$[\mathbf{1}]|]\mathbf{1}$ $\mathrm{mon}_g risrgb.9, .9, .9$
define@key

Monoïdes et automates admettant un produit de mélange

August 27, 2001

Remerciements

La réalisation d'une thèse ne ressemble en rien à celle d'autres textes, elle est faite de recherches qui se ramifient à l'infini, de trouvailles et d'impasses, car elle a ceci de particulier qu'elle mobilise beaucoup de bonnes volontés que l'unique signataire se fait un plaisir de remercier au terme de ses années de peine et d'enthousiasme.

Les remerciements qui me viennent le plus naturellement, vont à mon directeur de thèse Gerard Duchamp qui a été pour moi un guide irremplaçable et dévoué, faisant fi de son temps, il a toujours su m'aiguiller et m'amener vers les voies du savoir, et ce depuis mon DEA, avec la même patience et constance.
Pour tout cela, je lui suis infiniment redevable et reconnaissant.

Messieurs Jacques Désarménien, Gérard Jacob et Xavier Viennot m'ont fait le très grand honneur d'être rapporteurs. Je tiens à leur exprimer toute ma gratitude pour leurs précieuses remarques qui ont contribué à l'aboutissement de ce travail.

J'adresse mes remerciements aux membres du Jury pour l'intérêt qu'ils ont porté à ce travail: Messieurs Laurent Vuillon, Jean-Yves Thibon, Daniel Krob et tout particulièrement à Jean-Francis Michon pour l'attention qu'il a su me consacrer.

Les membres du LIFAR m'ont apporté beaucoup de sympathie durant ces années. Ma gratitude à leur égard est considérable.

Mes collègues de l'équipe Calcul Symbolique, bénévoles et dévoués, reconnaîtront ici et là, ce que je dois à leur spécialité. Pour les renseignements de tous ordres qu'ils ont bien voulu me donner et l'amitié qu'il m'ont procurée, je remercie:

Christophe Carré et ses invitations chaleureuses, Jean-Philippe Dubernard

le "grand vigneron", une mention toute spéciale pour Marianne Flouret et Eric Laugerotte.

Philippe Andary et Bruno Patrou ont mis leur compétence et leur bonne humeur à ma disposition en ce qui concerne les mots de Lyndon, qu'ils trouvent ici l'expression de mon estime et de mon amitié.

Les secretaires ont réglé de nombreux problèmes pratiques qui m'ont fait gagner un temps précieux, je pense en particulier à Philippe Chaussier, Pierre Langlard et Maryse Brochot.

Jean-Luc Ponty, grâce à ses prouesses, porte à bout de bras le parc des machines du département d'informatique, et permet ainsi aux chercheurs de travailler sereinement, je le remercie sincèrement.

Sans oublier ma famille, mes amis, qui ont fait preuve d'une grande patience à mon égard et en particulier ma mère pour son soutien, mon père pour ses conseils en Latex, Séverine, ma petite correctrice qui a relu avec toute son application ces "chroniques martiennes".

Contents

Chapter 1

Introduction générale

Le produit de mélange dans A^* a été introduit par Chen, Fox et Lyndon dans "Free differential calculus" [?]. Ce produit peut se généraliser à d'autres monoïdes dont le plus connu est le monoïde partiellement commutatif libre. Sa généralisation au cadre des commutations partielles n'est pas la simple projection du produit de mélange de A^* dans (A, θ). En effet, si on considère les commutations $a - b \quad c$ alors $ab_\theta c = abc + acb + bac + cab$ ce n'est pas la projection de $abc = abc + acb + cab$. Si on veut le généraliser par une projection, il faut utiliser sa loi duale qui est un coproduit ([?]). Par ce biais, on peut justifier la notion de paires complémentaires sous-mots partiellement commutatifs (sous-traces).

Dans un premier temps, on peut se demander s'il y a d'autres relateurs que les commutations partielles qui permettent le passage au quotient du coproduit. La discussion, qui occupera le chapitre 4 de notre mémoire, s'organise ainsi:

Pour les semi-anneaux qui ne sont pas des anneaux et pour les anneaux dont la caractéristique n'est pas un nombre premier (c'est à dire 0 et les nombres composés), il n'y a que les commutations partielles. En caractéristique p d'autres phénomènes curieux apparaissent.

En fait, le monoïde partiellement commutatif admet une combinatoire assez proche de celle du monoïde libre. Dans les deux premiers chapitres de cette thèse, nous étudierons quelques propriétés de ce monoïde. Le monoïde des traces ou monoïde partiellement commutatif libre a été introduit dans le cadre de l'informatique théorique par Mazurkiewicz [?, ?], mais il a été défini quelques années plus tôt par Cartier et Foata pour des probèmes combinatoires [?] .

La notion de commutation partielle ne se restreint pas aux monoïdes, d'autres structures libres peuvent se généraliser. Nous utiliserons en particulier, l'algèbre des polynômes (resp. séries) partiellement commutatifs, le groupe et l'algèbre des polynômes (resp. séries) de Lie, ces notions sont définies dans [?, ?, ?].

Dans le premier chapitre, nous nous intéresserons à la notion de factorisation du monoïde des traces. Cette notion, qui a été très étudiée par Viennot [?, ?] puis par Schützenberger [?, ?], possède de nombreuses propriétés généralisables aux commutations partielles. En effet, nous verrons que l'existence d'un coproduit de mélange nous permet de définir une algèbre de séries de Lie, ce qui interviendra dans la preuve d'une version partiellement commutative du théorème de factorisation de Schützenberger [?]. Ce théorème, que nous avons prouvé en collaboration avec M.Flouret [?], est utile à plusieurs titres. Non seulement, il permet de relier les notions de classe de conjugaison (étudiées dans ce cadre par Choffrut et Duboc [?, ?]) et de factorisation, mais aussi, va nous encourager à réaliser une généralisation du procédé d'élimination de Lazard. En effet, les classes de conjugaison et les bases de l'algèbre de Lie partiellement commutative libre ont la même combinatoire et donc il en est de même pour les factorisations complètes.

Il est alors légitime de vouloir construire bijectivement un ensemble de factorisations complètes et un ensemble de bases, de la même façon que dans le cas non commutatif.

X. Viennot [?] construit bijectivement de tels ensembles en utilisant la notion de bascule. Cette notion semble pour l'instant difficile à appréhender dans le cadre des commutations partielles, nous nous intéresserons donc à un sous-ensemble: les factorisations utilisant les bisections de type "Lazard". Nous donnerons une généralisation de ces bisections, ainsi qu'une méthode pour construire des factorisations et des bases en les utilisant ([?]). Pour certains monoïdes, nous donnerons une généralisation des ensembles de Hall [?].

Le chapitre suivant porte sur un travail que nous avons réalisé en collaboration avec E.Laugerotte [?]: l'étude du support d'une famille d'algèbres de Lie partiellement commutatives libres. Le problème du support est lié à l'étude du projecteur orthogonal [?, ?, ?], le produit de mélange intervient dans cette étude. En effet, un théorème de Ree [?] montre qu'un polynôme est orthogonal à tout polynôme de Lie si et seulement si il est une combinaison linéaire de mélanges propres et on peut montrer facilement que ce

théorème vaut encore dans le cadre des commutations partielles. Le problème du support a été résolu dans le cadre non commutatif par Duchamp et Thibon [**?**]. Ce chapitre répond à la question suivante: quels sont les alphabets à commutations pour lesquels ce problème se généralise de façon "agréable"? (c.-à-d. la solution est proche du cadre non commutatif). En fait, nous verrons que ce n'est pas toujours le cas et nous donnerons la famille d'alphabets qui satisfait à cette condition.

Le chapitre trois est consacré à la généralisation du produit de mélange à d'autres monoïdes. On a vu que la généralisation de ce produit au cas partiellement commutatif passe par la projection de son coproduit. Pour trouver une généralisation, il suffit donc de trouver les congruences compatibles avec ce dernier. Tout d'abord, nous montrerons que la notion de mélange d'automates à multiplicités dans un semi-anneau et sur un monoïde quotient $A^*/_{\equiv}$ est stable si (et seulement si quand on considère les automates minimaux à multiplicités dans un corps) le coproduit passe au quotient. Puis nous donnerons, une forme combinatoire explicite pour les congruences compatibles avec le produit de mélange sur des semi-anneaux qui ne sont pas des anneaux et des anneaux de caractéristiques non premières. Dans le cas des anneaux de caractéristique première, nous donnerons une décomposition des congruences. Grâce à ce coproduit, nous verrons que les notions de sous-mots, d'image miroir et d'éléments primitifs peuvent se généraliser à ces monoïdes.

Enfin, je parlerai de ma participation au projet SEA, nous donnerons un algorithme de minimisation des automates à multiplicités dans un anneau principal. Nous donnerons des exemples de minimisation dans et $[X]$. Puis j'expliquerai notre choix des structures de données afin de programmer les diverses opérations sur les automates à multiplicités sur n'importe quel semi-anneau.

Chapter 2

Factorisations partiellement commutatives libres

2.1 Factorisations du monoïde

2.1.1 Introduction

Dans ce chapitre, nous étudions quelques propriétés combinatoires des monoïdes partiellement commutatifs libres. Ces monoïdes sont des monoïdes quotients $A^*/_{\equiv}$ où A est un alphabet et $\equiv$ une congruence engendrée par des couples (ab, ba)[1]. En fait, sans perte de généralité, on ne considérera ici que les commutations.
Les commutations peuvent être représentées à minima par des graphes non-orientés sans boucle[2]. Si θ est une relation de commutation, on note $(A, \theta) = A^*/_{\equiv_\theta}$, où $\equiv_\theta$ est la congruence engendrée par les relateurs $ab \equiv_\theta ba$ pour tout couple $(a, b) \in \theta$, le monoïde partiellement commutatif libre sur l'alphabet à commutations (A, θ).
Le monoïde partiellement commutatif libre a été, déjà, l'objet de nombreuses études. Il est défini par Mazurkiewicz ([?]) en 1977, dans le cadre du parallélisme, mais il apparaît dans des articles antérieurs comme celui de P.Cartier et D.Foata [?]. En fait il est étudié selon trois voies:

[1] Les seuls monoïdes admettant un produit de mélange sur un anneau de caractéristique 0 sont les monoïdes quotients $A^*/_{\equiv}$ où $\equiv$ est engendrée par des couples de la forme (a, b) ou (ab, ba) avec $a, b \in A$ [?].

[2] "Independance alphabet" dans *The book of traces* [?]

- Algébrique par Cartier et Foata [?], Dick [?], Droms [?, ?])...
- Combinatoire par Cori [?],Choffrut et Duboc ([?, ?]),Viennot [?]), Duchamp et Krob [?, ?, ?]), Lalonde [?], Kobayashi ([?]), Sakarovitch ([?, ?], Perrin [?]...
- Informatique par Zielonka [?, ?],Aalbersberg et Hoogebomm [?], Diekert [?, ?], Gastin [?, ?, ?], Gaubert et Mairesse [?, ?], Muscholl [?], Vuillon [?]...

Dans la suite, nous utiliserons essentiellement les notations que l'on peut trouver dans "*The book of traces*" [?]. Le monoïde partiellement commutatif libre admet une réalisation géométrique remarquable trouvée par X. Viennot, celle des empilements qui a trouvé son application toute naturelle dans l'étude de problèmes de "job-shop" [?, ?, ?].
Par exemple, si on considère les commutations suivantes

(10,2) (2.5,0)(7,0) (4,0)(4.7,1.5) (5.5,0)(4.7,1.5)
(2.5,0)[linestyle=none,fillstyle=solid]**b** (4,0)[linestyle=none,fillstyle=solid]**d**
(5.5,0)[linestyle=none,fillstyle=solid]**a** (7,0)[linestyle=none,fillstyle=solid]**c**
(4.7,1.5)[linestyle=none,fillstyle=solid]**c**

la trace *abcde* peut être représentée par l'empilement

(-4,-1)(9,5) viewpoint=-1 -1 .8 [normal=0 0 1](0,0,0)[gridlabels=0](-1,-1)(4,2)linecolor=white,fillstyle=solid,fillcolor=gray(-1,-1)(1,1)(1,-1)(1,0)(2,-1)(2,0)(3,-1)) 000a1 0-11b2 1-12c3 2-13d4
-1-12e3

Ces monoïdes sont appelés partiellement commutatifs libres car ils sont libres pour la catégorie des alphabets à commutations. En effet, définissons un morphisme ϕ de (A, θ) dans (A', θ') comme une application telle que $(a, b) \in \theta$ implique $(\phi(a), \phi(b)) \in \theta'$ ou $\phi(a) = \phi(b)$. Tout monoïde peut être considéré lui-même comme un alphabet à commutations: en terme de catégories, on peut définir un foncteur d'oubli O de la catégorie des monoïdes dans la catégorie des alphabets à commutations par $O = (, \theta_)$ où θ est l'ensemble des couples $(x, y) \in^2$, $x \neq y$ tel que $xy = yx$. On peut donc reformuler la propriété d'universalité de (A, θ) de la façon suivante. Soit un monoïde tel qu'il existe un morphisme d'alphabet à commutations ϕ de (A, θ) dans alors il existe un unique morphisme de monoïde ϕ de (A, θ) dans tel que $\phi = \phi \circ i_\theta$ (où i_θ est l'injection canonique de (A, θ) dans (A, θ)).

(3,3) (0.5,2.5)(A,θ) ->(1,2.5,1)(2.2,2.5) (2.5,2.5) (1.5,2.8)ϕ (1.5,0.5)(A,θ)
->(0.4,2.2)(1.45,0.8) ->(1.55,0.8)(2.4,2.2) (0.4,1.4)i (2.4,1.4)ϕ

En particulier si $M =^{(A)}$, on obtient une flèche naturelle $M \xrightarrow{\phi}{}^{(A)}$ qui fournit le multidegré. Les $M_\alpha = \phi^{-1}(\alpha)$ sont appelées classes de multihomogénéité de M. La donnée de $= (A, \theta)$ est équivalente à celle de (A, θ) car $A = -(-1)^2 - 1$ et $\theta = \{(x, y) \in A \times A | x \neq y \text{ et } xy = yx\}$, nous serons amenés de nombreuses fois dans la suite à discuter d'une propriété de en fonction de la forme de (A, θ).

Nous nous intéresserons ici à la notion de factorisation. Cette notion est bien connue dans le monoïde libre et a été intensivement étudiée dans [?], [?], [?], [?], [?] et [?][3]. La première partie, qui contient les premiers résultats de ce mémoire, porte sur un travail que j'ai réalisé en collaboration avec G.Duchamp et M.Flouret [?], sur la combinatoire des classes de conjugaison et des factorisations de (A, θ) en monoïdes libres[4]. Il s'agit en fait d'une généralisation à ce cadre du théorème de factorisation de Schützenberger [?]. Nous verrons que les factorisations complètes admettent une "bonne combinatoire". Plus précisément, le nombre d'éléments d'une factorisation complète de multidegré égal à un multidegré donné vérifie la formule de Witt généralisée [?], ce qui fait de ce type de factorisation de bons candidats pour la réalisation de bases de $L_K(A, \theta)$. La notion de classe de conjugaison a été traitée par Duboc dans [?].
Ensuite, nous expliquerons comment généraliser les bisections de Lazard au cadre partiellement commutatif et, par itération, comment réaliser de nouvelles factorisations complètes. Cette partie provient d'un article écrit en collaboration avec G.Duchamp [?]. Enfin, nous montrerons que l'on peut étendre les notions d'ensembles de Hall et d'ensembles de Lazard à une famille particulière de monoïdes partiellement commutatifs libres en util-

[3]On connaît quelques factorisations du monoïde partiellement commutatif telles que les traces de Lyndon définies par Krob et Lalonde dans [?] et [?], on peut aussi citer une généralisation des bisections de Lazard [?, ?, ?, ?, ?] au cadre partiellement commutatif donnée par Duchamp et Krob dans [?] et [?]. Cette généralisation peut être encore étendue à celle de bisection transitive, notion stable car les membres droits et gauches d'une bisection transitive sont encore des monoïdes partiellement commutatifs libres (nous verrons que, contrairement au cas non commutatif, ce n'est pas le cas de toutes les bisections images de bisections de Lazard - c'est à dire obtenues par des éliminations d'un certain nombre de lettres-) et qui sera définie et discutée plus tard (cf. chap.2.1.4).

[4]Non commutatifs

isant ces nouvelles factorisations. J'obtiendrai alors des bases de l'algèbre de Lie partiellement commutative libre ayant des propriétés similaires aux bases de Hall du cas non commutatif. Ainsi, nous mettrons en évidence une correspondance Hall-Lazard et une algorithmique liée aux séquences standard.

2.1.2 Combinatoire des classes de conjugaison

Si $u = t^p$, on notera $\sqrt[p]{u} = t$ la *racine* $p^{\text{ième}}$ de u. L'unicité d'une telle trace est montrée dans [**?**]. Dans le même article, il est montré que si g, r, et t sont trois traces de (A, θ) telles que $g = r^q = t^p$ avec $q, p \in$, alors il existe $g' \in (A, \theta)$ et $m \in$ tels que $q|m$, $p|m$ et $g = g'^m$. Ceci permet de justifier l'existence et l'unicité d'une plus petite racine $\sqrt{g}$ d'une trace g. On peut donc définir l'*exposant* d'une trace g comme étant l'entier p tel que $g = g'^p$ où g' est la plus petite racine de g.

Exemple 1 *Soit le graphe*

$$(A, \theta) = a - b \quad c$$

on a $\sqrt{babcac} = bac$ *et* $\exp(babcac) = 2$

Deux mots w et w' du monoïde libre A^* sont dits *conjugués* lorsqu'il existe deux mots u et v tels que $w = uv$ et $w' = vu$. L'ensemble des couples conjugués forme une relation d'équivalence sur A^*. Cette notion peut s'étendre au cas partiellement commutatif. Deux traces t et t' de (A, θ) sont dites *transposées* (resp. *élémentairement transposées*) si et seulement si il existe deux traces u et v telles que $t = uv$ et $t' = vu$ (resp. une lettre $a \in A$ et une trace v telle que $t = av$ et $t' = va$); elles seront dites *conjuguées* si et seulement si il existe une trace u non triviale telle que $tu = ut'$. Clairement, si t et t' sont transposées alors elles sont aussi conjuguées. Notons cependant que la réciproque est fausse.

