n+1}^{(k)}$ est dans $\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_n^{(k)}\}A^*}$, c'est que $u_{n+1}^{(k)} \in A^* - \{u_1^{(k)}, \ldots, u_n^{(k)}\}A^*$, de sorte que les mots $u_1^{(k)}, \ldots, u_n^{(k)}$ ne sont pas préfixes du mot $u_{n+1}^{(k)}$. En particulier, $u_n^{(k)} \neq u_{n+1}^{(k)}$. Nous allons montrer que $u_n^{(k)} < u_{n+1}^{(k)}$; on en déduira, par (3.1), que $u_{n+1}^{(k)}$ n'est pas préfixe de $u_n^{(k)}$. Supposons qu'au contraire $u_{n+1}^{(k)} < u_n^{(k)}$; on a donc $U_{n+1}^{(k)} < U_n^{(k)}$. On sait alors, par (3.1), que $[1, u_{n+1}^{(k)}] \cap u_n^{(k)}A^* = \emptyset$, de sorte que:

$$[1, U_{n+1}^{(k)}] \cap \mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_n^{(k)}\}A^*} = [1, U_{n+1}^{(k)}] \cap \mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*}.$$

Ainsi:

$$\begin{aligned} & [1, U_{n+1}^{(k)}] \cap \left(\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_n^{(k)}\}A^*} \cup \bigcup_{i=k+1}^{q} \mathcal{S}_{i,\overline{X}_i} \right) \\ = \; & [1, U_{n+1}^{(k)}] \cap \left(\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*} \cup \bigcup_{i=k+1}^{q} \mathcal{S}_{i,\overline{X}_i} \right). \end{aligned}$$

Or, comme le premier membre de cette égalité est linéairement dépendant, et que $U_{n+1}^{(k)} < U_n^{(k)}$, le second membre contredit la minimalité du vecteur simple $U_n^{(k)}$. On doit donc avoir $u_n^{(k)} < u_{n+1}^{(k)}$. ◇

Nous allons poser pour toute la suite $\overline{\mathcal{S}} = \bigcup_{k=1}^{q} \mathcal{S}_{k,\overline{X}_k}$. Pour chaque vecteur simple $U_n^{(k)}$, il existe une relation K-linéaire (mod $\mathcal{M}$) qui lie $U_n^{(k)}$ avec ses prédécesseurs (qui sont dans $\overline{\mathcal{S}}$. Ainsi, pour chaque n et k, il existe un vecteur de polynômes $V_n^{(k)}$ du sous-module $\mathcal{M}$, qui peut s'écrire sous la forme:

$$V_n^{(k)} = U_n^{(k)} + \sum_{\substack{W \in \overline{\mathcal{S}} \\ W < U_n^{(k)}}} (V_n^{(k)}, W)W \quad \in \mathcal{M}.$$

Selon le Lemme 3.5.13, la famille de mots $\{u_n^{(k)}\}_{n\geq 1}$, si elle n'est pas vide est un code préfixe; cela implique, selon le Th. 3.2.11, que la famille de polynômes $\{\pi_k(V_n^{(k)})\}_{n\geq 1}$ est indépendante, puisqu'on a $r(\pi_k(V_n^{(k)})) = u_n^{(k)}$. Par conséquent, la famille de vecteurs $\{V_n^{(k)}\}_{\substack{k=1,\ldots,q\\ n\geq 1}}$ forme une base indépendante du sous-module qu'elle engendre. Par construction, elle en est aussi la base standard. En effet, un vecteur simple qui apparaît dans $V_n^{(k)}$, soit est $U_n^{(k)}$, soit il est dans

$$\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*} \quad \cup \quad \bigcup_{i=k+1}^{q} \mathcal{S}_{i,\overline{X_i}} \quad .$$

En effet, selon le point (i) de la Rem. 3.4.3, pour $v < u_n^{(k)}$, on a $v \in \overline{X_k}$ si et seulement si $v \in A^* - \{u_1^{(k)}, \ldots, u_{n-1}^{(k)}\}A^*$. Afin de montrer que les vecteurs $V_n^{(k)}$ forment la base standard du sous-module $\mathcal{M}$, il suffit donc de montrer qu'ils engendrent $\mathcal{M}$. Les deux prochains résultats généralisent le Lemme 3.4.4 et le Lemme 3.4.5 que nous avons montrés au paragraphe 3.4.

Lemme 3.5.14 *Soit $V \in K\langle A\rangle^q$. Il existe une famille $\{Q_{n,k}\}_{\substack{k=1,\ldots,q\\ n\geq 1}}$ de polynômes presque tous nuls et des scalaires $\{\alpha_W\}_{W\in\overline{\mathcal{S}}}$ presque tous nuls tels que V puisse être écrit sous la forme:*

$$V = \sum_{\substack{k=1,\ldots,q\\ n\geq 1}} V_n^{(k)} Q_{n,k} + \sum_{W\in\overline{\mathcal{S}}} \alpha_W W.$$

Démonstration. Il suffit de montrer le lemme dans le cas d'un vecteur simple $W_0 \notin \overline{\mathcal{S}}$. Supposons W_0 de rang k; on a donc $\pi_k(W_0) \in X_k A^*$. Alors il existe un mot $w \in A^*$ et un vecteur simple $U_n^{(k)}$ tels que $W_0 = U_n^{(k)} w$. On procède par récurrence sur les couples $(k, |w|)$ ordonnés par $(k_1, i) < (k_2, j)$ si et seulement si soit $k_1 > k_2$, soit $k_1 = k_2$ et $i < j$. On a:

$$W_0 \quad = \quad U_n^{(k)} w \quad = \quad V_n^{(k)} w - \sum_{\substack{W\in\overline{\mathcal{S}}\\ W<U_n^{(k)}}} W w.$$

Dans la somme du membre droit, soit le vecteur simple Ww est de niveau supérieure à k, soit il est de rang k et alors deux cas sont possibles. Soit $Ww \in \mathcal{S}_{k,\overline{X_k}}$, soit $Ww = U_{n'}^{(k')} w'$. Dans cette dernière éventualité on trouve $\pi_k(Ww) = vw = u_{n'}^{(k')} w' = \pi_k(U_{n'}^{(k')} w')$ avec $|w'| < |w|$ (puisque $v \in \overline{X_k}$). On peut donc conclure par récurrence et le lemme est montré. ◇

Lemme 3.5.15 *La famille de vecteurs simples $\{W\}_{W\in\overline{\mathcal{S}}}$ est linéairement indépendante mod $\mathcal{M}$.*

Démonstration. Si $X_1 = \{u_n^{(1)}\}_{n\geq 1}$ est vide ou si X_1 est fini alors c'est précisément parce que la famille $\{W\}_{W\in\overline{\mathcal{S}}}$ est linéairement indépendante mod $\mathcal{M}$. En effet, si X_1 est vide alors c'est que $[1,W]\cap(\mathcal{S}_{1,A^*} \cup \bigcup_{i=2}^{q}\mathcal{S}_{k,\overline{X}_k})$ est linéairement independant mod $\mathcal{M}$ pour tout $W\in\mathcal{S}_{1,A^*}$; c'est donc dire que la famille $\overline{\mathcal{S}} = \mathcal{S}_{1,A^*} \cup \bigcup_{q}^{k=2}\mathcal{S}_{k,\overline{X}_k}$ est linéairement indépendante mod $\mathcal{M}$. Si le code X_1 est fini, le résultat est évident.

Il reste donc à considérer le cas où X_1 est infini. Supposons qu'au contraire il existe des scalaires $\{\alpha_W\}_{W\in\overline{\mathcal{S}}}$ presque tous nuls (mais non tous nuls) tels que $\sum\alpha_W W\in\mathcal{M}$. Soient n et k tels que:

$$U_n^{(k)} = \inf\{U_i^{(j)} : U_i^{(j)} > W \text{ pour tout } W \text{ tel que } \alpha_W\neq 0\}.$$

Alors, comme $W < U_n^{(k)}$ et $W\in\overline{\mathcal{S}}$, on a en fait

$$W\in\mathcal{S}_{k,A^*-\{u_1^{(k)},\ldots,u_{n-1}^{(k)}\}A^*} \cup \bigcup_{i=k+1}^{q}\mathcal{S}_{k,\overline{X}_k}.$$

De sorte que la relation $\sum\alpha_W W = 0 \bmod \mathcal{M}$ contredit la minimalité du vecteur simple $U_n^{(k)}$. ◇

Proposition 3.5.16 *Les vecteurs* $\{V_n^{(k)}\}_{\substack{k=1,\ldots,q\\ n\geq 1}}$ *engendrent* $\mathcal{M}$.