Exemple 2 *Soit le graphe*

$$(A, \theta) = a - b \quad c.$$

Les traces aabac et acabb sont transposées (donc conjuguées), mais aacbb et abcab sont conjuguées et non transposées puisque

$$aacbb.(aacab) = aacaabbcab = aacababcab = (aacab)abcab.$$

La transposition est une relation symétrique (en général non transitive), par contre la conjugaison est une relation d'équivalence. En effet si $tu = ut'$ et $t'v = vt"$ alors

$$tuv = ut'v = uvt".$$

En fait, la conjugaison est la fermeture transitive de la transposition [5].

La proposition suivante permet de relier les notions de classes de conjugaison et de radicaux de traces.

Proposition 1 *Soit C une classe de conjugaison, soit $f \in C, g \in (A, \theta)$ et $p \in$ tels que $f = g^p$ alors pour tout $f' \in C$, il existe $g' \in (A, \theta)$ tel que $f' = g'^p$. De plus, g' est conjuguée à g.*

Preuve Il suffit de montrer que cette propriété est vraie pour les transpositions élémentaires. Soit f' une transposée élémentaire de $f \in C$; alors il existe $a \in A$ et $u \in (A, \theta)$ tels que $f = ua$ et $f' = au$. Si a commute avec toutes les lettres de u alors $f' = au = ua = f$. Dans le cas contraire, il existe $g'' \in (A, \theta)$ telle que $g = g''a$, alors $f = g^{p-1}g''a$ et donc $f' = ag^{p-1}g'' = a(g''a)^{p-1}g'' = (ag'')^p$.

Soit C une classe de conjugaison. On déduit de ce qui précède que l'exposant est constant sur C. On appellera cet entier l'*exposant* de C. L'ensemble des traces $\{\sqrt{g}\}_{g \in C}$ forme une classe de conjugaison que l'on nommera la classe *racine* de C et que l'on notera $\sqrt{C}$.

Exemple 3 *Soit le graphe*

$$(A, \theta) = \begin{array}{ccc} a & - & b \\ | & & | \\ c & - & d. \end{array}$$

La classe de conjugaison de la trace abcdabcd est

$$C = \{abcdabcd, dbcadbca, acbdacbd, dcbadcba\}$$

On a alors $\exp(C) = 2$ *et l'ensemble*

$$\sqrt{C} = \{abcd, dbca, acdb, dcba\}$$

est la classe de conjugaison de abcd.

[5] et donc de la transposition élémentaire(voir [**?**]).

Dans le cas non commutatif, un mot est dit *primitif* s'il n'est pas puissance non triviale d'un mot plus petit. Cette notion s'étend au cas d'un monoïde partiellement commutatif. Soit (A, θ) un alphabet à commutations et t une trace, t est dite primitive si son exposant est 1. Elle est dite *fortement primitive* si et seulement si $t = uv = vu$ implique $u = 1$ ou $v = 1$.

Exemple 4 *Soit le graphe*

$$(A, \theta) = a - b \quad c.$$

La trace accb est fortement primitive, aabbaba est primitive mais non fortement, et acacac n'est pas primitive.

P.Lalonde a montré dans [?] qu'une trace est fortement primitive si et seulement si elle est primitive et connexe et que toute trace conjuguée d'une trace primitive (resp. fortement primitive) est primitive (resp. fortement primitive). Ceci permet de mettre en évidence la notion de classe de conjugaison primitive (resp. fortement primitive) définie comme étant une classe de conjugaison dont tous les éléments sont primitifs (resp. fortement primitifs).

2.1.3 Extension du théorème de factorisation de Schützenberger

Soit un monoïde et $= (_i)_{i \in J}$ une famille de sous-monoïdes de (totalement ordonnée sur J par la relation d'ordre $<$). On dit que est une *factorisation* de si tout élément x de peut s'écrire de façon unique sous la forme

$$x = f_1 \cdots f_n \text{ avec } f_i \in_{j_i}$$

avec $j_1 > j_2 > \cdots > j_n$. Par souci de clarté, dans le cas des monoïdes libres ou partiellement commutatifs libres, une factorisation sera représentée par la famille de ses générateurs minimaux[6].
Si $= (Y_i)_{i \in J}$ est une factorisation de (A, θ), on appelera $\bigcup_{i \in J} Y_i$ le contenu de la factorisation [7]. On le notera .

[6] Le monoïde (A, θ) étant localement fini alors tous ses sous monoïdes aussi. Un sous monoïde n'admet alors qu'un et un seul ensemble générateur minimal (qui s'appelle base) $-(-1)^2 - 1$, il n'y a donc pas d'ambiguïté dans cette représentation.

[7] Cette notion est due à Viennot [?]

Remarque 5 *En fait* $= (Y_i)_{i\in J}$ *est une factorisation de* (A,θ) *si et seulement si on peut écrire*

$$\underline{(A,\theta)} = \overleftarrow{\prod_{i\in J}} \underline{< Y_i >}.$$

On dit qu'une factorisation $= (_i)_{i\in J}$ est une *bisection* si $|J| = 2$; c'est une *factorisation complète* si tous les éléments de sont des singletons.

Exemple 6 *Considérons l'ordre lexicographique sur* A^+*. Les mots de Lyndon sont les mots primitifs minimaux dans leur classe de conjugaison. Ils forment une factorisation complète de* A^**.*
Si l'alphabet est $A = \{a,b,c\}$ *avec* $a < b < c$*, aababc et bbcbc sont des mots de Lyndon, contrairement à abaab et bcbc. Si l'on choisit un mot quelconque de* A^**, bbabaabbacbabbaa par exemple, il se décompose bien de façon décroissante en mots de Lyndon, soit ici bb.ab.aabbacbacbabb.a.a.*
Plus généralement, on peut créer une factorisation complète de A^* *en engendrant un ensemble de Lazard de la façon suivante. Un sous-ensemble* L *de* A^+ *est un ensemble de Lazard sur* A^* *si et seulement si il est totalement ordonné* $(\prec)$ *et que pour tout degré* n *on ait* $L \cap A^{\leq n} = \{z_1, \cdots, z_k\}$ *avec* $z_1 \prec z_2 \prec \cdots \prec z_k$ *tels qu'il existe une famille* $(Z_i)_{i\in[1..k+1]}$ *de codes vérifiant*

- $Z_1 = A$,
- $\forall i \in [1,k], z_i \in Z_i$,
- $\forall i \in [1,k], Z_{i+1} = z_i^*(Z_i - z_i)$,
- $Z_{k+1} \cap A^{\leq n} = \emptyset$.

Nous verrons dans la section **??** *comment étendre cette notion à une famille de monoïdes de traces.*
Les mots de Lyndon sont un cas particulier de factorisation de Lazard. La notion de mots de Lyndon peut se généraliser aux monoïdes partiellement commutatifs libres de la façon suivante.

Soit π_θ la surjection canonique de A^* dans (A,θ), le mot *standard* (t) d'une trace t est le plus grand mot pour l'ordre lexicographique dans $\pi_\theta^{-1}(t)$. On définit *l'ordre standard* comme l'ordre total $<$ sur (A,θ) tel que $t <'_t$ si et seulement si $(t) <_{lex} std(t')$. Les *traces de Lyndon* sont définies comme étant des traces fortement primitives minimales pour l'ordre standard dans

leurs classes de conjugaison. Dans [**?**] G.Duchamp et D.Krob montrent que l'ensemble de ces traces muni de l'ordre standard forme une factorisation complète de (A, θ). On notera cet ensemble (A, θ).

Exemple 7 *Soit le graphe*

$$(A, \theta) = c - a - b - d.$$

On a $bac <_a cb$. *En effet le plus grand élément de* $\pi_\theta(bac) = \{bac, abc, bca\}$ *pour l'ordre lexicographique est* bca *et le plus grand élément de* $\pi_\theta(acb) = \{acb, cab, cba\}$ *est* cba.

Exemple 8 *Soit le graphe*

$$(A, \theta) = c - a - b - d$$

avec $a < b < c < d$. *AFlors* $acd, acb \notin (A, \theta)$ *et* $adc \in (A, \theta)$. *En effet, ces trois traces sont conjuguées, leur classe de conjugaison est l'ensemble*

$$\{acd, dac, cda, adc\}.$$

Il faut alors rechercher le plus petit des maximaux des ensembles $\pi_\theta^{-1}(acd) = \{acd, cad\}$, $\pi_\theta^{-1}(dac) = \{dac, dca\}$, $\pi_\theta^{-1}(cda) = \{cda\}$ *et* $\pi_\theta^{-1}(adc) = \{adc\}$. *Cet élément se trouve dans* $\pi_\theta^{-1}(adc)$ *d'où le résultat.*

On a la propriété suivante.

Proposition 2 *Soit* C *une classe de conjugaison connexe. Alors,*

$$\left(C \cap \bigcup_{l \in (A,\theta)} l^* \right) = 1.$$

Preuve Soit p l'exposant de C. Puisque C est connexe, $\sqrt{C}$ est fortement primitive donc $\sqrt{C} \cap Ly(A, I) = \{l\}$. Soit $l' \in (A, \theta)$ telle que $l'^q \in C$. Alors $q = p$ et $l' \in \sqrt{C} \cap (A, \theta)$, d'où $l = l'$.

On va ici énoncer le résultat principal de cette section.
Soit $(Y_i)_{i \in J}$ une famille de sous-ensembles non-commutatifs (i.e. pour tout coupe déléments $x, y \in Y_i^2$ on a $xy \neq yx$) de (A, θ). On considère les assertions suivantes.

(I) Chaque $t \in (A, \theta)$ possède au plus une écriture sous la forme

$$t = f_1 f_2 ... f_n \text{ avec } f_i \in Y_{j_i} \text{ et } j_1 \geq j_2 \geq ... \geq j_n.$$

(II) Chaque $t \in (A, \theta)$ possède au moins une écriture sous la forme

$$t = f_1 f_2 ... f_n \text{ avec } f_i \in Y_{j_i} \text{ et } j_1 \geq j_2 \geq ... \geq j_n.$$

(III) Chaque monoïde $\langle Y_i \rangle$ est libre pour $i \in J$. Pour toute classe de conjugaison C de (A, θ), si C est connexe alors il existe un unique $i \in J$ tel que $C \cap \langle Y_i \rangle \neq \emptyset$ et dans ce cas $C \cap \langle Y_i \rangle$ est une $\langle Y_i \rangle$-classe de conjugaison (au sens non commutatif), par contre si C n'est pas connexe alors pour tout $i \in J, C \cap \langle Y_i \rangle = \emptyset$.

Schützenberger a montré dans le cas non-commutatif un analogue du théorème suivant[8][**?**].

Théorème 3 *Deux des affirmations précédentes entraînent la troisième.*

Preuve Pour tout $i \in J$, l'ensemble minimal de générateurs de $\langle Y_i \rangle$ est $F_i = (\langle Y_i \rangle - 1) - (\langle Y_i \rangle - 1)^2$. On peut remarquer que si les conditions (I) et (II) sont réunies alors $\langle Y_i \rangle$ est libre de base Y_i. Pour montrer que (I) et (II) $\Rightarrow$ (III), le lemme suivant est nécessaire.

Lemme 4 *Soit* $= (Y_i)_{i \in J}$ *une factorisation de* (A, θ) *en monoïdes libres de codes* Y_i *non commutatifs. Alors*

$$\log\left(\underline{(A, \theta)}\right) - \sum_{f \in F} \log\left(\frac{1}{1 - \underline{Y_i}}\right)$$

est une combinaison linéaire (infinie) de polynômes de la forme $uv - vu$ $(u, v \in (A, \theta))$.

Preuve Soit la famille $\left(S_i = \dfrac{1}{1 - Y_i}\right)_{i \in J}$. Pour tout $i \in J$ on a $(S_i, 1) = 1$. Il résulte de la proposition **??** (annexe A) que la différence

$$\log\left(\underline{(A, \theta)}\right) - \sum_{i \in J} \log\left(\frac{1}{1 - \underline{Y_i}}\right)$$

[8]Dans le cas non commutatif l'assertion (III) est remplacée par:
(III) Chaque monoïde $\langle Y_i \rangle$ est libre. Pour toute classe de conjugaison C de A^*, il existe un unique $i \in J$ tel que $C \cap \langle Y_i \rangle \neq \emptyset$ et dans ce cas $C \cap \langle Y_i \rangle$ est une $\langle Y_i \rangle$-classe de conjugaison.

est une série de Lie sans terme de degré 1.

D'après le lemme **??**,

$$\log(\underline{(A,\theta)}) - \sum_{i\in J} log(\underline{Y_i^*})$$

est une combinaison linéaire (peut-être infinie) de polynômes de la forme $uv - vu$ (avec $u, v \in (A,\theta)$). Soit C une classe de conjugaison.
Alors,

$$(\underline{C}, \log(\underline{(A,\theta)})) = (\underline{C}, \sum_{i\in J} \log(\underline{Y_i^*})).$$

Or

$$\underline{(A,\theta)} = \overleftarrow{\prod_{l\in(A,\theta)}} \underline{l^*},$$

et donc

$$(\underline{C}, \log(\underline{(A,\theta)}) = (\underline{C}, \sum_{l\in(A,\theta)} \log(\underline{l^*})) = (\underline{C}, \sum_{l\in(A,\theta)} \sum_{m\geq 1} \frac{1}{m} l^m).$$

De plus, comme Y_i est un code pour tout $i \in J$ (car dans le cas contraire l'assertion (I) serait fausse). On a donc

$$\log(\underline{Y_i^*}) = \sum_{m\geq 1} \frac{1}{m} \underline{Y_i^m}.$$

Finalement,

$$(\underline{C}, \sum_{l\in(A,\theta)} \sum_{m\geq 1} \frac{1}{m} l^m) = (\underline{C}, \sum_{i\in J} \sum_{m\geq 1} \frac{1}{m} \underline{Y_i^m}).$$

Deux cas se présentent alors selon que C est connexe ou non.

Supposons tout d'abord que C ne soit pas connexe. Toute trace de Lyndon l étant connexe par définition, on a pour tout $m \geq 0, (\underline{C}, l^m) = 0$. D'où

$$(\underline{C}, \sum_{i\in J} \sum_{m\geq 1} \frac{1}{m} \underline{Y_i^m}) = (\underline{C}, \sum_{l\in(A,\theta)} \sum_{m\geq 1} \frac{1}{m} l^m) = 0.$$

Ceci implique que pour tout $i \in J$, $Y_i^* \cap C = \emptyset$.
Supposons à présent que C soit connexe. Si C est fortement primitive, il résulte de [**?**] que

$$(\underline{C}, \sum_{l\in(A,\theta)} \sum_{m\geq 1} \frac{1}{m} l^m) = (\underline{C}, \sum_{l\in(A,\theta)} l) = 1,$$

et donc

$$(\underline{C}, \sum_{i\in J}\sum_{m\geq 1}\frac{1}{m}\underline{Y_i^m}) = 1.$$

Comme toutes les traces de C sont d'exposant 1, il en est a fortiori de même dans les Y_i^* et comme ces derniers sont libres on a, si $Y_i^m \cap C \neq \emptyset$, $(C \cap Y_i^m) \geq m$ et donc

$$(\underline{C}, \sum_{m\geq 1}\frac{1}{m}\underline{Y_i^m}) \geq 1.$$

Il existe donc un unique $i \in J$ tel que $C \cap Y_i^* \neq \emptyset$, de plus $Card(C \cap Y_i^m) = m$, ce qui prouve que $C \cap Y_i^*$ est une Y_i^*-classe de conjugaison.
Si C n'est pas fortement primitive (C est toujours supposée connexe) alors $\sqrt{C}$ est fortement primitive. D'après le cas fortement primitif, il existe un unique $i \in J$ tel qu'il existe $g \in Y_i^* \cap \sqrt{C}$. Alors $g^p \in C$ où p est l'exposant de C donc $C \cap Y_i^* \neq \emptyset$. Supposons que $\sqrt{g} \in \sqrt{C} \cap Y_j^*$, alors $g \in Y_i^* \cap Y_j^*$ et donc $i = j$. Ceci implique que l'exposant de g dans Y_i^* est supérieur ou égal à p. Comme p est l'exposant de g dans (A, θ) il y a en fait égalité entre ces deux entiers. Or $C \cap Y_i^*$ est une réunion de Y_i^*-classes de conjugaison.
Posons $C \cap Y_i^* = \bigcup_{1\leq j<k} C_j$ où $k \in$ et où pour tout j, C_j est une Y_i^*-classe de conjugaison. Cette union étant disjointe, on a

$$(\underline{C}, \sum_{m\geq 1}\frac{1}{m}\underline{Y_i^m}) = \sum_{j=1}^{k}(\underline{C_j}, \sum_{m\geq 1}\underline{Y_i^m}).$$

Or Y_i^* est un monoïde libre de code Y_i et donc

$$(\underline{C_j}, \sum_{m\geq 1}\frac{1}{m}\underline{Y_i^m}) = \frac{1}{p}.$$

D'où

$$(\underline{C}, \sum_{m\geq 1}\frac{1}{m}\underline{Y_i^m}) = \frac{k}{p}.$$

Or d'autre part, on a

$$(\underline{C}, \sum_{i\in J}\sum_{m\geq 1}\frac{1}{m}\underline{Y_i^m}) = (\underline{C}, \sum_{l\in(A,\theta)}\sum_{m\geq 1}\frac{1}{m}l^m) = \frac{1}{p}$$

d'après la proposition **??**. D'où l'unicité et $k = 1$.

Réciproquement, montrons que (I) et (III) (resp. (II) et (III)) impliquent (II) (resp. (I)). Soit C une classe de conjugaison de (A, θ). On considère à nouveau deux cas.

Si C est connexe, il existe un unique $i \in J$ et une unique F_i^*-classe de conjugaison C_i telle que $C_i = C \cap F_i^*$. Or

$$(\underline{C}, \sum_{i \in J} \sum_{m \geq 1} \frac{1}{m} \underline{F_i}^m) = (\underline{C_i}, \sum_{m \geq 1} \frac{1}{m} \underline{F_i}^m) = \frac{1}{p}$$

où p est l'exposant de C_i, et

$$(\underline{C}, \log(\underline{(A, \theta)})) = (\underline{C}, \sum_{l \in (A,\theta)} \sum_{m \geq 1} \frac{1}{m} l^m) = \frac{1}{p}$$

d'après la proposition **??**.
Donc,

$$(\underline{C}, \log(\underline{(A, \theta)})) = (\underline{C}, \sum_{i \in J} \sum_{m \geq 1} \frac{1}{m} \underline{F_i}^m).$$

Si C n'est pas connexe, on a

$$(\underline{C}, \log(\underline{(A, \theta)})) = (\underline{C}, \sum_{l \in (A,\theta)} \sum_{m \geq 1} \frac{1}{m} l^m) = 0.$$

D'autre part,

$$(\underline{C}, \sum_{i \in J} \sum_{m \geq 1} \frac{1}{m} \underline{F_i}^m) = 0$$

par hypothèse.
Ainsi, pour toute classe de conjugaison C, connexe ou non, de (A, θ), on a

$$(\underline{C}, \log(\underline{(A, \theta)})) = (\underline{C}, \sum_{i \in J} \sum_{m \geq 1} \frac{1}{m} \underline{F_i}^m).$$

Soit Ω une classe de multi-homogénéïté de (A, θ). Alors Ω est une réunion de classes de conjugaison.
Donc,

$$(\underline{\Omega}, \log(\underline{(A, \theta)})) = (\underline{\Omega}, \sum_{i \in J} \sum_{m \geq 1} \frac{1}{m} \underline{F_i}^m).$$

Ceci permet d'écrire,

$$\phi[\log(\underline{(A,\theta)})] = \phi\left[\sum_{i\in J}\sum_{m\geq 1}\frac{1}{m}\underline{F_i}^m\right].$$

Où ϕ est la surjection canonique de $<< A,\theta >>$ dans $[[A]]$. Comme ϕ est continu, ceci est équivalent à

$$\log(\phi(\underline{(A,\theta)})) = \log(\prod_{i\in J}\phi(\underline{F_i^*})),$$

et donc

$$\phi(\underline{(A,\theta)}) = \prod_{i\in J}\phi(\underline{F_i^*}).$$

La condition (I) (resp. (II)) implique qu'il existe $S \in \langle\langle A,\theta\rangle\rangle$ telle que

$$\underline{(A,\theta)} = \overleftarrow{\prod_{i\in J}}\underline{F_i^*} + \epsilon.S$$

avec $(S,t) > 0$ et $\epsilon = 1$ (resp. $\epsilon = -1$) pour tout t de (A,θ).
On peut donc écrire

$$\phi(\underline{(A,\theta)}) = \epsilon.\phi(S) + \phi(\overleftarrow{\prod_{i\in J}}\underline{F_i^*}) = \prod_{i\in J}\phi(\underline{F_i^*}),$$

ce qui implique que $\phi(S) = 0$ et donc que $S = 0$ car S est à coefficients positifs. La famille $(F_i^*)_{i\in J}$ est donc une factorisation de (A,θ).

Si $A = \{a_1,\cdots,a_n\}$, on écrira $T^\alpha = a_1^{\alpha(a_1)}\cdots a_n^{\alpha(a_n)} \in (A,A^2)$ pour tout $\alpha \in^A$, en notant $\alpha = (\alpha(a_1),\cdots,\alpha(a_n))$. Soit X un sous-ensemble de (A,θ), on notera $X_\alpha = \{t \in X/\phi(t) = T^\alpha\}$

La propriété suivante se déduit du théorème **??** et de l'égalité des distributions des factorisations complètes et généralise une propriété classique dans le monoïde libre.

Proposition 5 *Soit une factorisation complète de (A,θ), et C une classe de conjugaison de (A,θ). Alors,*

$$(C\cap) = \begin{cases} 1 \text{ si } C \text{ est fortement primitive} \\ 0 \text{ sinon} \end{cases}$$

Preuve Une factorisation complète est une factorisation de (A,θ) en monoïdes libres. On peut donc utiliser le théorème **??**, et donc, si C est fortement primitive, $(C\cap) = 1$.
On aura besoin du lemme suivant.

Lemme 6 *Soit* $\alpha \in^A$, *et et deux factorisations complètes de* (A,θ). *Alors,*

$$(_\alpha) = (_\alpha).$$

Preuve On a

$$\prod_{f\in} \frac{1}{1-\phi(f)} = \prod_{\alpha\in A} \prod_{f\in\alpha} \frac{1}{1-\phi(f)} = \prod_{\alpha\in A} \left(\frac{1}{1-T^\alpha}\right)^{(\alpha)}.$$

De même,

$$\prod_{f\in} \frac{1}{1-\phi(f)} = \prod_{\alpha\in A} \left(\frac{1}{1-T^\alpha}\right)^{(\alpha)}.$$

Or, et sont deux factorisations complètes de (A,θ). Donc,

$$\underline{(A,\theta)} = \overleftarrow{\prod_{f\in}} \frac{1}{1-f} = \overleftarrow{\prod_{f\in}} \frac{1}{1-f}.$$

En appliquant le morphisme continu ϕ à cette égalité on obtient

$$\prod_{\alpha\in A} \left(\frac{1}{1-T^\alpha}\right)^{(\alpha)} = \prod_{\alpha\in A} \left(\frac{1}{1-T^\alpha}\right)^{(\alpha)}.$$

D'où

$$\prod_{\alpha\in A} \left(\frac{1}{1-T^\alpha}\right)^{(\alpha)-(\alpha)} = 1.$$

Ceci correspondant à un cas particulier du lemme 1 p.35 dans [**?**], on obtient finalement $(_\alpha) = (_\alpha)$.

Le fait que toute classe de conjugaison fortement primitive possède une trace de implique l'inégalité

$$(_\alpha) \geq (_\alpha(A,\theta)),$$

qui est stricte si et seulement si $_\alpha$ admet un élément non fortement primitif. Or (A,θ) étant une factorisation complète de (A,θ), le lemme **??** implique

que toute trace $f \in$ est fortement primitive et appartient à une classe de conjugaison fortement primitive.
Ceci prouve que les factorisations complètes de (A, θ) possèdent une combinatoire analogue au cas non commutatif. L'un des invariants de l'algorithme de constructions des ensembles de Lazard[9] est de garantir qu'à chaque étape on a utilisé au plus une fois chaque classe de conjugaison. Ceci nous permet de penser qu'il existe une construction similaire dans (A, θ). Dans la suite de ce chapitre, nous développerons une méthode permettant de généraliser les bisections de Lazard puis, pour une famille de monoïdes, les ensembles de Lazard.

2.1.4 Bisections transitives

Le but de cette section est de généraliser au cas partiellement commutatif les bisections de Lazard (cf [?] et [?] par exemple). Une bisection est le cas particulier des factorisations ne possédant que deux facteurs. Formellement, soit un monoïde, un couple $(_1, _2)$ forme une bisection si et seulement si l'application

$$\begin{array}{ccc} {}_1 \times {}_2 & \to & \\ (m_1, m_2) & \to & m_1 m_2 \end{array}$$

est une bijection.

Dans A^*, les bisections de Lazard sont définies de la façon suivante. Si B est un sous alphabet de A, alors $(A - B)B^*$ est un code et on a

$$\underline{A^*} = \underline{B^*}.\underline{((A - B)B^*)^*}.$$

Soit X un sous-ensemble de (A, θ), on pose

$$\theta_X = \{(x_1, x_2) \in X^2 | x_1) \times x_2) \subseteq \theta\}$$

Les commutations considérées ici sont strictement alphabétiques, c'est à dire que pour tout couple $(x_1, x_2) \in \theta_X$ on a $x_1) \cap x_2) = \emptyset$. On notera $\theta_= \theta_{(A,\theta)}$.
Dans [?] et [?], Choffrut introduit la notion de codes partiellement commutatifs comme étant les ensembles générateurs des sous-monoïdes partiellement commutatifs libres de (A, θ). En fait si X est un tel code, alors toute trace $t \in < X >$ admet une unique décomposition sur X aux commutations près, ou plus précisément (X, θ_X) est l'alphabet à commutations de $< X >$ [10].

[9] Procédé d'élimination de Lazard.
[10] De façon équivalente:

Exemple 9 *(i) Pour tout alphabet à commutations, les sous alphabets B de A sont des codes partiellement commutatifs.*
(ii) Considérons

$$(A, \theta) = a - b \quad c.$$

Alors l'ensemble de traces $\{c, cb, ca\}$ est un code partiellement commutatif, le monoïde engendré est en fait non-commutatif libre.
(iii) Pour le même alphabet à commutations, l'ensemble $\{b, a, ca\}$ est lui aussi un code partiellement commutatif, son graphe étant

$$a - b \quad ca$$

il est de plus isomorphe à (A, θ).
(iv) Soit maintenant l'ensemble $X = \{b, a, ca, cb\}$. Bien que ce soit un ensemble générateur minimal de $\langle X \rangle$, ce n'est pas un code partiellement commutatif. En effet on a $ca.b = cb.a$.

Dans la suite, on utilisera les notations suivantes:

- $AI(t)$ pour désigner l'alphabet initial $\{z \in A/t = zw, w \in (A, \theta)\}$ d'une trace t,
- $AT(t)$ l'alphabet terminal $\{z \in A/t = wz, w \in (A, \theta)\}$ de t,

ces notations sont empruntées à l'ouvrage [?].
Il existe une généralisation du lemme de Levi ([?] chap.1) au cadre partiellement commutatif que nous utiliserons de nombreuses fois par la suite.

Lemme 7 *(Levi) Soient $x, y, t, z \in (A, \theta)$ quatre traces telles que*

$$xy = tz.$$

---

1. Le monoïde $< X >$ est isomorphe à (X, θ_X) et $< X > -(< X > -1)^2 - 1 = X$.
2. Le diagramme suivant commute.

$$a(X, \theta)$$

$$- > abi_1 - > aci_2 < - bci_2$$

$$b(X, \theta_X) \qquad c < X >$$

Alors il existe quatre traces $p, q, r, s \in (A, \theta)$ *telles que*

$$x = pr, \quad y = sq,$$
$$t = ps, \quad z = rq.$$

et $r) \times s) \subseteq \theta$.

Déterminer si un sous monoïde $'$ d'un monoïde est le facteur gauche (droit) d'une bisection n'est pas un problème trivial. Il est montré dans [?] que si $=_1 \cdot_2$ est une bisection alors $_1$ satisfait $(u, uv \in_1) \Rightarrow (v \in_1)$. Cette condition n'est pas suffisante, en général, on peut le voir en posant $_1 = 2 \subset =$[11].
La proposition suivante traite le cas particulier des bisections de Lazard de (A, θ).

Proposition 8 *Soit* (A, θ) *un alphabet à commutations et* $B \subseteq A$. *Alors* (B, θ_B) *est le facteur droit (resp. gauche) d'une bisection de* (A, θ)

Preuve En fait, il suffit de prouver que la série $\underline{(B, \theta_B)}^{-1}.\underline{(A, \theta)}$ (resp. $\underline{(A, \theta)}.\underline{(B, \theta_B)}^{-1}$) est la série caractéristique d'un monoïde. Si l'on traite le cas gauche (le droit étant symétrique) on a

$$\underline{(B, \theta_B)}^{-1}.\underline{(A, \theta)} = \underline{< X >}$$

où $X = \{zw | z \in A - B, w \in (B, \theta_B), (zw) = \{z\}\}$.

Définition 9 *Soient* BA *un sous-alphabet (quelconque) de* A *et* $Z = A - B$ *on notera*

$$\beta_Z(B) = \{zw | z \in Z, w \in (B, \theta_B), (zw) = \{z\}\}.$$

Le monoïde $< \beta_Z(B) >$ n'est pas toujours partiellement commutatif libre. En effet si on pose

$$(A, \theta) = a - b \quad c$$

et $B = \{c\}$ alors $a, b, ac, bc \in \beta_Z(B)$ et $a.bc = b.ac$.
Il existe pourtant de nombreux cas pour lesquels $\beta_Z(B)$ est un code partiellement commutatif. Par exemple, G.Duchamp et D.Krob ont montré dans [?] que lorsque $Z = A - B$ est non- commutatif (i.e. $Z \times Z \cap \theta = \emptyset$) alors $\beta_Z(B)$ est un code non-commutatif (i.e. $< \beta_Z(B) >= \beta_Z^*(B)$).
Il existe d'autres cas. En effet, si on pose

$$(A, \theta) = a - b - c$$

[11] Elle l'est lorsque M est libre (cf. [?], [?], [?]).

et $B = \{c\}$, le monoïde $< \beta_{a,b}(c) >= (\beta_{a,b}(c), \theta_{\beta_{a,b}(c)})$ admet comme alphabet à commutations

$$\begin{array}{ccccc} & & ac & & \\ & & | & & \\ a & - & b & - & ac^2 \\ & \dots & | & \vdots & \\ & & ac^n & & \end{array}$$

Cela est équivalent à

$$\underline{\langle \beta_Z(B) \rangle} = \frac{1}{1 - (b + \sum_{n \geq 0} ac^n) + \sum_{n \geq 0} bac^n}$$

Un critère simple permettant de décider que $\beta_Z(B)$ est un code partiellement commutatif nous conduit à la définition suivante.

Définition 10 *Soit $B \subset A$. On dira que B est un sous-alphabet* transitivement factorisant (SATF) *si et seulement si pour tout $z_1 \neq z_2 \in Z$ et $w_1, w_2, w_1', w_2' \in (A, \theta)$ tels que $(z_1 w_1) = (z_1 w_1') = \{z_1\}$ et $(z_2 w_2) = (z_2 w_2') = \{z_2\}$ on a*

$$z_1 w_1 z_2 w_2 = z_2 w_2' z_1 w_1' \Rightarrow w_1 = w_1', w_2 = w_2'$$

La bisection $(B, \beta_Z(B))$ sera dite transitive.

On a le théorème suivant.

Théorème 11 *Soit $B \subset A$. les assertions suivantes sont équivalentes.*

1. *Le monoïde $< \beta_Z(B) >$ est partiellement commutatif libre,*
2. *Le sous alphabet B est SATF,*
3. *Pour tout couple $(z, z') \in Z^2 \cap \theta$, le graphe de non commutation*[12] *n'admet aucun graphe partiel de la forme*

   $$z - b_1 - \ldots - b_n - z'$$

   avec $b_1, ..., b_n \in B$,
4. *Pour tout couple $(z, z') \in Z^2$ on a*

   $$(z, z') \in \theta \Leftrightarrow \beta_z(B) \times \beta_{z'}(B) \subseteq \theta.$$

[12] Dependence graph [?].

Preuve Prouvons tout d'abord l'implication (1)⇒(2) par contraposition. Si B n'est pas un SATF, on peut trouver quatre traces z_1w_1, z_1w_1', z_2w_2, $z_2w_2' \in \beta_Z(B)$ telles que $z_1w_1.z_2w_2 = z_2w_2'.z_1w_1'$ avec $w_1 \neq w_1'$ ou $w_2 \neq w_2'$, ce qui implique que $\beta_Z(B)$ n'est pas un code partiellement commutatif.

Montrons maintenant que (2)⇒(3). Supposons que

$$z - b_1 - \ldots - b_n - z',$$

avec $(z, z') \in Z^2 \cap \theta$ et pour tout $i \in [1, n]$, $b_i \in B$, soit un graphe partiel du graphe de non commutation. Alors il existe un sous-graphe du graphe de non commutation de la forme

$$z - c_1 - \ldots - c_m - z'$$

avec $c_i \in B$. Soit k le plus petit entier tel que $(c_{k+1}, z') \notin \theta$. Alors on a

$$zc_1 \ldots c_k.z'c_{k+1} \ldots c_m = z'.zc_1 \ldots c_m,$$

ce qui prouve que B n'est pas un SATF.

Montrons que (3)⇒ (1). Supposons que $zw_1.z'w_2 = z'w_2'.zw_1'$ avec

$$zw_1, z'w_2, zw_1', z'w_2' \in \beta_Z(B)$$

et

$$w_2' \neq w_2, \quad w_1' \neq w_1.$$

Le lemme de Levi appliqué à l'équation

$$zw_1.z'w_2 = z'w_2'.zw_1'$$

implique l'existence d'une trace $w' \in (B, \theta_) - \{1\}$ telle que $w_1' = w_1w'$ et $w_2 = w_2'w'$. De plus, si $zw \in \beta_Z(B)$ et $b \in w$), il existe un graphe partiel du graphe de non commutation de la forme

$$z - b_1 - \ldots - b_n - b.$$

Il en découle, si on prend $c \in w'$), que le graphe de non commutation admet un graphe partiel de la forme

$$z - b_1 - \ldots - b_n - c - b_m' - \ldots - b_1' - z'.$$

Ceci prouve que (3)⇒(1).

Montrons que (3)⇒ (4). Supposons que l'on ait (3). Si $\beta_z(B) \times \beta_{z'}(B) \subseteq \theta$ alors de façon triviale $(z, z') \in \theta$.
Réciproquement, supposons que $(z, z') \in \theta$. Soient $zw \in \beta_z(B)$ et $z'w' \in \beta_{z'}(B)$. Si $(zw, z') \notin \theta$, comme $z \neq z'$ et $|w|_Z = 0$, on a nécessairement $zw.z' \neq z'.zw$. Ceci implique qu'il existe un graphe partiel du graphe de dépendance de la forme

$$z - b_1 - \ldots - b_n - z'$$

avec $b_i \in w) \subset B$ pour tout $i \in [1, n]$, ce qui contredit (3). Supposons maintenant que $(z', zw) \in \theta$ et $(z'w', zw) \notin \theta$. On peut alors écrire $zw.z'w' = z'u.zwv$ où $w' = uv$ et u est le plus grand préfixe de w' tel que $(u, zw) \in \theta$. Ceci implique alors que $zwv, z'u \in \beta_Z(B)$, et donc B n'est pas un SATF. Or on a vu que (2)⇔ (3). Cela contredit donc nos hypothèses et prouve l'assertion.

Enfin, montrons que (4)⇒(1). Soit μ l'application de Z dans $K << A, \theta >>$ définie par $\mu z = \underline{\beta_z(B)}$.
Comme

$$(z, z') \in \theta_Z \Rightarrow [\mu z, \mu z'] = [\underline{\beta_z(B)}, \underline{\beta_{z'}(B)}] = 0$$

et que $(\mu z, 1) = 0$, on peut étendre μ en un morphisme continu de $K << Z, \theta_Z >>$ dans $K << A, \theta >>$. Soit s le morphisme de $< \beta_z(B) >$ dans (Z, θ_Z) défini par $szw = z$ pour tout $zw \in \beta_Z(B)$.
On a

$$\begin{array}{rcl} \underline{< \beta_z(B) >} & = & s^{-1}(\underline{(Z, \theta_Z)}) \\ & = & \sum_{w \in (Z, \theta_Z)} s^{-1}(w) \\ & = & \sum_{w \in (Z, \theta_Z)} \mu w \\ & = & \mu\underline{(Z, \theta_Z)} \end{array}$$

Soit le polynôme $P(\theta_Z) = \frac{1}{\underline{(Z, \theta_Z)}}$. Comme μ est un morphisme continu, on a

$$< \beta_Z(B) >= \frac{1}{\mu(P(\theta_Z))} = \frac{1}{P(\theta_{\beta_Z(B)})}.$$

C'est la série caractéristique de $(\beta_Z(B), \theta_{\beta_Z(B)})$.