Démonstration. Soit $\vartheta : K\langle A\rangle^q \to K\langle A\rangle^q/\mathcal{M}$ le morphisme canonique de $K\langle A\rangle$-module (à droite). Soit $V\in\mathcal{M}$; on a alors $\vartheta(V) = \mathbf{0}$. Selon le Lemme 3.5.14, il existe des polynômes $\{Q_{n,k}\}_{\substack{k=1,\ldots,q\\ n\geq 1}}$ presque tous nuls et des scalaires $\{\alpha_W\}_{W\in\overline{\mathcal{S}}}$ presque tous nuls tels que:

$$V = \sum_{\substack{k=1,\ldots,q\\ n\geq 1}} V_n^{(k)}Q_{n,k} + \sum_{W\in\overline{\mathcal{S}}}\alpha_W W.$$

On a donc:

$$\begin{aligned}\mathbf{0} = \vartheta(V) &= \vartheta\Big(\sum_{\substack{k=1,\ldots,q\\ n\geq 1}} V_n^{(k)}Q_{n,k} + \sum_{W\in\overline{\mathcal{S}}}\alpha_W W\Big)\\ &= \vartheta\Big(\sum_{\substack{k=1,\ldots,q\\ n\geq 1}} V_n^{(k)}Q_{n,k}\Big) + \vartheta\Big(\sum_{W\in\overline{\mathcal{S}}}\alpha_W W\Big)\\ &= \vartheta\Big(\sum_{W\in\overline{\mathcal{S}}}\alpha_W W\Big).\end{aligned}$$

On en déduit $\alpha_W = 0$ pour tout $W\in\overline{\mathcal{S}}$ puisque la famille $\{W\}_{W\in\overline{\mathcal{S}}}$ est linéairement indépendante mod $\mathcal{M}$, selon le Lemme 3.5.15. Par conséquent, on obtient:

$$V = \sum_{\substack{k=1,\ldots,q\\ n\geq 1}} V_n^{(k)}Q_{n,k} \quad ,$$

et le résultat est montré. ◇

Théorème 3.5.17 *Soit $V_1, \ldots, V_n$ une famille indépendante. Il est possible de calculer, à l'aide d'une suite de réécritures élémentaires, la base standard du sous-module $\mathcal{M}$ engendré par les vecteurs $V_1, \ldots, V_n$. De plus, la partition et les codes préfixes associés à la base standard de $\mathcal{M}$ sont respectivement égaux à la partition et aux codes préfixes associés à $V_1, \ldots, V_n$.*

Démonstration. Nous allons procéder comme au Th. 3.4.9 et construire un outil de récurrence pour la démonstration. On pose, pour $V \in K\langle A\rangle^q$, $R(V) = \max\{W \in S : W \in V\}$; le vecteur simple $R(V)$ est donc le vecteur simple maximum qui apparaît dans V. Etant donné les codes préfixes $X_1, \ldots, X_q$, on définit le multi-indice $\overline{\nu} = \overline{\nu}(V_1, \ldots, V_n) = (\varrho_W)_{W \in \bigcup_{i=1}^q S_{i,X_iA^*}}$, en posant $\varrho_W = |\{i : W \in V_i, W \neq R(V_i)\}|$. Pour $W \in \bigcup_{i=1}^q S_{i,X_iA^*}$, l'entier ϱ_W compte le nombre de vecteurs dans lesquels le vecteur simple apparaît, sans en être l'élément maximal. On ordonne ces multi-indices selon l'ordre lexicographique inverse. Plus précisément, pour $\overline{\nu'} = (\varrho'_W)_{W \in \bigcup_{i=1}^q S_{i,X_iA^*}}$ et $\overline{\nu} = (\varrho_W)_{W \in \bigcup_{i=1}^q S_{i,X_iA^*}}$, on aura $\overline{\nu'} < \overline{\nu}$ si et seulement s'il existe un vecteur simple $W \in \bigcup_{i=1}^q S_{i,X_iA^*}$ tel que $\varrho'_W < \varrho_W$ et $\varrho'_U = \varrho_U$ pour tout $U > W$.