Remarque 10 *Ceci prouve que la liberté de $\beta_Z(B)$ (qui est généralement infini) est décidable. Grâce à l'assertion (3) du théorème* **??**, *nous ramenons le problème à un calcul de composantes connexes sur les graphes engendrés par les alphabets $B \cup \{z, z'\}$ pour tout couple $(z, z') \in \theta_Z$.*

Exemple 11 *1. Soit (A, θ) le graphe de commutation suivant.*

(2,0)(13,8) linestyle=dashed, framearc=1,fillstyle=solid,
fillcolor=$mon_gris(3,5)(11,7.5)(3,0.5)(12,3)[135](4.5,6.0)a[45](9.5,6.0)e[270](4.5,1.5)d[270](7.5,1$

Alors $B = \{b, c, d\}$ n'est pas un SATF. En effet, le graphe de non commutation admet le graphe partiel

$$a - b - d - e.$$

Cela peut aussi se vérifier en constatant l'égalité $ed.ab = a.edb$.

2. Soit (A, θ) le graphe de commutation suivant.

(7,7) linecolor=red(1,5.5)(3.5,3.5)(1,1.5)(6,5.5) (1,5.5)(6,5.5)
(1,5.5)(1,1.5) (1,1.5)(6,1.5) (6,1.5)(6,5.5)
*(1,5.5)[linestyle=none,fillstyle=solid]***c**
*(1,1.5)[linestyle=none,fillstyle=solid]***d**
*(3.5,3.5)[linestyle=none,fillstyle=solid]***a**
*(6,1.5)[linestyle=none,fillstyle=solid]***b**
*(6,5.5)[linestyle=none,fillstyle=solid]***e** *linestyle=dashed [linearc=0.5,linecolor=green](0.25,.75)(0.25,6.25)(1.75,6.25)(1.75,2.25)(6.75,2.25)*
(6.75,.75) [linearc=0.5,linecolor=green](2.75,3.75)(3.75,2.75)(6.75,5.25)(5.75,6.25)
(4.5,3.75)Z *(3.5,1.2)*B

Alors $B = \{a, d, b\}$ est un SATF de A. Cela peut se vérifier sur le graphe de non commutation.

(7,7) linecolor=red(1,5.5)(7,7)(6,1.5)(3.5,3.5)(6,1.5)(1,1.5)(2.25,
*4.5)(6,5.5)(6,5.5) (1,5.5)[linestyle=none,fillstyle=solid]***c**
*(1,1.5)[linestyle=none,fillstyle=solid]***d**
*(3.5,3.5)[linestyle=none,fillstyle=solid]***a**
*(6,1.5)[linestyle=none,fillstyle=solid]***b**
*(6,5.5)[linestyle=none,fillstyle=solid]***e**

En effet, les lettres a et e sont sur deux composantes connexes différentes.

Le graphe

$$\begin{array}{c}(2,0)(14,7)\ \ framearc{=}1\ (1.5,3.5)(13.5,6.5)\ (2,0.5)(10.5,3)\\ border{=}2pt\ (3,4.5)(3,2)\ (3,4.5)(8,2)\ (6.5,4.7)(3,2)\ (6.5,4.7)(8,2)\\ (10.5,4.7)(3,2)\ (10.5,4.5)(8,2)\ \ fillstyle{=}solid,\\ fillcolor{=}mon_gris(3,5)(.7,.7)(11,5)(2,1)(8,2)(.7,.7)(3,5)ab^+\\ (6.5,4.7)[linestyle{=}none,fillstyle{=}solid]a\ (11,5)ab^+c(b+c)^*\\ (5,6)\beta_a(c,d,b)\ (5,1)\beta_e(c,d,b)\ (3,2)[linestyle{=}none,fillstyle{=}solid]e\\ (8,2)ed^+\end{array}$$

est le graphe de commutation de $< \beta_Z(B) >$.

2.1.5 Factorisations transitives

Rappelons tout d'abord quelques définitions données par Viennot dans [**?**] et [**?**].

Définition 12 *Soit un monoïde et* $'\subseteq$ *un sous-monoïde. Soit* $=(_i)_{i\in J}$ *une factorisation de . On notera* $|_{'}=(_{i_k})_{k\in K}$ *où* $K=\{k\in J/_k\subseteq{}'\}$ *la* restriction *de à* $'$.

Remarque 12 *En général, la restriction d'une factorisation à un monoïde n'est pas une factorisation.*

Définition 13 *Soit un monoïde. On définit* $\prec$ *l'ordre partiel sur l'ensemble des factorisations de par* $=(_i)_{i\in J}\prec'=(_i')_{i\in J'}$ *si et seulement si* J' *admet une décomposition en une somme ordonnée d'intervalles* $J'=\sum_{i\in J}J_i$ *telle que pour tout* $i\in J$, *la famille* $(_j')_{j\in J_i}$ *soit une factorisation de* $_i$. *On dira dans ce cas que* $'$ *est* plus fine *que .*

On a, de façon triviale, la propriété suivante.

Proposition 14 *Soit un monoïde. Soient* $=(_i)_{i\in I}$ *et* $'$ *deux factorisations de telle que* $\preceq'$. *Alors pour tout* $i\in I$, $'|_i$ *est une factorisation de* $_i$.

Définition 15 *Soient* $= (B_1, B_2)$ *une bisection et* $= (Y_i)_{i\in J}$ *une factorisation toutes deux de* (A, θ). *On dira que* Y_i *est* coupé *par* $$ *si et seulement si les monoïdes* $_i() =< B_1 > \cap < Y_i >$ *et* $_i() =< B_2 > \cap < Y_i >$ *sont non-triviaux (i.e. différents de* 1*).*

Nous aurons, dans la suite, besoin du lemme suivant.

Lemme 16 *Soient* $= (B_1, B_2)$ *une bisection de* (A, θ) *et* $= (Y_i)_{i\in[1,n]}$ *une factorisation de* (A, θ) *telles qu'il existe une factorisation* $= (G_k)_{k\in K}$ *telle que* $, \preceq$ *alors* $\preceq$ *si et seulement si aucun* Y_i *n'est coupé par* $$.

Preuve Comme $, \preceq, K$ peut se décomposer en une somme ordonnée d'intervalles

$$K = J_1 + J_2 = \sum_{i\in[1,n]} I_i$$

en accord avec la définition **??**. Il existe donc un entier $k \in [1, n]$ tel que $J_1 = \sum_{i\in[1,k-1]} {}_i + I'_K$ et $J_2 = I''_k + \sum_{i\in[k+1,n]} I_i$ avec $I_k = I'_k + I''_k$. Ceci prouve le résultat.

(7,4) (1,3.4)(6,3.4) (6.5,3.4) (1,3.35)(1,3.45) (4.5,3.35)(4.5,3.45) (1,2)(6,2) (6.5,2) (1,2.05)(1,1.95) (3,2.05)(3,1.95) (4.5,2.05)(4.5,1.95) (5,2.05)(5,1.95) (5.5,2.05)(5.5,1.95) (6,2.05)(6,1.95) (1,1)(6,1) (6.5,1) (1,1.05)(1,0.95) (3,1.05)(3,0.95) (4.5,1.05)(4.5,0.95) (5,1.05)(5,0.95) (5.5,1.05)(5.5,0.95) (6,1.05)(6,0.95) (3.4,1.05)(3.4,0.95) (2.1,1.05)(2.1,0.95) (2.5,1.05)(2.5,0.95) (5.7,1.05)(5.7,0.95) linestyle=dashed (4.5,3.4)(4.5,1) (3,2)(3,1) (5,2)(5,1) (5.5,2)(5.5,1)

Définition 17 *Soit* $= (_i)_{i\in I}$ *une factorisation d'un monoïde* $$ *et pour un* $k \in I$, *soit* $' = (_i')_{i\in I'}$ *une factorisation de* $_k$. *La* composition *de* $$ *et* $'$ *est la factorisation* $'\circ = (_i'')_{i\in I''}$ *où l'ensemble* $I'' = I \cup I' - \{k\}$ *est ordonné par la relation* $i < j$ *si et seulement si*

1. $(i, j \in I$ *et* $i <_I j)$ *ou* $(i, j \in I'$ *et* $i <_{I'} j)$,
2. $i \in I, i <_I k$ *et* $j \in I'$,
3. $i \in I'$, $j >_I k$ *et* $j \in I$

et

$$'' = \begin{cases} _i & si\ i \in I \\ '_i & si\ i \in I' \end{cases}$$

Définition 18 *On appellera* factorisation transitive *toute factorisation qui est composée de bisections transitives.*

(7,4) (1,3)(6,3) (1,2)(1.9,2) (2.1,2)(3.9,2) (4.1,2)(6,2) (1,1)(6,1)
(1,3.2)(1,2.8) (2,3.2)(2,2.8) (4,3.2)(4,2.8) (6,3.2)(6,2.8) (1,2.2)(1,1.8)
(1.3,2.2)(1.3,1.8) (1.9,2.2)(1.9,1.8) (2.1,1.8)(2.1,2.2) (2.5,1.8)(2.5,2.2)
(3.2,1.8)(3.2,2.2) (3.9,1.8)(3.9,2.2) (4.1,1.8)(4.1,2.2) (5,1.8)(5,2.2)
(6,1.8)(6,2.2) (1,0.8)(1,1.2) (1.3,0.8)(1.3,1.2) (2,0.8)(2,1.2) (2.5,0.8)(2.5,1.2)
(3.2,0.8)(3.2,1.2) (4,0.8)(4,1.2) (5,0.8)(5,1.2) (6,0.8)(6,1.2) linestyle=dashed
(1.3,2)(1.3,1) (2,3)(2,1) (2.5,2)(2.5,1) (3.2,2)(3.2,1) (4,3)(4,1) (5,2)(5,1)
(0.5,3) (1.5,2.5)$_1$ (3,2.5)$_2$ (5,2.5)$_3$ (3.5,0.5)$_3$ $\circ_2$ $\circ_1\circ$

Exemple 13 *Si on considère le graphe*

$$\begin{array}{ccc} a & - & b \\ | & & | \\ d & - & c \end{array}$$

et les bisections transitives $_1 = (a, \{d, b\} \cup ca^*)$ *et* $_2 = (ca^*, \{d, b\})$ *alors la factorisation*

$$= (a, ca^*, \{b, d\}) =_2 \circ_1$$

est transitive.

Lemme 19 *Soit* $= (Y_i)_{i\in[1,p]}$ *une factorisation transitive de* (A, θ) *et soit* $= (B, \beta_Z(B))$ *une bisection transitive telle qu'il existe une factorisation plus fine que et . Alors, il existe au plus un* Y_i *coupé par et si un tel facteur existe il vérifie les assertions suivantes*

1. *Le sous-ensemble* $T = Y_i \cap (B, \theta_B)$ *est un SATF de* Y_i *et* $_i()$ *est le monoïde droit de la bisection associée (c'est à dire* $_i() = (\beta_{Y_i - T})(T), \theta_{\beta_{Y_i-T}(T)}))$,
2. *La famille* $(Y_1, \ldots, Y_{i-1}, T)$ *est une factorisation transitive de* (B, θ_B),
3. *La famille* $(\beta_{Y_i-T}(T), Y_{i+1}, \ldots, Y_1)$ *est une factorisation transitive de* $(\beta_Z(B), \theta_{\beta_Z(B)})$

Preuve Supposons que $i > j$ soient deux indices de I tels que Y_i et Y_j soient coupés par . Alors, le fait que et aient un majorant commun implique que

$$_j() \subseteq (B, \theta_B) \cap (\beta_Z(B), \theta_{\beta_Z(B)}) = \{1\}$$

et contredit le fait que Y_j soit coupé par . D'où $i = j$.

(7,4)
(1,3.4)(6,3.4) (6.5,3.4) (1,3.35)(1,3.45) (4,3.35)(4,3.45) (1,2)(6,2) (6.5,2)
(1,2.05)(1,1.95) (3,2.05)(3,1.95) (4.5,2.05)(4.5,1.95) (5,2.05)(5,1.95)
(5.5,2.05)(5.5,1.95) (6,2.05)(6,1.95) (1,1)(6,1) (6.5,1) (1,1.05)(1,0.95)
(3,1.05)(3,0.95) (4.5,1.05)(4.5,0.95) (5,1.05)(5,0.95) (5.5,1.05)(5.5,0.95)
(6,1.05)(6,0.95) (3.4,1.05)(3.4,0.95) (2.1,1.05)(2.1,0.95) (2.5,1.05)(2.5,0.95)
(5.7,1.05)(5.7,0.95) (4,1.05)(4,0.95) (3.5,1.7)T (4.6,1.7)$\beta_{Y_i}(T)$ (4,2.4)Y_i
linestyle=dashed (4,3.4)(4,1) (3,2)(3,1) (5,2)(5,1) (5.5,2)(5.5,1) (4.5,2)(4.5,1)

Supposons qu'il existe un indice $i \in I$ tel que Y_i soit coupé par . Montrons tout d'abord l'assertion (1).
Par identification des facteurs on trouve alors

$$\underline{(B, \theta_B)} = \prod_{l<i} \underline{(Y_l, \theta_{Y_l})}.S_1$$

et

$$\underline{(\beta_Z(B), \theta_{\beta_Z(B)})} = S_2. \prod_{l>i} \underline{(Y_l, \theta_{Y_l})}$$

Avec $\underline{(Y_i, \theta_{Y_i})} = S_1.S_2 = (1 + S_1^+)(1 + S_2^+) = 1 + S_1^+ + S_2^+ + S_1^+S_2^+$. Donc[13]

$$S_1 = \underline{(Y_i, \theta_{Y_i})} \odot \underline{(B, \theta_B)} = \underline{(Y_i, \theta_{Y_i}) \cap (B, \theta_B)}$$

$$S_2 = \underline{(Y_i, \theta_{Y_i})} \odot \underline{(\beta_Z(B), \theta_{\beta_Z B})} = \underline{(Y_i, \theta_{Y_i}) \cap (\beta_Z(B), \theta_{\beta_Z(B)})}$$

Si on pose $T = Y_i \cap (B, \theta_B)$, on a alors

$$(Y_i, \theta_{Y_i}) \cap (B, \theta_B) = (T, \theta_T)$$

D'où

$$\underline{(Y_i, \theta_{Y_i})} = \underline{(T, \theta_T)}.S_2.$$

[13]Le signe $\odot$ désigne le produit de Hadamard des séries défini par $(S \odot T, w) := (S, w)(T, w)$

Ceci prouve que S_2 est la série caractéristique de $\langle \beta_{Y_i - T}(T) \rangle$ dans la bisection $' = (T, Y_i - T)$. De plus $Y_i - T \in (\beta_Z(B), \theta_{\beta_Z(B)})$.
On va montrer maintenant que T est un SATF de Y_i (ce qui correspond à l'assertion (1)).
Supposons que T ne soit pas $SATF$. Alors, il existe $y_1, y_2 \in Y_i - T$ tel que $(y_1, y_2) \in \theta_{Y_i}$ et une suite $(t_i)_{i \in [1,p]}$ (avec $p > 0$) d'éléments de T telle que

$$y_1 - t_1 - ... - t_p - y_2$$

soit un graphe partiel du graphe de non commutation de θ_{Y_i}. De plus, comme Y_i est le code d'un facteur d'une factorisation $SATF$, alors toute trace t_i est connexe.
On aura besoin du lemme suivant.

Lemme 20 *Soient (A, θ) un alphabet à commutations et B un SATF de A. Soit $t \in (\beta_Z(B), \theta_{\beta_Z}(B)$ une trace connexe. Alors pour tout couple de lettres $(x, y) \in (t) \times (t)$, il existe une chaîne de non commutations*

$$x - a_1 - \cdots - a_n - y$$

où $a_i \in t$).

Preuve Soit $x \in (t)$ et $y \in AT(t)$. Alors, comme $t \in (\beta_Z(B), \theta_{\beta_Z}(B)$, on a nécessairement $x \in Z$. Par contre pour y, il faut considérer deux cas.

1. Si $y \in B$, lorsqu'il n'existe pas une telle chaîne on peut écrire $t = yt'$, ce qui contredit la définition de $\beta_Z(B)$.

2. Si $y \in Z$, supposons qu'il n'existe pas ce type de chaîne de non commutation. Alors on peut écrire t sous la forme

   $$t = xwz_1w_1 \cdots z_kw_ky = yxwz_1w_1 \cdots z_kw_k$$

   avec $z_iw_i, xw \in \beta_Z(B)$. Or B est un SATF donc cette commutation est alphabétique, ce qui signifie que t est non connexe et contredit nos hypothèses.

Comme Y_i est le code d'un facteur d'une factorisation transitive, il existe un SATF B' de A tel que $Y_i \subset (B', \theta_{B'})$. Le fait que

$$y_1 - t_1 - \ldots - t_p - y_2$$

soit une chaîne de non commutation implique que la trace $y_1 t_1 \cdots t_n y_2$ est connexe. Soit $a \in (y_1)$et $b \in (y_2)$. Alors le lemme **??** montre qu'il existe une suite de lettres $(c_i)_{i\in\{1,\ldots,q\}}$ telle que

$$a - c_1 - \cdots - c_q - b$$

soit une chaîne de non commutation.
Posons

$$\alpha := \max\{j \in \{1,\ldots,q\} | c_j \in y_1)\}$$

et

$$\beta := \min\{j \in \{1,\ldots,q\} | c_j \in y_2)\}$$

Comme $(y_1, y_2) \in \theta_{Y_i}$ on a $\beta - \alpha > 0$ et

$$c_\alpha - c_{\alpha+1} - \ldots - c_{\beta-1} - c_\beta$$

est une chaîne de non commutation. Et donc

$$y_1 - c_{\alpha+1} - \cdots - c_{\beta-1} - y_2$$

aussi. On posera $a_1 := c_{\alpha+1}, \ldots, a_l := c_{\beta-1}$.
On peut supposer que $i = j$ si et seulement si $a_i = a_j$. En effet, si $a_i = a_j$ alors

$$y_1 - a_1 - ... - a_{i-1} - a_j - a_{j+1} - ... - a_l - y_2$$

est une chaîne de non commutation.
Posons $y_1 = z_1 w_1 ... z_k w_k$ et $y_2 = z'_1 w'_1 ... z'_{k'} w_{k'}$ où $z_i, z'_j \in Z$ et $z_i w_i, z'_j w'_j \in \beta_Z(B)$. Comme $(y_1, a_1) \notin \theta$, il existe $i \in [1, k]$ tel que $(z_i w_i, a_1) \notin \theta$. Si $a_1 \in Alph(w_i)$ alors il existe un facteur gauche u de w_i tel que $z_i u a_1 \in \beta_Z(B)$. Si $a_1 \notin Alph(w_1)$, alors $z_i w_i a_1 \in \beta_Z(B)$.