Soient $E_1, \ldots, E_q$ et $X_1, \ldots, X_q$ la partition associée et les codes préfixes associés à la famille $V_1, \ldots, V_n$. On peut supposer, en vertu du Cor. 3.5.8, qu'en chacune des composantes la famille de polynômes $\{\pi_k(V_i)\}_{i \in E_k}$ est une base standard de l'idéal qu'elle engendre. On procède par récurrence sur $\overline{\nu}(V_1, \ldots, V_n)$.

Si la famille $V_1, \ldots, V_n$ n'est pas standard c'est qu'il existe deux vecteurs de la base, V_i et V_j, avec $i \in E_{k_1}$, $j \in E_{k_2}$ et $k_1 < k_2$, un vecteur simple W de niveau k_2 et des mots $v, w \in A^*$ tels que $W = R(V_j)$, $\pi_{k_2}(W) = w = r(\pi_{k_2}(V_j))$ et $Wv \in V_i$. On a donc $(V_j, W) = 1$ car $r(\pi_{k_2}(V_j)) = w$. Posons $V'_m = V_m$ pour $m \neq i$ et $V'_i = V_i - (V_i, W)V_jv$. On a maintenant $(V'_i, Wv) = 0$. Cette réécriture élémentaire ne modifie pas la $k_1^{\text{ème}}$ composante du vecteur V_i puisqu'on a supposé $k_1 < k_2$. Par conséquent, la partition associée et les codes préfixes associés restent inchangés. On est donc en mesure de comparer $\overline{\nu}(V_1, \ldots, V_n)$ et $\overline{\nu}(V'_1, \ldots, V'_n)$. Si $W' \neq W$ est un vecteur simple dans V_jv alors $W' < W$. En effet, tous ces vecteurs simples sont de la forme $W' = Uv$ pour un $U \in V_j$. Le niveau de U est au moins égal à k_2, car $j \in E_{k_2}$. Donc, soit U est de niveau plus grand que k_2, soit il est de niveau k_2 et alors $\pi_{k_2}(U) = u < w = r(lpi_{k_2}(V_j))$ entraîne $\pi_{k_2}(W') = \pi_{k_2}(Uv) = \pi_{k_2}(U)v = uv < wv = \pi_{k_2}(V_jv)$, en vertu de (3.1). Cela montre que $\overline{\nu}(V'_1, \ldots, V'_n) < \overline{\nu}(V_1, \ldots, V_n)$. Selon le Lemme 3.5.6, ces deux familles de vecteurs engendrent le même sous-module; on peut donc conclure par récurrence. ◇

Remarque 3.5.18 Le Th. 3.5.7 (comme le Th. 3.5.17 ci-haut) peut aussi être montré en faisant une récurrence sur le multi-indice (défini plutôt de façon analogue au multi-indice des recteurs des polynômes - paragraphe 3.3). La démonstration que nous en

avons donnée a toutefois l'avantage de mettre en évidence le fait que le calcul de la base indépendante d'un sous-module s'effectue composante par composante. ◇

Exemple 3.5.19 Reprenons la base indépendante du sous-module engendré par les vecteurs V_1, V_2, V_3, V_4 et V_5, calculée à l'Ex. 3.5.9 (et les notations que nous avons utilisées). Disposons ces vecteurs dans une matrice.

$$\begin{pmatrix} ac+b & ab-2a & 0 & 0 & 0 \\ bc-ac & abb+4a & abc+\frac{1}{6}(ac+1) & bc-\frac{1}{4}(ac+3) & 0 \\ -\frac{1}{2}cbac & cba & \frac{1}{12}(cbac+a+b) & -\frac{1}{8}(cbac-4c+2b-6a) & c+2a \end{pmatrix}$$

Cette base n'est pas la base standard du sous-module qu'elle engendre. On 'nettoie' les supports des polynômes en deuxième composante. Le travail est dans ce cas assez simple; seul le premier vecteur doit subir une réécriture, qui est $C_1 \rightarrow C_1 - C_4$:

$$\begin{pmatrix} ac+b & ab-2a & 0 & 0 & 0 \\ -\frac{3}{4}(ac-1) & abb+4a & abc+\frac{1}{6}(ac+1) & bc-\frac{1}{4}(ac+3) & 0 \\ -\frac{1}{2}cbac & cba & \frac{1}{12}(cbac+a+b) & -\frac{1}{8}(cbac-4c+2b-6a) & c+2a \end{pmatrix}$$

On poursuit le travail sur la troisième composante des vecteurs en appliquant les réécritures $C_1 \rightarrow C_1 + \frac{1}{2}C_5bac$, $C_2 \rightarrow C_2 - C_5ba$, $C_3 \rightarrow C_3 - 1/12C_5bac$, $C_4 \rightarrow C_4 + 1/8C_5bac$ et $C_4 \rightarrow C_4 - \frac{1}{2}C_5$:

$$\begin{pmatrix} ac+b & ab-2a & 0 & 0 & 0 \\ -\frac{3}{4}(ac-1) & abb+4a & abc+\frac{1}{6}(ac+1) & bc-\frac{1}{4}(ac+3) & 0 \\ abac & -2aba & \frac{1}{12}(-2abac+a+b) & \frac{1}{4}(abac-b-a) & c+2a \end{pmatrix}$$

La base formée des vecteurs:

$$V_1'' = \begin{pmatrix} ac+b \\ -\frac{3}{4}(ac-1) \\ abac \end{pmatrix}, V_2'' = \begin{pmatrix} ab-2a \\ abb+4a \\ -2aba \end{pmatrix}, V_3'' = \begin{pmatrix} 0 \\ abc+\frac{1}{6}(ac+1) \\ \frac{1}{12}(-2abac+a+b) \end{pmatrix},$$

$$V_4'' = \begin{pmatrix} 0 \\ bc-\frac{1}{4}(ac+3) \\ \frac{1}{4}(abac-b-a) \end{pmatrix}, V_5'' = \begin{pmatrix} 0 \\ 0 \\ c+2a \end{pmatrix}.$$

est la base standard du sous-module engendré par les vecteurs V_1, V_2, V_3, V_4 et V_5. ◇

Comme dans le cas $q = 1$, l'unicité de la base standard (Th. 3.5.11 et Prop. 3.5.16) et la possibilité d'en effectuer le calcul (Th. 3.5.17) nous permettent de tester si deux sous-modules finiment engendrés sont égaux. On est aussi en mesure de tester l'appartenance d'un vecteur à un sous-module $\mathcal{M}$ (finiment engendré), et on peut calculer son image dans le quotient $K\langle A\rangle^q/\mathcal{M}$.

Corollaire 3.5.20 *Il est possible de tester si deux ensembles finis de vecteurs engendrent le même sous-module.* ◇

Corollaire 3.5.21 *Soient V et $V_1, \ldots, V_n \in K\langle A\rangle^q$ tels que la famille $V_1, \ldots, V_n$ est la base standard du sous-module $\mathcal{M}$ qu'elle engendre. Il est possible de calculer l'image de V, dans le quotient $K\langle A\rangle^q/\mathcal{M}$. En particulier, il est possible de tester si $V \in \mathcal{M}$.*

Démonstration. On désigne par $\vartheta : K\langle A\rangle^q \to K\langle A\rangle^q/\mathcal{M}$ la projection canonique. Il nous suffit de savoir calculer l'image d'un vecteur simple $W \in \mathcal{S}$. On procède par récurrence sur l'ordre défini sur $\mathcal{S}$. Soient $E_1, \ldots, E_q$ et $X_1, \ldots, X_q$, respectivement la partition associée et les codes préfixes associés à la famille $V_1, \ldots, V_n$. Supposons W de niveau k. Si $\pi_k(W) \in \overline{X_k}$ alors $\vartheta(W) = W$. Sinon, il existe un mot w et un vecteur V_i avec $i \in E_k$ tels que $\pi_k(W) = r(\pi_k(V_i))w$.