Ceci implique, grâce au lemme **??**, que dans tous les cas, il existe un graphe partiel du graphe de non commutation de θ de la forme

$$z_i - b_1 - ... - b_t - a_1$$

avec $b_1, ..., b_t \in B$. De même on montre qu'il existe un graphe partiel du graphe de non commutation de θ de la forme

$$z'_j - c_1 - ... - c_s - a_l$$

avec $j \in [1, k']$ et $c_1, ..., c_s \in B$. Ceci implique que

$$z_i - b_1 - ... - b_t - a_1 - ...a_l - c_s - ... - c_1 - z'_j$$

est un graphe partiel du graphe de non-commutation de θ. Or $(z_i, z_j) \in \theta$, donc B n'est pas un SATF de A. Il y a une contradiction avec les hypothèses, ce qui prouve que T est un SATF de Y_i.

Montrons maintenant (2) et (3) par induction sur p.
Si $p = 1$ alors le résultat est trivial, sinon on peut écrire sous la forme $=_1 \circ_2 \circ'$ où $' = (B', \beta_{Z'}(B'))$ est une bisection transitive, $_1 = (Y_1, \ldots, Y_k)$ une factorisation transitive de (B', θ'_B) et $_2 = (Y_{k+1}, \ldots Y_p)$ une factorisation transitive de $(\beta_{Z'}(B'), \theta_{\beta_{Z'}(B')})$. Si $='$ alors le résultat est trivial. Dans le cas contraire, le fait que et $'$ aient un majorant commun implique que l'on a nécessairement $B \subset B'$ ou bien $B' \subset B$. Supposons tout d'abord $B' \subset B$, et considérons la trisection transitive $(B', \beta_{B-B'}(T), \beta_Z(B))$. Les hypothèses d'induction impliquent que

$$(Y_{k+1}, \ldots, Y_{i-1}, T) \text{ et } (\beta_{Y_i - T}(T), Y_{i+1}, \ldots, Y_p)$$

sont des factorisations transitives, respectivement, des monoïdes

$$(\beta_{B-B'}(B'), \theta_{\beta_{B-B'}(B)}) \text{ et } (\beta_Z(B), \theta_{\beta_Z(B)}).$$

Alors

$$(Y_1, \ldots, Y_{i-1}, T) =_1 \circ(Y_{k+1}, \ldots, Y_{i-1}) \circ (B', \beta_{B-B'}(B'))$$

est une factorisation transitive.
Maintenant supposons $B \subset B'$. En utilisant les hypothèses d'induction, les factorisations $(Y_{k+1}, \ldots, Y_{i-1}, T)$ et $(\beta_{Y_i - T}(T), Y_{i+1}, \ldots, Y_p)$ sont transitives et

$$(\beta_{Y_i - T}(T), Y_{i+1}, \ldots, Y_1) =_2 \circ(\beta_{Y_i - T}, Y_{i+1,\ldots,Y_k}) \circ (B' - B, \beta_{\beta_Z(B) - B'}(B' - B))$$

est une factorisation transitive. Ceci prouve le résultat.

(7,4) (1,3.4)(6,3.4) (6.5,3.4) (1,3.35)(1,3.45) (4,3.35)(4,3.45) (1,2)(6,2) (6.5,2) (1,2.05)(1,1.95) (3,2.05)(3,1.95) (4.5,2.05)(4.5,1.95) (5,2.05)(5,1.95) (5.5,2.05)(5.5,1.95) (6,2.05)(6,1.95) (1,1)(6,1) (6.5,1) (1,1.05)(1,0.95) (3,1.05)(3,0.95) (4.5,1.05)(4.5,0.95) (5,1.05)(5,0.95) (5.5,1.05)(5.5,0.95) (6,1.05)(6,0.95) (3.4,1.05)(3.4,0.95) (2.1,1.05)(2.1,0.95) (2.5,1.05)(2.5,0.95) (5.7,1.05)(5.7,0.95) (4,1.05)(4,0.95) (3.5,1.7)T (4.6,1.7)$\beta_{Y_i}(T)$ (4,2.4)Y_i (1,0)(6,0) (6.5,0)$'$ linestyle=dashed (4,3.4)(4,0) (3,2)(3,0) (5,2)(5,0) (5.5,2)(5.5,0) (4.5,2)(4.5,0)

Lemme 21 *Soient* $= (B, \beta_Z(B))$ *une bisection transitive et* $= (Y_i)_{i\in[1,n]}$ *une factorisation transitive telle que* $\preceq$. *Alors les factorisations* $|_{(B,\theta_B)}$ *et* $_{(\beta_Z(B),\theta_{\beta_Z(B)})}$ *sont transitives.*

Preuve Il s'agit d'un cas particulier du lemme **??** en posant $=$.

Proposition 22 *Soient* $= (Y_i)_{i\in J}$ *et* $' = (Y'_j)_{j\in J'}$ *deux factorisations transitives finies de* (A, θ) *telles qu'il existe une factorisation* $$ *avec* $,' \preceq$. *Alors il existe une factorisation transitive finie* $''$ *telle que*

1. *On a l'inégalité*
$$, ' \preceq' \preceq$$
2. *Pour tout* $j \in J$, *la factorisation* $'|_{(Y_j,\theta_{Y_j})}$ *est transitive finie.*
3. *Pour tout* $j \in J'$, *la factorisation* $'|_{(Y'_j,\theta_{'Y_j})}$ *est transitive finie.*

Preuve Sans restriction, on peut poser $J = \{1, \ldots, n\}$ et $J' = \{1, \ldots, n'\}$ avec $n, n' \in$. Raisonnons par induction sur n. Si $n = 1$, le résultat est trivial. Si $n = 2$, le résultat découle directement des lemmes **??**, **??** et **??**. Supposons alors que $n > 2$. On peut poser $=_1 \circ_2 \circ$ où $= (B, \beta_Z(B))$ est une bisection transitive de (A, θ), $_1 = (Y_1, \ldots, Y_k)$ une factorisation transitive de $(B, \beta_Z(B))$ et $_2 = (Y_{k+1}, \ldots, Y_n)$ une factorisation transitive de $(\beta_Z(B), \theta_{\beta_Z(B)})$. Grâce au lemme **??**, on peut construire la factorisation transitive finie

$$'' = \begin{cases} ' & \text{si } \preceq' \\ (Y'_1, \ldots, Y'_{i-1}, T, \beta_{Y'_i}(T), Y'_{i+1}, \ldots, Y'_{n'}) & \text{sinon} \end{cases}$$

où i est l'unique indice tel que Y'_i soit coupé par . Cette factorisation vérifie l'inégalité

$$', \preceq'' \preceq .$$

De plus chaque $''|_{(Y'_j,\theta_{Y'_j})}$ est une factorisation transitive de $(Y'_i, \theta_{Y'_i})$. En effet, si $i \neq j$ il s'agit de la factorisation triviale (sinon $''|_{(Y'_i,\theta_{Y'_i})} = (T, \beta_{Y_i}(T))$ qui est transitive d'après le lemme **??**). De la même façon, les factorisations

$$''|_{(B,\theta_B)} = (Y'_1, \ldots, Y'_{i-1}, T)$$

et

$$''|_{(\beta_Z(B),\theta_{\beta_Z(B)})} = (\beta_{Y'_i - T}, Y'_{i+1}, \ldots, Y'_{n'})$$

sont transitives.
On peut donc utiliser les hypothèses d'induction pour construire une factorisation $''_1$ telle que

1. On a l'inégalité
$$_1,'' |_{(B,\theta_B)} \preceq''_1 \preceq |_{(B,\theta_B)},$$
2. Les factorisations $''_1|_{(Y_j,\theta_{Y_j})}$ pour $j \in \{1,\ldots,k\}$ sont transitives finies,
3. Les factorisations $''_1|_{(Y'_j,\theta_{Y'_j})}$ pour $j \in \{1,\ldots,i-1\}$ et $''_1|_{(T,\theta_T)}$ sont transitives finies

et une factorisation $''_2$ telle que

1. On a l'inégalité
$$_2,'' |_{(\beta_Z(B),\theta_{\beta_Z(B)})} \preceq''_2 \preceq |_{(\beta_Z(B),\theta_{\beta_Z(B)})},$$
2. Les factorisations $''_2|_{(Y_j,\theta_{Y_j})}$ pour $j \in \{k+1,\ldots,n\}$ sont transitives finies,
3. Les factorisations $''_2|_{(Y'_j,\theta_{Y'_j})}$ pour $j \in \{i+1,\ldots,n'\}$ et la factorisation $''_2|_{(\beta_{Y'_i-T}(T),\theta_{\beta_{Y'_i-T}(T)})}$ sont transitives finies.

Posons $' =''_1 \circ''_2\circ$. On a $,' \preceq G' \preceq$. Les hypothèses d'induction, le lemme **??** et la construction de $''$ nous permettent de conclure.

(5,5) (2.5,2.5)(2.5,2.5)
hatchwidth=.1pt,fillstyle=crosshatch*,linestyle=dotted (2.5,3.5)(1.5,1.5)
$(2,4)_1$ $(3,4)_2$ $(2.5,2.5)'$ (2.5,1) ->(2,3.8)(2.5,2.7):U$\preceq$ ->(3,3.8)(2.5,2.7):U$\preceq$
->(2,3.8)(2.3,1.2):U$\preceq$ ->(3,3.8)(2.7,1.2):U$\preceq$ (6,4)Transitives finies
(6,1)Factorisations (6,3.8)(3.5,3) (6,1.2)(4,2)

Remarque 14 *La méthode de construction décrite dans la preuve de la proposition* **??** *est utile lorsque l'on veut décider si deux factorisations transitives ont un majorant commun. En effet, si on arrive à construire la factorisation $'$ la réponse est évidemment affirmative. Dans le cas contraire on s'arrête lorsque l'on doit calculer le majorant de deux bisections $(B,\beta_Z(B))$ et $(B',\beta_{Z'}(B'))$ telles que $B \not\subseteq B'$ et $B' \not\subseteq B$ (car de telles bisections n'ont pas de majorant commun).*

Exemple 15 *1. Considérons le graphe de commutation suivant*

$$(A,\theta) = a - b - c$$

avec $a > b > c$. Soient les bisections transitives $_1 = (\{b,c\}, ac^*)$ et $_2 = (c, \{b\} \cup ac^*)$. Alors on a

$$_{1,2} \preceq (A,\theta) = (c, b, a, ac, ac^2, \ldots, ac^n, \ldots)$$

La factorisation recherchée est $' = (c, b, ac^*)$.

2. Examinons un cas un peu plus compliqué.
Soit le graphe suivant

$$(A,\theta) = \begin{array}{ccccccc} a & - & b & & & & \\ | & & | & & & & \\ c & - & d & - & e & . & \end{array}$$

On condidère les trisections

$$_1 = (\{a,d,e\}, ce^*, (\{b,c\}e^+a\{a,d,e\}^* \cup be^*)(ce^*)^*)$$

et

$$\begin{aligned} _2 \;=\; & (\{a,e\}, ce \cup d(a^* \cup a\{a,e\}^*), \\ & \{b \cup c\}((ce \cup da^*e\{a,e\}^*)^* \cup \\ & \cup e^*a\{a,e\}^*(da^* \cup da^+\{a,e\}^*)^* \cup \{b, ce\}e^+(da^+\{a,e\}^*)^*). \end{aligned}$$

Ces deux trisections sont transitives. En effet, $_1$ peut s'écrire sous la forme

$$_1 =_2 \circ_1$$

avec

$$_1 = (\{a,d,e\}, \{b,c\}e^*(\{1\} \cup ea\{a,d,e\}^*)$$

et

$$_2 = (ce^*, (\{b,c\}e^+a\{a,d,e\}^* \cup be^*)(ce^*)^*)).$$

La trisection $_2$ peut, elle aussi, s'écrire comme la composée de deux bisections transitives

$$_2 =_4 \circ_3$$

avec

$$_3 = (\{a,e\}, be^* \cup ce^* \cup be\{a,e\}^* \cup ce\{a,e\}^* \cup da^* \cup da\{a,e\}^*)$$

et

$$\begin{aligned} _4 \;=\; & (ce \cup d(a^* \cup a\{a,e\}),\\ & \{b \cup c\}((ce \cup da^*e\{a,e\}^*)^* \cup \\ & \cup e^*a\{a,e\}^*(da^* \cup da^+\{a,e\}^*)^* \cup \{b,ce\}e^+(da^+\{a,e\}^*)^*)). \end{aligned}$$

Suivons l'algorithme décrit dans la proposition **??**. *On remarque tout d'abord que* $_1$ *coupe* $[ce \cup d(a^* \cup a\{a,e\}^*)]$. *Pn définit donc la factorisation transitive*

$$\begin{aligned} {}'_2 \;=\; & (\{a,e\}, d(a^* \cup a\{a,e\}^*), ce(da\{a,e\})^*,\\ & \{b \cup c\}((ce \cup da^*e\{a,e\}^*)^* \cup \\ & \cup e^*a\{a,e\}^*(da^* \cup da^+\{a,e\}^*)^* \cup \{b,ce\}e^+(da^+\{a,e\}^*)^*)). \end{aligned}$$

Si on pose $X = \{b,c\}e^*(\{1\} \cup ea\{a,d,e\}^*)$, *il faut maintenant trouver un majorant commun aux bisections* $_2$ *et*

$$\begin{aligned} {}'_2|_X \;=\; & (ce(da\{a,e\})^*,\\ & \{b \cup c\}((ce \cup da^*e\{a,e\}^*)^* \cup \\ & \cup e^*a\{a,e\}^*(da^* \cup da^+\{a,e\}^*)^* \cup \{b,ce\}e^+(da^+\{a,e\}^*)^*) \end{aligned}$$

Comme on n'a ni $ce^* \subseteq ce(da\{a,e\})^*$ *ni* $ce(da\{a,e\})^* \subseteq ce^*$, *on peut en déduire que* $_1$ *et* $_2$ *n'ont pas de majorant commun pour* $\preceq$.

Corollaire 23 *Soient* $= (Y_i)_{i\in I}$ $\preceq'$ *deux factorisations transitives finies. Pour tout* $i \in I$, *la restriction* $'|_{(Y_i,\theta_{Y_i})}$ *est une factorisation transitive finie.*

Preuve Il suffit d'utiliser la proposition précédente en posant $,' \preceq'$.

La définition suivante est l'adaptation au cas partiellement commutatif d'une définition due à Viennot [**?**].

Définition 24 *Une factorisation* $(Y_i)_{i\in I}$ *de* (A,θ) *a* **localement la propriété** P *si et seulement si pour tout sous alphabet fini* $B \subset A$ *et tout entier* $n > 0$, *il existe une factorisation* $(Y'_i)_{i\in I'}$ *avec la propriété* P *et une application strictement croissante* $\psi : I' \to I$ *vérifiant*

$$Y'_i \cap B^{\leq n} = Y_{\psi(i)} \cap B^{\leq n}$$

et

$$Y_j \cap B^{\leq n} = \emptyset$$

si $j \notin \psi(I')$.

Définition 25 *On notera* $CLTF(A, \theta)$ *l'ensemble des factorisations complètes localement transitives finies.*

Remarque 16 *Cet ensemble comprend les factorisations de Lyndon, les factorisations de Lazard dans le cas non-commutatif, les factorisations définies par Duchamp et Krob dans [?] (ces factorisations sont obtenues en effectuant des bisections transitives avec* Z *totalement non-commutatif, puis en appliquant le principe de factorisation de Lazard sur chacun des monoïdes facteurs). Il comprend aussi d'autres factorisations comme le montre l'exemple suivant:*
Considérons le graphe

$$(A, \theta) = a - b - c - d \quad .$$

On construit une factorisation complète localement transitive finie en éliminant successivement les traces c, ac^2, b, d, ac *et* a *(on obtient alors la factorisation*

$$\underline{(A, \theta)} = \underline{c^*}.\underline{(ac^2)^*}.\underline{b^*}.\underline{d^*}.\underline{(ac)^*}.\underline{a^*}.$$

où est un monoïde (non-commutatif) libre) puis en factorisant par un ensemble de Lazard sur .
Montrons que l'on ne peut pas obtenir une telle factorisation en utilisant seulement des bisections transitives avec un membre droit non-commutatif.
Examinons les différentes bisections non commutatives de (A, θ)

1. $_1 = (\{a, c\}, \beta_{b,d}(a, c))$
2. $_2 = (\{b, c\}, \beta_{a,d}(b, c))$
3. $_3 = (\{b, d\}, \beta_{a,c}(b, d))$
4. $_4 = (\{a, b, c\}, \beta_d(a, b, c))$
5. $_5 = (\{a, c, d\}, \beta_b(a, c, d))$
6. $_6 = (\{b, c, d\}, \beta_a(b, c, d))$

7. $_7 = (\{a, b, d\}, \beta_c(a, b, d))$

Imaginons que la factorisation coïncide pour $n \leq 3$ avec une factorisation transitive finie de la forme $' =_1' \circ_2' \circ_i$ pour $i \in [1, 7]$. On doit donc examiner chaque cas:

1. *impossible puisque dans notre factorisation on a $ac < b$*
2. *impossible puisque dans notre factorisation on a $ac^2 > b$*
3. *impossible puisque dans notre factorisation on a $c > b$*
4. *impossible puisque dans notre factorisation on a $a < d$*
5. *impossible puisque dans notre factorisation on a $b > a$*
6. *impossible puisque dans notre factorisation on a $ac^2 > d$*
7. *impossible puisque dans notre factorisation on a $c > a$*

Ceci prouve le résultat.