$$\begin{aligned} \vartheta(W) &= \vartheta(W - V_i w) + \vartheta(V_i w) \\ &= \vartheta(W - V_i w) + 0 \\ &= \vartheta(W - V_i w), \end{aligned}$$

Le vecteur $W - V_i w$ fait apparaître des vecteurs simples W' qui soit sont de niveau supérieure à k, soit sont de niveau k et ont une composante $\pi_k(W')$ plus petite que le mot $r(\pi_k(V_i))w$. On peut donc, par récurrence, terminer le calcul. ◇

Conclusion

Nous avons vu que plusieurs propriétés des mots de Lyndon étaient communes à toutes les familles de mots de Hall, et que ces propriétés tiennent au tissu subtil d'inégalités qui se tisse derrière chaque arbre de Hall. Le cas des mots de Lyndon n'en demeure pas moins unique. En effet, dans ce cas le choix des mots et la construction de la base de l'algèbre de Lie libre qu'ils fournissent, peuvent être faits directement à partir du monoïde libre (cf. [Ga 88, Lo 82, Vi 76]). Ce n'est pas le cas pour les autres familles de mots de Hall. Pour cette raison, il serait très utile d'obtenir une caractérisation des ordres sur le monoïde libre, qui autorisent la construction de ces factorisations et de leurs bases de l'algèbre de Lie libre associées, comme on le fait pour les mots de Lyndon. On obtiendrait du même coup une approche rénovée pour la construction des bases de la série centrale descendante du groupe libre.

Nous avons cherché une réponse à ce problème sans arriver à de résultats satisfaisants. Il est possible de donner des conditions assez techniques qui permettent de choisir des mots dans le monoïde libre et de leur associer une structure arborescente, de façon à ce que la famille de mots forme un ensemble de Hall. Cependant, il semble impossible d'éviter, de façon élégante, de formuler des conditions de la trempe des conditions (1.6), (1.7) et (1.8). Le problème mérite qu'on s'y attarde encore.

Comme nous l'avons mentionné dans l'introduction de ce travail, les idéaux à droite de l'anneau des polynômes non commutatifs et les sous-algèbres de Lie de l'algèbre de Lie libre sont intimement liés. Širšov[Ši 53] a montré que les sous-algèbres de Lie de l'algèbre de Lie libre sont elles-mêmes des algèbres de Lie libres. Ce sont ces deux résultats qui nous ont poussés à entreprendre notre travail sur le calcul des bases standard des idéaux à droite (de l'anneau des polynômes non commutatifs), dans le but de donner un calcul effectif des familles basiques des sous-algèbres de Lie de l'algèbre de Lie libre. Nos résultats sur le calcul des bases des idéaux à droite laissent espérer qu'il sera possible d'en faire autant pour le calcul de familles basiques des sous-algèbres de Lie (de l'agèbre de Lie libre). Le travail sur les sous-algèbres de Lie fera partie de recherches futures; les travaux de Cohn [Co 61, Co 64, Co 69] pourraient nous être encore une fois d'une grande inspiration.

Bibliographie

[BR 88] Berstel J., Reutenauer C., *Rational Series and Their Languages*, Springer, Berlin Heidelberg New York (1988).

[Bo 60] Bourbaki N., *Eléments de mathématiques, Topologie générale*, Hermann, Paris, (1960). (Chapitre 3, *Groupes topologiques*)

[Bu 85] Buchberger B., Gröbner Bases: an Algorithmic Method in Polynomial Ideal Theory, *in N. K. Bose Ed., Recent Trends in Multidimensional System Theory*, Reidel, (1985).

[CFL 58] Chen K. T., Fox R. H., Lyndon R. C., Free differential calculus IV, The quotients of the lower central series, *Ann. of Math.* **68**, **1**, (1958), 81–95.

[Co 61] Cohn P. M., On a generalization of the Euclidean algorithm, *Proc. Cambridge Phil. Soc.* **57**, (1961), 18–30.