2.1.6 Algorithmes de décomposition

Soit B un sous alphabet de A non forcément SATF. Alors, on peut facilement trouver la factorisation d'une trace t suivant la bisection $(B, \beta_Z(B))$ en appliquant l'algorithme donné dans la proposition suivante.

Proposition 26 *L'algorithme*

Algorithme 17 `Décomposition_bisection`
`Entrée:` *t une trace et $= (B, \beta_Z(B))$ une bisection.*
`Sortie:` *(x, y) la factorisation de t selon*
`Début`
`Si` $|t|_Z = 0$ `Alors retourner`$(t, 1)$
`Sinon`

On pose $t = t'zw$ avec $t \in (A, \theta)$, $z \in Z$ et $w \in (B, \theta_B)$.
Soit w' le préfixe maximal de w tel que $(z, w) \in \theta$, posons alors $w = w'w''$
$(x, y) \leftarrow$`Décomposition_bisection`$(t'w',)$
`Si` $y = 1$ `Alors retourner`(x, zw'')
`Sinon retourner`$(x, y.zw'')$
`Fin si`

`Fin si`
`Fin`

calcule la décomposition d'une trace t selon une bisection de la forme $(B, \beta_Z(B))$.

Preuve Par induction sur la longueur de la trace.

Exemple 18 *Soient l'alphabet à commutations*

$$(A, \theta) = a - b - c \quad d$$

et $B = \{c, d\}$. L'algorithme **??** *trouve la décomposition de la trace dccbcabcdcac en effectuant les étapes suivantes.*

$$\begin{array}{c}(dccbcabcdc\underline{ac}, 1)\\ (dccbcab\underline{\underline{c}}dc, ac)\\ (dccbc\underline{ac}, \overline{bd}c.ac)\\ (dccb\underline{\underline{c}}, ac.bdc.ac)\\ (dccc, \overline{\overline{b}}.ac.bdc.ac)\end{array}$$

On utilise alors cet algorithme pour calculer la décomposition d'une trace selon une factorisation transitive finie.

Algorithme 19 `Décomposition_FT`
`Entrée:` *t une trace et $=_n \circ \cdots \circ =_1$ une factorisation transitive finie.*
`Sortie:` *La décomposition t selon .*
`Début`
$(x, y) \leftarrow$ `Décomposition_Bisection`$(t_{,1})$
`Si` $n = 1$ `Alors retourner`(x, y)
`Sinon`

$(x_1, \ldots, x_k) \leftarrow$ `Décomposition_FT`$(x, |_{(B,\theta_B)})$
$(x_{k+1}, \ldots, x_{n+1}) \leftarrow$ `Décomposition_FT`$(y, |_{(\beta_Z(B),\theta_{\beta_Z(B)})})$
`retourner`$(x_1, \ldots, x_n)$

`Fin si`
`Fin`

2.2 Décomposition transitive

2.2.1 Élimination transitive

Le théorème suivant montre que l'on peut généraliser l'élimination de Lazard dans $L_K(A,\theta)$ de la même façon que la bisection de Lazard dans (A,θ).

Théorème 27 *Soit (B,Z) une partition de A. Alors,*

1. *On a la décomposition en somme directe*

$$L_K(A,\theta) = L_K(B,\theta_B) \oplus J$$

où J est l'idéal de Lie engendré par

$$\tau_Z(B) = \{[\ldots[z,b_1],\ldots,b_n] | n \in, zb_1\ldots b_n \in \beta_Z(B)\}.$$

2. *La sous algèbre J est partiellement commutative libre si B est un SATF de A.*

3. *Réciproquement, si $\tau_Z(B)$ est une famille basique de J alors B est un SATF de A.*

Preuve Dans le cas (non-commutatif) libre, l'élimination de Lazard s'écrit

$$L_K(A) = L_K(B) \oplus L_K(T_Z(B))$$

où

$$T_Z(B) = \{[\ldots[z,b_1],\ldots],b_n] | n \in, z \in Z, b_1,\ldots,b_n \in B\}.$$

Soit π_θ la surjection naturelle de $L_K(A)$ sur $L_K(A,\theta)$. On remarque que

$$\pi_\theta[\ldots[z,b_1],\ldots],b_n] = 0 \Leftrightarrow zb_1\ldots b_n \notin \beta_Z(B).$$

En effet, si on suppose $zb_1\ldots b_n \notin \beta_Z(B)$ alors il existe $m \in \{1,\ldots,n\}$ tel que $(zb_1\ldots b_{m-1}, b_m) \in \theta$. Ceci prouve que $[\ldots[z,b_1]\ldots b_{m-1}], b_m] = 0$ dans $L_K(A,\theta)$. On a donc $\pi_\theta(T_Z(B)) = \tau_Z(B)$, d'où découle (1).

Montrons (2). Supposons que B est un SATF de A. Considérons l'algèbre de Lie partiellement commutative libre $L_K(\beta_Z(B),\theta_{\beta_Z(B)})$. Soit $b \in B$. On définit l'application D_b de $\beta_Z(B)$ dans $L_K(\beta_Z(B),\theta_{\beta_Z(B)})$ telle que

$$D_b(zw) = \begin{cases} zwb & \text{si } zwb \in \beta_Z(B) \\ 0 & \text{sinon} \end{cases}$$

pour tout $zw \in \beta_Z(B)$ avec $z \in Z$. On a besoin du lemme suivant.

Lemme 28 *Si B est un SATF de A alors D_b peut être étendue en une unique dérivation de $L_K(\beta_Z(B), \theta_{\beta_Z(B)})$.*

Preuve Il suffit de montrer que pour tout couple $(z_1w_1, z_2w_2) \in \theta_{\beta_Z(B)}$, on a

$$D_b(z_1w_1)z_2w_2 + z_1w_1D_b(z_2w_2) = D_b(z_2w_2)z_1w_1 + z_2w_2D_b(z_1w_1). \qquad (2.1)$$

Supposons que z_1w_1b et z_2w_2b appartiennent toutes deux à $\beta_Z(B)$. Alors, il existe des lettres $b_1, \ldots, b_n, b'_1, \ldots, b'_n \in B$ avec $n, m \geq 0$ telles que le graphe de dépendance admette le graphe partiel

$$z_1 - b_1 - \ldots - b_n - b - b'_1 - \ldots - b'_m - z_2.$$

Ceci contredit le fait que B soit un SATF de A. Donc soit $z_1w_1b \notin \beta_Z(B)$ soit $z_2w_2b \notin \beta_Z(B)$. L'équation (**??**) est alors simple a établir.

Suite de la preuve du théorème ?? On notera D_b la dérivation engendrée par D_b.
Soit D le morphisme de B dans $(L_K(\beta_Z(B), \theta_{\beta_Z(B)}))$ défini par $D(b) = D_b$. On a besoin du lemme suivant.

Lemme 29 *Il existe un morphisme de Lie*

$$L_K(B, \theta_B) \to (L_K(\beta_Z(B), \theta_{\beta_Z(B)}))$$

prolongeant D.

Preuve Grâce à la propriété d'universalité de $L_K(B, \theta_B)$, il suffit de prouver que $[D_b, D_{b'}] = 0$ lorsque $(b, b') \in \theta_B$. Soit $zw \in \beta_Z(B)$. Si $zwb, zwb' \in \beta_Z(B)$ alors

$$[D_b, D_{b'}](zw) = D_bD_{b'}(zw) - D_{b'}D_b(zw) = zwbb' - zwb'b = 0.$$

Si $zwb \notin \beta_Z(B)$ ou $zwb' \notin \beta_Z(B)$ alors

$$D_bD_{b'}zw = D_{b'}D_bzw = 0.$$

Ceci prouve le résultat.

Suite de la preuve du théorème ?? On définit un morphisme d'algèbre de Lie

$$\alpha : L_K(\beta_Z(B), \theta_{\beta_Z(B)}) \to (\tau_Z(B), \theta_{\tau_Z(B)})$$

en posant $\alpha(zb_1 \dots b_n) = [\dots[z, b_1] \dots,]b_n]$ pour toute trace $zb_1 \cdots b_n \in \beta_Z(B)$ et une application

$$\phi : L_K(\beta_Z(B), \theta_{\beta_Z(B)}) \ltimes_D L_K(B, \theta_B) \to L_K(A, \theta)$$

telle que pour tout polynôme $P \in L_K(\beta_Z(B), \theta_{\beta_Z(B)})$ et $Q \in L_K(B, \theta_B)$, on ait $\phi(P, Q) = \alpha(P) + Q$.
Montrons que ϕ est un morphisme d'algèbre de Lie. Soit $P, P' \in L_K(\beta_Z(B), \theta_{\beta_Z(B)})$ et $Q, Q' \in L_K(B, \theta_B)$. On a :

$$[\phi(P, Q), \phi(P', Q')] = [\alpha(P), \alpha(P')] - [Q', \alpha(P)] + [Q, \alpha(P')] + [Q, Q'].$$

On a besoin du lemme suivant.

Lemme 30 *On a*

$$\alpha(D_Q(P)) = [\alpha(P), Q]$$

pour tout $P \in L_K(\beta_Z(B), \theta_{\beta_Z(B)})$ *et* $Q \in L_K(B, \theta_B)$.

Preuve Montrons le résultat par induction sur Q. Si $Q = b \in B$ alors on montre le résultat par induction sur P. Si $p = z \in Z$ alors le résultat est évident. Si $P = [P_1, P_2]$ on a

$$\alpha(D_b([P_1, P_2])) = [[\alpha(P_1), b], P_2] + [\alpha(P_1), [\alpha(P_2), b]].$$

Par induction et en utilisant l'identité de Jacobi on trouve le résultat. Supposons que $Q = [Q_1, Q_2]$ alors

$$\alpha(D_{[Q_1,Q_2]}(P)) = [[\alpha(P), Q_2], Q_1] - [[\alpha(P), Q_1], Q_2]$$

en appliquant les hypothèses d'induction sur Q. L'identité de Jacobi nous donne encore le résultat.

Fin de la preuve du théorème ?? En utilisant le lemme **??**, on a

$$\begin{aligned} [\phi(P, Q), \phi(P', Q')] &= \alpha([P, P'] - D_{Q'}(P) + D_Q(P')) + [Q, Q'] \\ &= \phi([(P, Q), (P', Q')]. \end{aligned}$$

Soit ψ l'application de A dans $L_K(\beta_Z(B), \theta_{\beta_Z(B)}) \ltimes_D L_K(B, \theta_B)$ définie par

$$\forall a \in A, \psi(a) = \begin{cases} (a,0) & \text{si } a \in Z \\ (0,a) & \text{si } a \in B \end{cases}.$$

On peut voir facilement que pour tout couple $(a,b) \in \theta$, $[\psi(a), \psi(b)] = 0$. La propriété d'universalité de $L_K(A,\theta)$ permet d'étendre ψ en un morphisme d'algèbre de Lie de $L_K(A,\theta)$ dans $L_K(\beta_Z(B), \theta_{\beta_Z(B)}) \ltimes_D L_K(B,\theta_B)$. De plus, un rapide calcul donne

$$\psi \circ \phi = Id_{L_K(\beta_Z(B),\theta_{\beta_Z(B)}) \ltimes_D L_K(B,\theta_B)}$$

et $\phi \circ \psi = Id_{L_K(A,\theta)}$. Donc, les algèbres de Lie partiellement commutatives $L_K(A,\theta)$ et $L_K(\beta_Z(B), \theta_{\beta_Z(B)}) \ltimes L_K(B,\theta_B)$ sont isomorphes. Il en résulte que $L_K(\beta_Z(B), \theta_{\beta_Z(B)})$ et J sont isomorphes, ce qui prouve le résultat.

Montrons (3). Supposons qu'il existe un couple de lettres $(z,z') \in \theta_Z$ et une suite de lettres $b_1, \ldots, b_n \in B$ tels que le graphe de non commutation admette le sous-graphe

$$z - b_1 - \ldots - b_n - z'.$$

On a alors

$$\begin{array}{rcc} [z,[[\ldots[z',b_n],\ldots b_2],b_1] & = & z[\ldots[z',b_n]\ldots b_2]b_1 - zb_1[\ldots[z',b_n]\ldots b_2] \\ & & -[\ldots[z',b_n]\ldots b_2] + b_1[\ldots[z',b_n]\ldots b_2]z \\ & = & [\ldots[z',b_n]\ldots b_2]zb_1 - zb_1[\ldots[z',b_n]\ldots b_2] \\ & & -[\ldots[z',b_n]\ldots b_2]b_1z + [\ldots[z',b_n]\ldots b_2]b_1z \\ & = & [\ldots[z',b_n]\ldots b_2],[z,b_1]] \\ & (*) & \end{array}$$

Ceci prouve que J n'est pas libre de famille basique $\tau_Z(B)$.

Remarque 20 *La partie* (3) *de ce théorème ne signifie pas forcément que J n'est pas une algèbre de lie partiellement commutative libre. En effet, on peut imaginer qu'elle admet une famille basique autre que $\tau_Z(B)$. Nous n'avons pas réussi à prouver ni à réfuter cette version forte du théorème.*

2.2.2 Construction de bases de l'algèbre de Lie

On définit dans ce paragraphe une classe de bases contenant les bases trouvées par Duchamp et Krob dans [?], [?] et [?] en utilisant des partitions chromatiques de l'alphabet ainsi que les bases de Lyndon partiellement commutatives trouvées par Lalonde dans [?, ?].

Définition 31 *Soit* $= (Y_i)_{i\in[1,n+1]}$ *une factorisation transitive finie. On notera* $\tilde{}$ *l'ensemble des n-uplets de bisections transitives* $(_1, \ldots, _n)$ *tels que* $=_n \circ \ldots _1$. *Les éléments de* $\tilde{}$ *seront appelés les* `historiques` *de* .
Soit une factorisation transitive et $f = (_1, \ldots, _n) \in \tilde{}$. *On notera* f_n^{-1} *l'historique* $(_1, \ldots, _{n-1})$ *(de la factorisation* $_{n-1} \circ \cdots \circ _1$*).*

Dans le cas général, pour une factorisation transitive donnée , l'ensemble $\tilde{}$ possède plus d'un élément. Sa décomposition en bisections transitives n'est pas unique comme le montre l'exemple suivant.

Exemple 21 *Soit le graphe à commutations*

$$(A, \theta) = a - b - c$$

et la factorisation transitive $= (c, b, ac^*)$ *alors*

$$\tilde{=}\{(((\{b, c\}, ac^*), (\{b, c\})), ((c, \{b\} \cup ac^*), (b, ac^*))\}$$

Le but de la prochaine définition est d'étendre la construction de la décomposition associée à une bisection transitive à toutes factorisations transitives finies.

Définition 32 *Soient* $= (Y_i)_{i\in[1,n+1]}$ *une factorisation transitive finie et* $f \in$. *Le* crochetage *de suivant* f *est l'application*

$$\Pi_f :\rightarrow L_K(A, \theta)$$

définie inductivement de la façon suivante.
Si $n = 1$ *(* *est une bisection transitive et* f *est une séquence de longueur* 1 *de la forme* $((B, \beta_Z(B))))$ *alors pour toute trace* $t \in$

$$\Pi_f t = \begin{cases} t \text{ si } t \in B \\ [\ldots[z, b_1]\ldots b_k] \text{ si } w = zb_1\ldots b_k \in \beta_Z(B) \text{ et } z \in Z. \end{cases}$$

Si $n > 1$, choisissons $f = (_1, \ldots, _n) \in \tilde{}$ et posons $_{n-1} \circ \ldots \circ _1 = (Y'_i)_{i\in[1,n]}$. Soit $j \in [1,n]$ tel que $_n = (Y''_j, \beta_{Y'_j - Y''_j}(Y''_j))$ (avec $Y''_j \subset Y'_j$). L'application Π_f est alors définie de la façon suivante. Pour tout trace $t \in$

$$\Pi_f t = \begin{cases} \Pi_{f_n^{-1}} t \text{ si } t \in -Y'_j \cup Y''_j \\ \quad [\ldots[\Pi_{f_n^{-1}} y_1, \Pi_{f_n^{-1}} v_1], \ldots, \Pi_{f_n^{-1}} v_k] \text{ si } w \in_n -Y''_j. \\ \text{En posant } w = y_1 v_1 \ldots v_k \text{ avec } y_1 \in Y'_j - Y''_j \text{ et } v_1 \ldots v_k \in Y''_j. \end{cases}$$

Exemple 22 *Considérons le graphe*

$$(A,\theta) = \begin{array}{ccccc} a & - & b & & \\ | & & | & & \\ c & - & d & - & e \end{array}$$

et la factorisation

$$= (\{a,d,e\}, ce^*, (\{b,c\}e^+ a\{a,d,e\}^* \cup be^*)(ce^*)^*).$$

On a

$$\begin{array}{rcl} f & = & ((\{a,d,e\}, \{b,c\}e^*(\{1\} \cup ea\{a,d,e\}^*), \\ & & (ce^*, (\{b,c\}e^+ a\{a,d,e\}^* \cup be^*)(ce^*)^*))) \in \tilde{}. \end{array}$$

On peut donc définir Π_f. Soit la trace $t = be^2aadecece^2ce^5$. Si on pose

$$= (\{a,d,e\}, \{b,c\}e^*(\{1\} \cup ea\{a,d,e\}^*),$$

on a

$$\begin{array}{rcl} \Pi_f t & = & [[[\Pi_() be^2 aade, \Pi_() ce], \Pi_() ce^2], \Pi_() ce^5] \\ & = & [[[[[[[[[b,e],e],a],a],d],e],[c,e]],[[c,e],e]],[[[[c,e],e],e],e],e]]. \end{array}$$

En utilisant le théorème **??**, on montre par induction sur le nombre de bisections la proposition suivante.

Proposition 33 *Soit $= (Y_i)_{i\in[1,n]}$ une factorisation transitive. Alors, pour tout $f \in \tilde{}$, on a la décomposition en somme directe*

$$L_K(A,\theta) = \bigoplus_{i\in[1,n-1]} L_K(\Pi_f Y_i, \theta_i)$$

où pour tout $i \in [1,n]$

$$\theta_i = \{(\Pi_f y_1, \Pi_f y_2) | y_1, y_2 \in, (y_1, y_2) \in \theta_\}.$$

Exemple 23 *Si on reprend l'exemple* **??**, *on trouve que*

$$L_K(A,\theta) = L_K(B,\theta_B) \oplus L_K(X_1,\theta_{X_1}) \oplus L_K(X_2,\theta)$$

où $B = \{a,d,e\}$, $X_1 = \Pi_f ce^*$ *et* $X_2 = \Pi_f(\{b,e\}e^+a\{a,d,e\}^* \cup be^*)(ce^*)^*)$.

Dans la suite, nous généralisons la notion de crochetage aux factorisations localement transitives finies.

Définition 34 *Soit* $= (Y_i)_{i\in J}$ *une factorisation localement transitive finie. Un crochetage* Π *de* *est une application de* *dans* $L_K(A,\theta)$ *telle que pour tout sous-alphabet fini* $B \subset A$ *et pour tout entier* $n > 0$, *il existe une factorisation transitive* $_{n,} = (Y_i^{n,B})_{i\in J_{n,B}}$ *et un historique* $f \in \tilde{}_{n,B}$ *tels que pour toute trace* $t \in \cap B^{\leq n}$ *on a* $\Pi t = \Pi_{f_{n,B}} t$.

On a besoin du lemme suivant.

Lemme 35 *Soient* $\preceq'$ *deux factorisations transitives finies. Alors pour tout* $f \in \tilde{}$, *il existe* $f' \in \tilde{}'$ *vérifiant, pour toute trace* $t \in$, *l'identité* $\Pi_f t = \Pi_{f'} t$.

Preuve Posons $= (Y_i)_{i\in[1,n+1]}$. D'après le corollaire **??**, les restrictions $'|_{(Y_i,\theta_{Y_i})}$ sont transitives finies. Choisissons $f = (_1,\ldots,_p) \in \tilde{}$ et pour tout $i \in [1,n]$ $f_i = (^i_1,\ldots^i_{k_i}) \in \tilde{}'_{(Y_i,\theta_{Y_i})}$. Alors, l'historique

$$f' = (_1,\ldots,_p,^1_1,\ldots,^1_{k_1},\ldots,^p_1,\ldots,^p_{k_p})$$

vérifit, pour toute trace $t \in$, l'égalité $\Pi_f t = \Pi_{f'} t$.

Théorème 36 *Soit* (A,θ) *un alphabet à commutations. Toute factorisation localement transitive finie de* (A,θ) *admet un crochetage.*

Preuve Soit $= (Y_i)_{i\in J}$ une factorisation localement transitive finie. En utilisant la proposition **??**, on peut construire une séquence de factorisations transitives finies $(_{n,B})_{n\in,B\subset A,B<\infty}$ telle que

1. Si $n \leq n'$ et $B \subset B'$ alors $_{n,B} \preceq_{n',B'}$
2. Pour tout $n \in$ et $B \subset A$, $_{n,B} \preceq$

3. Pour tout $n \in$ et tout sous-alphabet fini B de A, si on pose $_{n,B} = (Y_i^{n,B})_{i\in[1,k_{n,B}]}$, il existe une application strictement croissante $\phi_{n,B}$ de $[1, k_{n,B}]$ dans J vérifiant

$$(Y_i^{n,B}, \theta_{Y_i^{n,B}}) \cap B^{\leq n} = (Y_{\phi_{n,B}(i)}, \theta_{Y_{\phi_{n,B}(i)}})$$

et

$$j \notin \phi_{n,B}([1, k_{b,B}]) \Rightarrow (Y_j, \theta_{Y_j}) \cap B^{\leq n} = \emptyset.$$

Grâce au lemme **??**, on peut définir, pour tout $n > 0$ et pour tout sous alphabet fini B de A une séquence $f_{n,B} \in \tilde{}_{n,B}$ telle que pour tout $m \prec n$, tout $B' \subset B$ et toute trace $t \in_{m,B'} \cap B'^{\leq n}$, on a l'indentité $\Pi_{f_{m,B'}} t = \Pi_{f_{n,B}} t$. On définit donc Π comme l'application de dans $L_K(A, \theta)$ telle que $\Pi t = \Pi_{f_{|t|,t)}} t$.

On a maintenant, facilement, le résulat suivant.

Proposition 37 *Soit $\in CLTF(A, \theta)$ et Π un crochetage de alors la séquence $(\Pi f)_{f\in}$ est une base de $L_K(A, \theta)$ en tant que K-module.*

Exemple 24 *Soit le graphe à commutations*

$$(A, \theta) = a - b - c - d$$

On peut construire "localement" pour $n \leq 3$ la base
$([[a, d], b],\ [[a, d], d],\ [[a, d], a],\ [a, d],\ [a, [a, c]],\ a,\ [a, c],\ [[a, c], c],\ [[a, d], c],$ $[b, d],\ [[b, d[, b],\ [[b, d], d],\ b,\ c,\ d\ )$.

Remarque 25 *Sur les exemples exposés, les bases sont les mêmes que celles obtenues dans [?], seul l'ordre change, ce qui donne lieu à de nouvelles bases de Poincaré-Birkhoff-Witt. Cela permet aussi de développer une algorithmique spécifique de décomposition des polynômes. Dans le paragraphe suivant nous étudierons la décomposition dans le cas général et, un peu plus loin, nous verrons que dans certains cas particuliers, l'algorithmique est plus agréable et utilise des notions comme les séquences standard adaptées du cas libre.*

2.2.3 Algorithmes de décomposition

Soit B est un sous alphabet de A (non nécessairement transitif). L'algorithme suivant permet de décrire un polynôme de Lie suivant la famille de générateurs $\tau_Z(B)$ ou B (suivant son appartenance au facteur droit au gauche de

la bisection).
Soit $P \in L(A, \theta)$. On considèrera ici uniquement les crochetages de traces (la décompositions des autres polynômes de Lie pouvant alors être obtenue en distribuant l'algorithme sur les composantes des polynômes).

1. Si $P \in A$ alors la décomposition est immédiate.
2. Sinon, on peut écrire P sous la forme $P = [P_1, P_2]$.
   (a) Si $P_1, P_2 \in L_K(B, \theta_B)$ alors le polynôme est déjà décomposé.
   (b) Si $P_1, P_2 \in <\tau_Z(B)>$ alors il suffit de décomposer P_1 et P_2 et de développer $[P_1, P_2]$
   (c) Si $P_1 \in <\tau_Z(B)>$ et $P_2 \in L_K(B, \theta_B)$ alors
      i. Si $P_1 \in \tau_Z(B)$ et $P_2 \in B$ alors il n'y a rien à faire (en effet dans ce cas $P \in \tau_Z(B)$ ou $P = 0$ si b commute avec P_1).
      ii. Si $P_1 \in \tau_Z(B)$ et $P_2 \in L_K(B, \theta_B)$ alors P_2 peut s'écrire sous la forme $P_2 = [P_2', P_2'']$. L'identité de Jacobi donne
      $$P = [[P_1, P_2'], P_2''] - [[P_1, P_2''], P_2'].$$
      Il suffit alors d'écrire les polynômes $[[P_1, P_2'], P_2'']$ et $[[P_1, P_2''], P_2']$ selon la bisection.
      iii. Si $P_1 \in <\tau_Z(B)> - \tau_Z(B)$ et $P_2 \in L_K(B, \theta)$ alors on peut écrire p sous la forme $P_1 = [P_1', P_1'']$. L'identité de Jacobi donne
      $$P = [P_1', [P_1'', P_2]] + [[P_1', P_2], P_1'']$$
      Il suffit donc d'écrire les polynômes P_1' et P_1'' selon la bisection en utilisant 2.b) et 2.c), puis $[P_1', P_2]$ et $[P_1'', P_2]$ en utilisant 2.c.ii).
   (d) Si $P_1 \in L_K(B, \theta_B)$ et $P_2 \in <\tau_Z(B)>$ alors il suffit d'utiliser 2.c) avec $-P$.

Exemple 26 *Si on considère le graphe suivant*

$$(A, \theta) = a - b - dc$$

l'algorithme précédent décompose le monôme $[[[b, c], a], [d, c]]$ *suivant les étapes ci-dessous*

1. $[[[b,c],a],[d,c]] = [[b,c],[a,[d,c]] + [[[b,c],[d,c]],a]$
2. $[a,[d,c]] = [[a,d],c] + [[a,c],d]$
3. $[[b,c],[d,c]] = [[[b,c],d],c] - [[[b,c],c],d]$.

D'où le résultat

$$\begin{aligned}[[[b,c],a],[d,c]] &= [[b,c],[[a,d],c]] - [[b,c],[[a,d],d] \\ &\quad +[[[[b,c],d],c],a] - [[[[b,c],c],d],a] \end{aligned} .$$

On peut étendre cet algorithme à toutes les factorisations transitives finies, dont on connaît une écriture sous forme de composition de bisections transitives, en utilisant l'algorithme précédent pour chacune de ces bisections.

2.2.4 Éliminations transitives dans d'autres structures

L'élimination transitive admet des analogues dans d'autres structures partiellement commutatives libres. La bisection de Lazard de (A,θ) donne immédiatement

$$K < A,\theta > \simeq K < B,\theta_B > \otimes K < \beta_Z(B),\theta_{\beta_Z(B)} >$$

si B est un SATF de A.
Le groupe partiellement commutatif libre se définit par la présentation

$$(A,\theta) =< A; \{ab = ba\}_{(a,b)\in\theta} >_{gr} .$$

La transposition au groupe demande de faire appel à l'alphabet des lettres inverses. Rappelons que l'on peut construire le groupe partiellement commutatif libre à l'aide de "réduites" [**?**, **?**]. Si A est un alphabet, on construit $\tilde{A} = A \cup A$ où A est une copie disjointe $\{a\}_{a\in A}$ de A.
L'alphabet $\tilde{A}$ est muni de l'involution (sans point fixe) $x \to x$ telle que $x = x$.
On étend θ par

$$\tilde{\theta} = \{(x,y) \in \tilde{A}^2 | \{(x,y),(x,y),(x,y),(x,y)\} \cap \theta \neq \emptyset\}.$$

On définit ensuite l'application naturelle $s_0 : \tilde{A} \to (A,\theta)$ par $s_0(a) = a$ et $s_0(a) = a^{-1}$ pour tout $a \in A$. Comme s_0 respecte les commutations de $\tilde{\theta}$, on a une factorisation

$$\begin{array}{lll} a\tilde{A} & c(A,\theta) & \\ & & -> acs_0 < -cbs -> ab \\ b(\tilde{A},\tilde{\theta}) & & . \end{array}$$

La flèche s est surjective. Pour tout $g \in (A, \theta)$, il existe un antécédent unique de plus petite longueur dans $s^{-1}(g)$. Cet élément est appelé la "réduite" de g (l'ensemble de toutes les "réduites" sera noté $red(\tilde{A}, \tilde{\theta})$, ses éléments seront appelés les traces réduites).
On a une décomposition similaire à celle de l'algèbre de Lie.

Théorème 38 *Soit (B, Z) une partition de A. Alors*

1. *On a la décomposition en produit semi-direct*

$$(A, \theta) = (B, \theta_B) \ltimes H_Z$$

où H_Z est le sous groupe engendré par

$$\rho_Z(B) = \{w^{-1}zw | z \in Z, w \in (B, \theta_B)\}.$$

2. *Le groupe H_Z est libre pour le code $\rho_Z(B)$ et les commutations*

$$\hat{\theta}_\rho := \{(t, t') \in \rho_Z(B)^2 | tt' = t't \text{ et } t \neq t'\}.$$

Preuve On montre l'assertion 1) par projection du cas libre.
Montrons 2). Soient $\hat{\rho} = \{a_t\}_{t \in \rho_Z(B)}$ un alphabet en bijection avec $\rho_Z(B)$ et $\hat{\theta}$ la relation de commutation sur $\hat{\rho}$ définie par $(a_t, a_{t'}) \in \hat{\theta}$ si et seulement si $t \neq t'$ et $tt' = t't$ dans (A, θ).
On définit pour tout $b \in B$, $\sigma_b : \hat{\rho} \to \hat{\rho}$ par $\sigma_b(a_t) = a_{b^{-1}tb}$. Cette application peut s'étendre en un automorphisme σ_b de $(\hat{\rho}, \hat{\theta})$. En effet, on peut remarquer que $b^{-1}tb \in \rho_Z(B)$ et que si $(a_t, a_{t'}) \in \hat{\theta}$ alors $(\sigma_b(a_t), \sigma_b(a_{t'})) \in \hat{\theta}$.
Soit $\sigma : B \to Aut((\hat{\rho}, \hat{\theta}))$ l'application définie par $\sigma(b) = \sigma_b$. Comme pour tout couple $(b, b') \in \theta_B$ on a $\sigma_b \sigma_{b'} = \sigma_{b'} \sigma_b$, cette application peut s'étendre en un morphisme $\sigma : (B, \theta_B) \to Aut((\hat{\rho}, \hat{\theta}))$.
On considère alors le produit semi-direct

$$\hat{=}(B, \theta_B) \ltimes_\sigma (\hat{\rho}, \hat{\theta}).$$

Montrons que $\hat{}$ et (A, θ) sont isomorphes.
Soit $\alpha : \hat{\rho} \to \rho_Z(B)$ l'application définie par $\alpha(a_t) = t$. Alors la définition de $\hat{\theta}$ et la propriété d'universalité de $(\hat{\rho}, \hat{\theta})$ impliquent que α s'étend en un morphisme $(\hat{\rho}, \hat{\theta}) \to (\rho_Z(B), \theta_{\rho_Z(B)})$.

Soit $\mu : \hat{\rightarrow}(A, \theta)$ l'application telle que $\mu((u, v)) = u\alpha(v)$. Montrons que μ est un morphisme de groupe. On a alors

$$\alpha(\sigma_u(v)) = u^{-1}\alpha(v)u. \tag{2.2}$$

Cette égalité se montre par une récurence sur $(|red(v)|, |red(u)|)$. On a donc

$$\begin{array}{rcccl} \mu((u_1, v_1))\mu((u_2, v_2)) & = & u_1\alpha(v_1)u_2\alpha(v_2) & = & u_1u_2\alpha(\sigma_{u_2}(v_1))\alpha(v_2) \\ & = & u_1u_2\alpha(\sigma_{u_2}(v_1)v_2)) & = & \mu((u_1u_2, \sigma_{u_2}(v_1)v_2)) \\ & = & \mu((u_1, v_1)(u_2, v_2)). & & \end{array}$$

Ceci prouve que μ est bien un morphisme de groupe.
Soit $s : A \rightarrow\hat{}$ l'application définie par $s(b) = (b, 1)$ si $b \in B$ et $s(z) = (1, a_z)$ si $z \in Z$. Un rapide calcul montre que s peut s'étendre en un morphisme de groupe (il suffit de montrer que si $(c, d) \in \theta$ alors $s(c)s(d) = s(d)s(c)$). En remarquant que l'applications $s \circ \mu$ (resp. $\mu \circ s$) restreinte au système de générateurs $\{(b, 1)|b \in B\} \cup \{(1, a_t)|t \in \rho_Z(B)\}$ (resp. A) est l'identité, on trouve que $s \circ \mu = Id$ (resp. $\mu \circ s = Id_{(A,\theta)}$). Ceci prouve

$$(A, \theta) \simeq (B, \theta_B) \ltimes_\sigma (\hat{\rho}, \hat{\theta}).$$

Il en résulte que α est un isomorphisme. Ceci achève la démonstration de la proposition.

Notons la différence entre l'algèbre de Lie et le groupe. On peut toutefois retrouver un phénomène analogue au théorème **??**.3 en ne considérant que les commutations alphabetiques.

Définition 39 *Soit $t \in (A, \theta)$. On notera t) l'ensemble des lettres apparaissant dans $red(t)$. Comme dans le cas du monoïde, si $E \subset (A, \theta)$, on notera*

$$\theta_E = \{(t, t') \in E^2 | tt' = t't \text{ et } t) \cap t') = \emptyset\}.$$

Proposition 40 *Le sous alphabet B est TFSA si et seulement si $\hat{\theta}_\rho = \theta_{\rho_Z(B)}$*

Preuve Supposons B est TFSA. Le fait que $(w_1^{-1}z_1w_1, w_2^{-1}z_2w_2) \in \hat{\theta}_\rho$ implique $(z_1, z_2) \in \theta$. Comme B est TFSA alors

$$w_1^{-1}z_1w_1) \cap w_2^{-1}z_2w_2) = z_1w_1) \cap z_2w_2) = \emptyset,$$

ce qui prouve que $\hat{\theta}_\rho = \theta_{\rho_Z(B)}$.
Réciproquement supposons que B ne soit pas TFSA. Il existe $(z_1, z_2) \in \theta_Z$ et une chaîne de non commutations minimale

$$z_1 - a_1 - \cdots - a_k - c - b_l - \cdots - b_1 - z_2.$$

La minimalité de cette chaîne donne

$$(a_k^{-1} \cdots a_1^{-1} z_1 a_1 \cdots a_k, b_l^{-1} \cdots b_1^{-1} z_2 b_1 \cdots b_l) \in \theta_{\rho_Z(B)} \subset \hat{\theta}_\rho.$$

En posant

$$t_1 = c^{-1} a_k^{-1} \cdots a_1^{-1} z_1 a_1 \cdots a_k c$$

et

$$t_2 = c^{-1} b_l^{-1} \cdots b_1^{-1} z_2 b_1 \cdots b_l c$$

on a $t_1 t_2 = t_2 t_1$. Pourtant $t_1) \cap t_2) = \{c\}$, ce qui prouve que $\hat{\theta}_\rho \not\subset \theta_{\rho_Z(B)}$.

Remarque 27 *Dans le cas du monoïde et de l'algèbre de Lie, le code est en bijection avec $\beta_Z(B)$ ($\{[\cdots[z, a_1], \cdots, a_n]\}_{za_1\cdots a_n \in \beta_Z(B)}$ pour l'algèbre de Lie). Dans le cas du groupe, il est en bijection avec l'ensemble $\beta_Z^R(\tilde{B})$ des traces réduites de $\beta_Z(\tilde{B})$ (il s'agit de $\{w^{-1}zw\}_{zw \in \beta_Z^R(\tilde{B})}$).*
Pour le groupe comme pour l'algèbre de Lie, le fait que les commutations de ces codes soient alphabétiques est équivalent à dire que B est TFSA.
Pour le groupe, si B n'est pas TFSA, autoriser toutes les commutations de (A, θ) rétablit la liberté; il n'en est pas de même de l'algèbre de Lie où d'autres identités peuvent apparaître (cf l'équation (*) de la section 2.2.1).