[Co 64] Cohn P. M., Subalgebras of Free Associative Algebras, Proc. Math. Soc. London, (3), **14**, (1964), 618–632.

[Co 69] Cohn P. M., Free Associative Algebras, *Bull. London Math. Soc.* **1**, (1969), 1–39.

[Co 85] Cohn P. M., *Free Rings and Their Relations*, Academic Press, London New York ($2^{\text{ème}}$ édition), (1985).

[Di 74] Dixmier J., *Algèbres enveloppantes*, Hermann, Paris, (1974).

[Du 83] Duval J. P., Factorizing words over an ordered alphabet, *J. of Algorithms* **4**, (1983), 363–381.

[Du 88] Duval J. P., Génération d'une section des classes de conjugaison et arbres des mots de Lyndon en longueur bornée, *Th. Comp. Sci.* **60**, (1988), 255–283.

[Ga 88] Garsia A., *Combinatorics of the free Lie algebra and the symmetric group*, Analysis Etc..., Research papers published in honor of Jurgen Moser's 60^{th} birthday, ed. Paul H. Rabinowitz and Eduard Zehnder, Academic Press, (1990).

[Go 69] Gorčakov Y. M., Commutator Subgroups, *Sibirski Matematischeski Zhurnnal* **10**, **5**, (1969), 1023–1033.

[HM 50a] Hall M., A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.* **1**, (1950), 575–581.

[HM 50b] Hall M., A topology for free groups and related groups, *Ann. of Math.* **52**, (1950), 127–139.

[HM 59] Hall M., *Theory of groups*, The MacMillan Company, (1959).

[HP 33] Hall P., A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* **2**, **36**, (1933), 29–95.

[Hu 72] Humphreys J. E., *Introduction to Lie algebras and representation theory*, Springer Verlag, (1972).

[Ja 62] Jacobson N., *Lie Algebras*, Interscience Publishers, John Wiley, (1962).

[Lo 82] Lothaire M., *Combinatorics on words*, Addison–Wesley, Reading Mass., (1982).

[Ly 54] Lyndon R. C., On the Burnside problem I, *Trans. Amer. Math. Soc.*, **77**, (1954), 202–215.

[LS 77] Lyndon R. C., Schupp P. E., *Combinatorial Group Theory*, Springer, Berlin Heidelberg New York (1977).

[Ma 35] Magnus W., Bezeihungen zwischen Gruppen und Idealen in einem speziellen Ring, *Math. Ann.*, **111**, (1935), 259–280.

[Ma 37] Magnus W., Über Bezeihungen zwischen höneren Kommutatoren, *J. Grelle*, **177**, (1937), 105–115.

[MKS 76] Magnus W., Karass A., Solitar D., *Combinatorial Group Theory*, Dover Publications ($2^{ème}$ Ed.) (1976).

[MW 52] Meier-Wunderli H., Note on a basis of P. Hall for the higher commutators in free groups, *Comm. Math. Helv.* **26**, (1952), 1–5.

[Me 91] Melançon G., Combinatorics of Hall trees and Hall words, à paraître dans *J. of Comb. Th. , Series 'A'.*

[MR 89] Melançon G., Reutenauer C., Lyndon words, Free algebras and shuffles, *Can. J. Math.* **XLI**, **4**, (1989), 577–591.

[Mo 85] Mora F., Groebner Bases for Non–commutative Polynomial Rings, *Lectures Notes in Computer Science* **229**, 3^{rd} *International Conference AAECC*-3 Proceedings, Grenoble, France, (1985), 353–362.

[PV 81] errin D., Viennot X., *A note on shuffle algebras*, (1981), non publié.

[Pi 88] Pin J. E., Topologies for the Free Monoid, *J. of Algebra*, vol. 137, no. 2, (1991), 297–337.

[Ra 79] Radford D. E., A natural ring basis for the shuffle algebra and an application to group schemes, *J. of Algebra*, **58**, (1979), 432–453.

[Ree 58] Ree R., Lie elements and an algebra associated with shuffles, *Ann. Math.*, **68**, (1958), 210–220.

[Ree 61] Ree R., On generalized Lie elements, *Can. J. Math.*, (1960), 493–502.

[Reu] Reutenauer C., *Free Lie algebras*, à paraître chez *Oxford University Press*.

[Reu 79] Reutenauer C., Une topologie du monoïde libre, *Semigroup Forum*, vol. **18**, (1979), 33–49.

[Reu 86] Reutenauer C., Mots de Lyndon et un théorème de Širšov, Ann. Sci. Math. Québec, **10**, (1986), 237–245.

[Reu 90] Reutenauer C., Applications of a non commutative Jacobian matrix, (1990).

[S 79] Scheunert M., The theory of Lie superalgebras: an introduction, *Lectures Notes in Math.* **716**, Springer-Verlag, Berlin (1979).

[Sc 58] Schützenberger M. P., Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de Mathématiques appliquées, *Séminaire Dubreuil-Pisot année* 1958–1959, Inst. Henri-Poincaré, Paris (1958).

[Sc 61] Schützenberger M. P., On the Definition of a Family of Automata, *Information and Control* **4**, (1961), 245–270.

[Sc 65] Schützenberger M. P., On a factorisation of free monoids, *Proc. Amer. Math. Soc.* **16**, **1**, (1965), 21–24.

[Sc 87] Schützenberger M. P., *Bases de Hall*, Notes manuscrites (Hiver 1986–1987).

[Ši 53] Širšov A. I., Subalgebras of Free Lie algebras. Mat. Sbarnik N.S., **33**, **75**, (1953), 441–452.

[Ši 62] Širšov A. I., On bases for a free Lie algebra, *Algebra i Logika* **1**, (1962), 14–19.

[Th 83] Thérien D., Subwords counting and nilpotent groups *in Combinatorics on words, Progress and perspectives*, Larry J. Cummings Ed., Academic Press, (1983), 297–305.

[Vi 76] Viennot X. G., Algèbres de Lie libres et monoïdes libres, *Lectures Notes in Math.* **691**, Springer-Verlag, Berlin (1976).

[Wa 69] Ward M. A., Basic commutators, *Philos. Trans. Roy. Soc. London* **A 264**, (1969), 343–412.

[Wi 37] Witt, E., Treue Darstellung Liescher Ringe, *J. für Reine und Ang. Math.*, t. **177**, (1937), 152–160.

Index terminologique

Index des notations

$\kappa : M(A) \to F(A)$	application canonique, 46
$\kappa(h), [h]$	commutateur de Hall, 47
$\gamma(s)$	élément de $F(A)$ associé à la suite s, 47
$s = ([h_1]^{\epsilon_1}, \ldots, [h_n]^{\epsilon_n})$	suite standard de commutateurs de Hall, 47
$\leq_{\deg}$	ordre total sur H, compatible avec le degré, 51
$\preceq$	ordre total sur $H \times H$, 51
$v(s)$	vecteur des montées éloignées, 51
$\to, \to'$	relations de réécriture, 52
$\mu(a) = 1 + a$	transformée de Magnus de $F(A)$, 59
$\omega(T)$	ordre de la série formelle T, 59
$w \mapsto \binom{w}{u}$	fonction sous-mot, 61
$n_h(g)$	exposant de $[h]$ dans le décomposition de g, 64
$s(w)$	suite standard formée des lettres de w, 65
$T(w)$	suite décroissante de commutateurs dérivée de w, 65
$\mathcal{E}([k])$	ensemble des indices des lettres dans $[k]$, 65
$\vartheta : F(A) \to K$	fonction représentative, 70
X	code préfixe, 79
$r(P)$	recteur du polynôme P, 81
I	idéal à droite dans $K\langle A\rangle$, 85
$(\vartheta_w)_{w \in A^*}$	multi-indice des recteurs, 86
$[u, v]$	intervalle des mots entre u et v, 91
$K\langle A\rangle^q$	$K\langle A\rangle$-module à droite des vecteurs de polynômes, 96
V	vecteur de polynômes, 96
$E_1, \ldots, E_q$	partition, 97
$\mathcal{M}$	sous-module de $K\langle A\rangle^q$, 100
$[U', U'']$	intervalle de vecteurs simples, 105
$\mathcal{S}_{k,P}$	vecteurs simples de niveau k à support dans P, 105