2.3 Ensembles de Hall transitifs

Dans cette section, on suppose que A est fini et on considère des graphes non orientés sans boucle dont les sommets sont des éléments du magma libre (A) (i.e. les arbres binaires dont les feuilles sont des lettres) muni de l'opération "." définie par $t_1.t_2 = (t_1, t_2)$.
On dira qu'un sous-ensemble $E \subseteq (A)$ est clos si et seulement si

$$(t_1, t_2) \in E \Rightarrow t_1, t_2 \in E.$$

Et on notera $(ba^n) = (\cdots((b, a), a), \cdots, a)$.
Pour tout arbre t, $t)$ désignera l'ensemble des lettres apparaissant dans t. Si θ est une relation de commutation sur l'alphabet A, on définit

$$\theta_{(A)} := \{(t, t') | t) \times t') \subset \theta\}.$$

Lorsqu'il n'y aura pas d'ambiguïté, on notera $\theta_{=}\theta_{(A)}$.

2.3.1 Réduction étoilée

Définition 41 *Soit (A, θ) un alphabet à commutations.*

1. *On appelle* `descente` *dans (A, θ) un n-uplet de lettres $(a_1, \ldots, a_n)$ tel que pour tout i dans $[1, n]$ et pour tout $b, c \in A - \{a_1, \ldots, a_i\}$, si $(b, c) \in \theta$ alors $(b, a_i) \in \theta$ ou $(c, a_i) \in \theta$.*

2. *La lettre a_1 sera appelée l'*`amorce de la descente`*.*

3. *On dira qu'une descente $(a_1, \ldots, a_n)$ est* `complète` *si et seulement si $A = \{a_1, \ldots, a_n\}$.*

4. *On dira que (A, θ) est de* `type H` *si et seulement si il admet une descente complète.*

Remarque 28 *On peut reformuler la définition (??) de façon récursive. Un alphabet (A, θ) est de type H si et seulement si*

1. *L'alphabet A est réduit à une lettre ou*

2. *$|A| > 1$ et il existe une lettre $a \in A$ telle que pour toute commutation $(a_1, a_2) \in \theta$ on ait $(a, a_1) \in \theta$ ou $(a, a_2) \in \theta$ et que $(A - a, \theta_{A-a})$ soit de type H.*

Exemple 29 1. *Pour l'alphabet à commutations*

$$(A, \theta) = \begin{array}{ccccc} a & - & d & - & e \\ | & & | & & \\ b & - & c & & \end{array}$$

la famille (a, d, b, c, e) est une descente complète de (A, θ) qui est donc de type H.

2. *L'alphabet à commutations*

$$(A, \theta) = \begin{array}{ccc} a & - & b \\ c & - & d \end{array}$$

n'est pas un alphabet de type H.

Définition 42 *Soient E un ensemble clos, $G = (A, \theta)$ un alphabet à commutations et $a \in A$. Le* `H-etoilé` *de (A, θ) selon a au rang E est l'alphabet $G_E^{*a} := (A_E^{*a}, \theta_E^{*a})$ défini par*

$$\begin{cases} A_E^{*a} &= (A - a) \cup \{(ba^n) \in E | n > 0, (b, a) \notin \theta\} \\ \theta_E^{*a} &= \theta_{A_E^{*a}}. \end{cases}$$

Lorsque $E = (A)^{\leq n}$ (l'ensemble des arbres construits sur au plus n lettres) on notera G_n^{*a}, A_n^{*a} et θ_n^{*a} à la place de G_E^{*a}, A_E^{*a} et θ_E^{*a}.

Exemple 30 *Soit l'alphabet à commutations*

$$(A, \theta) = a - b - c - d$$

alors

$$(A_4^{*c}, \theta_4^{*c}) = \begin{array}{ccccccc} & & & & (a,c) & & \\ & & & & | & & \\ a & - & b & & & -(ac^2) & d \\ & & & & | & & \\ & & & & (ac^3) & & \end{array}$$

Proposition 43 *Soit $G = (A, \theta)$ un alphabet à commutations de type H et $(a_1, \ldots, a_n)$ une descente complète. Alors pour tout ensemble clos fini E, $G_E^{*a_1}$ est de type H et $(a_2, \ldots, a_n)$ est une descente de $G_E^{*a_1}$.*

Preuve Soit $\Lambda_{a_1,E}(G) = (a'_1, \ldots, a'_m)$ une suite de sommets de $G_E^{*a_1}$ telle que

1. $a'_i = a'_j$ si et seulement si $i = j$,
2. $m = \sharp A_E^{*a_1}$[14]
3. $(a_2, \ldots, a_n)$ est une sous-suite de $(a'_1, \ldots, a'_m)$,
4. $(a_l a_1^p) < a_l$ pour tout $l \in [2, n]$ et $p \geq 1$ (cela implique $(a_1, a_l) \notin \theta$),
5. $(a_l a_1^p) > a_{l-1}$ pour tout $l \in [3, n]$ et $p \geq 1$ (cela implique $(a_1, a_l) \notin \theta$).

[14] Ici $\sharp E$ désigne le cardinal de E.

Montrons que $\Lambda_{a_1,E}(G)$ est une descente complète de $G_E^{*a_1}$. Il suffit de prouver que pour tout $k \in \{1, \ldots p\}$ et pour tout $k_1, k_2 > k$, si $(a'_{k_1}, a'_{k_2}) \in \theta_E^{*a_1}$ alors $(a'_{k_1}, a'_k) \in \theta_E^{*a_1}$ ou $(a'_{k_2}, a'_k) \in \theta_E^{*a_1}$.
Posons $a'_k = a_l a_1^p$, $a'_{k_1} = a_{l_1} a_1^{p_1}$ et $a'_{k_2} = a_{l_2} a_1^{p_2}$. Par définition $(a'_{k_1}, a'_{k_2}) \in \theta_E^{*a_1}$ implique $(a_{l_1}, a_{l_2}) \in \theta$ et $p_1 = 0$ ou $p_2 = 0$. Supposons que $p_2 = 0$ (l'autre cas étant totalement symétrique). D'après la définition de $\Lambda_{a_1,E}$, on a nécessairement $l < l_1, l_2$ et $(a_l, a_{l_1}) \in \theta$ ou $(a_l, a_{l_2}) \in \theta$.
On doit alors considérer deux possibilités:

1. Si $(a_l, a_1) \in \theta$ alors $p = 0$ et $(a'_k = a_l, a_{l_1} a_1^{p_1}) \in \theta_E^{*a_1}$ ou $(a_l, a_{l_2}) \in \theta_E^{*a_1}$ (car $(a_l, a_{l_1}) \in \theta$ ou $(a_l, a_{l_2}) \in \theta$).

2. Si $(a_l, a_1) \notin \theta$. Supposons tout d'abord que $p = 0$, si $(a_l, a_{l_2}) \in \theta$ alors le résultat est vérifié. Si $(a_l, a_{l_2}) \notin \theta$ alors $(a_l, a_{l_1}) \in \theta$, dans ce cas comme $(a_1, \ldots, a_n)$ est une descente $(a_1, a_{l_1}) \in \theta$ et donc $p_1 = 0$. Ceci prouve encore le résultat. Supposons maintenant que $p_1 \neq 0$. Si $(a_l, a_{l_1}) \in \theta$, on a $(a_1, a_{l_1}) \in \theta$ (ceci est impossible par hypothèse) ou $(a_1, a_{l_1}) \in \theta$ (ceci est impossible car $p_1 \neq 0$), ce qui est en contradiction avec nos hypothèses. Donc $(a_l, a_{l_1}) \notin \theta$ et $(a_l, a_{l_2}) \in \theta$ (car $(a_1, \ldots, a_n)$ est une descente). De plus $(a_l, a_1) \notin \theta$ implique (pour la même raison) $(a_{l_2}, a_1) \in \theta$ et $(a'_k, a'_{k_2}) \in \theta_E^{*a_1}$.

Ceci prouve que $\Lambda_{a_1,E}(G)$ est une descente. Comme $m = \sharp A_E^{*a_1}$, elle est complète et donc $G_E^{*a_1}$ est de type H. De plus, $(a_2, ..., a_n)$ étant une sous-suite de $(a'_1, \ldots, a'_p)$, c'est une descente de $G_E^{*a_1}$.

Exemple 31 *Soit l'alphabet à commutations*

$$(A, \theta) = a - b - c - d$$

alors $\Lambda_{a_1,4} = (c, b, ac, ac^2, ac^3, a, d)$.

2.3.2 Ensembles de Lazard transitifs

Définition 44 *Soit $G = (A, \theta)$ et $L \subset (A)$. On dira que L est un ensemble de Lazard transitif si et seulement si pour tout sous-ensemble E clos fini de (A) , $L \cap E = \{s_1, ..., s_k\}$ tel qu'il existe $k+1$ graphes $G_1 = (A_1, \theta_1), ..., G_{k+1} = (A_{k+1}, \theta_{k+1})$ vérifiant*

1. $G_1 := G$

2. $G_{k+1} := (\emptyset, \emptyset)$
3. *Pour tout* $i < k+1$, $s_i \in A_i$ *et* s_i *est l'amorce d'une descente complète sur* G_i.
4. $G_{i+1} := (G_i)_E^{*s_i}$.

On notera $s_1 > s_2 > \ldots > s_k$.

La proposition suivante montre que le test de cette définition peut être restreint aux ensembles d'arbres de taille bornée.

Proposition 45 *L est un ensemble de Lazard transitif si et seulement si pour tout $n \leq 1$ on a , $L \cap (A)^{\leq n} = \{s_1, ..., s_k\}$ tel qu'il existe $k+1$ graphes $G_1 = (A_1, \theta_1), ..., G_{k+1} = (A_{k+1}, \theta_{k+1})$ vérifiant*

1. $G_1 := G$
2. $G_{k+1} := (\emptyset, \emptyset)$
3. *Pour tout* $i < k+1$, $s_i \in A_i$ *et* s_i *est l'amorce d'une descente complète sur* G_i.
4. $G_{i+1} := (G_i)_n^{*s_i}$.

Preuve Si L est un ensemble de Lazard transitif alors il vérifie les propriétés de l'énoncé. En effet, il suffit de lui appliquer $E = (A)^{\leq n}$ qui est un ensemble clos.
Montrons la réciproque. Soient E un ensemble clos fini de (A) et L un ensemble décrit dans l'énoncé. Soit $n = \max\{|t|/t \in E\}$. D'après sa définition, $L \cap A^{\leq n} = \{s_1, ..., s_k\}$ et il existe $k+1$ graphes $G_1, ..., G_{k+1}$ vérifiant (1), (2), (3) et (4). Or $L \cap E \subset L \cap (A)^{\leq n}$. Il existe donc l $(0 < l \leq k)$ tel que $L \cap E = \{s_{i_1} ... s_{i_l}\}$ où $i_1, \ldots, i_l \in [1, k]$ et $i_1 > \ldots > i_k$. On définit

$$\begin{array}{rcl} A'_1 & := & A \cap E \\ \theta'_1 & := & \theta \cap E \times E \\ G'_1 & := & (A'_1, \theta'_1) \end{array}$$

et pour tout p $(0 < p < l+1)$

$$G'_{p+1} = (A'_p, \theta'_p) := (G'_p)_E^{*s_{i_p}}.$$

On a besoin des lemmes suivants.

Lemme 46 *Pour tout $p \in [1,l]$, $A'_p \cap E = A_{i_p} \cap E$.*

Preuve Montrons le résultat par induction sur p. Si $p = 1$ alors $A'_1 = A \cap E$, ce qui prouve le résultat.
Supposons l'hypothèse vraie pour tout $k < p$. Alors $A'_{p-1} \cap E = A_{i_{p-1}} \cap E$. Or pour tout $l \in [i_{p-1}, i_p - 1]$, $s_l \notin E$, ce qui implique que $A'_{p-1} \cap E = A_{i_p - 1} \cap E$. Comme $G_{i_p} = G_{i_{p-1}}^{*s_{i_{p-1}}}$, on peut écrire A_{i_p} sous la forme $A_{i_p} = A^+_{i_p} \cup A^-_{i_p}$ où

$$A^+_{i_p} := \{(s, s^k_{i_{p-1}}) \in (A)^{\leq n} | s \in A'_{p-1}, (s, s_{i_{p-1}}) \in \theta_{i_p - 1}\}$$

et

$$A^-_{i_p} := \{(s, s^k_{i_{p-1}}) \in (A)^{\leq n} | s \in A_{i_p - 1} - A'_{p-1}, (s, s_{i_{p-1}}) \in \theta_{i_p - 1}\}.$$

Montrons tout d'abord que $A^-_{i_p} \cap E = \emptyset$. Il suffit, en fait, de remarquer que si $s \notin A'_{p-1}$ alors soit $s \in A_{i_{p-1}}$, et dans ce cas par induction $s \notin E$, soit $s \notin A_{i_{p-1}}$, et dans ce cas $s = (s', s^{k'}_{l'})$ avec $i_{p-1} < l < i_p$. Or par définition $s_{l'} \notin E$, d'où $s \notin E$. Donc, $A^-_{i_p} \cap E = \emptyset$.
Il en découle $A_{i_p} \cap E = A^+_{i_p} \cap E$ et par induction

$$A_{i_p} \cap E = \{(s, s^k_{i_{p-1}}) \in E | s \in A_{i_{p-1}}, (s_{i_p}, s) \in \theta\} = A'_p \cap E.$$

Lemme 47 *Soient $G = (A, \theta)$ un graphe de commutation, $A' \subset A$ et $G' = (A', \theta')$ le sous-graphe de G engendré par A'. Si $s = (s_i)_{i \in [1,k]}$ est une descente complète de G alors la sous-suite de s' de s composée uniquement des éléments de A' est une descente complète de G'.*

Preuve Un rapide raisonnement par l'absurde montre que si s' n'est pas une descente alors s n'est pas une descente.
Le fait qu'il existe une descente complète de G_{i_p} d'amorce s_{i_p} implique, d'après le lemme **??**, qu'il existe une descente complète de G'_p d'amorce s_{i_p}. Montrons maintenant que $G'_{l+1} \cap E = (\emptyset, \emptyset)$. Soit $t \in A'_{i_{l+1}}$. Alors $t \in A_{i_l + 1} \subset L$. D'où $t \in L$ et donc $t \notin E$ par construction. De plus le lemme **??** implique que pour tout $p \in [1,l]$, $s_p \in G'_p$. Les graphes $G'_1, ..., G'_l$ vérifient donc les conditions (1), (2), (3) et (4) de la définition des ensembles de Lazard transitifs.

Proposition 48 *Un graphe G est de type H si et seulement si il existe un ensemble de Lazard transitif.*

Preuve Soit $(s_1, ..., s_n)$ une descente complète de G. Pour tout k, on construit la séquence N_k de la façon suivante. On pose

$$\begin{array}{ll} D_0 = (s_1, ..., s_n) & G_0 = G \\ D_{i+1} = \Lambda_{s_1^{(i)},(A)\leq k}(G_i) = (s_1^{(i+1)}...s_{n_{i+1}}^{(i+1)}) & G_{i+1} = G_k^{*s_1^{(i)}} \end{array}$$

et $N_k = (s_1^{(1)}...s_1^{(p)})$, où p est le plus petit entier positif [15] tel que $G_p = (\emptyset, \emptyset)$. De plus par construction N_k est une sous-suite de N_{k+1}. Ceci prouve que $L = \lim_{k\to\infty} N_k$[16] est un ensemble de Lazard.
Réciproquement, soit L un ensemble de Lazard transitif. Si on pose $L \cap A = \{a_1, \dots a_k\}$, la suite des éléments de A, $(a_1, \dots, a_k)$ classés dans l'ordre de L, est une descente complète de G.

Exemple 32 *Considérons l'alphabet à commutations.*

$$(A, \theta) = a - b - c - d.$$

Si on pose $n = 3$, on peut construire les familles suivantes en suivant l'algorithme utilisé dans la preuve de la proposition précédente.

$D_0 := (c, b, a, d)$,
$D_1 := (b, (a, c), (ac^2), a, d))$,
$D_2 := ((a, c), (ac^2), a, (d, b), (db^2), d)$,
$D_3 := ((ac^2), (a, (a, c)), a, (d, b), (db^2), (d, (a, c)), d)$,
$D_4 := ((a, (a, c)), a, (d, b), (db^2), (d, (a, c)), d)$,
$D_5 := (a, (d, b), (db^2), (d, (a, c)), d)$,
$D_6 := ((d, b), (db^2), (d, (a, c)), (d, a), (da^2), d)$,
$D_7 := ((db^2), (d, (a, c)), (d, a), (da^2), (d, (, b)), d)$,
$D_8 := ((d, (a, c)), (d, a), (da^2), (d, (d, b)), d)$,
$D_9 := ((d, a), (da^2), (d, (d, b)), d)$,
$D_{10} := ((da^2), (d, (d, b)), (d, (d, a)), d)$,
$D_{11} := ((d, (d, b)), (d, (d, a)), d)$,
$D_{12} := ((d, (d, a)), d)$,
$D_{13} := (d)$,

[15] Un tel entier existe puisque l'ensemble des arbres ayant moins de k feuilles $((A)^{\leq k})$ est fini.

[16] Au sens de la convergence par restriction aux arbres bornés avec un nombre de feuilles fixé.

$D_{14} := \emptyset$.

L'ensemble recherché est donc

$\{c, b, (a, c), ((a, c), c), (a, (a, c)), a, (d, b), ((d, b), b), (d, (a, c)), (d, a),$
$((d, a), a), (d, (d, b)), (d, (d, a)), d\}$

Dans la suite, on notera f_θ le morphisme canonique $(A) \to (A, \theta)$ que l'on nommera feuillage.

Proposition 49 *Soit $(B, \beta_Z(B))$ une bisection transitive. Pour tout $k > 0$, le graphe $(\beta_Z(B) \cap (A, \theta)^{\leq k}, \theta_{\beta_Z(B) \cap (A,\theta)^{\leq k}})$ est isomorphe à $(A_k^{*a}, \theta_k^{*a})$.*

Preuve Évident si on constate que $(t_1, t_2) \in \theta_k^{*a}$ si et seulement si $(f_\theta(t_1), f_\theta(t_2)) \in \theta_{\beta_Z(B)}$.

Définition 50 *On dira qu'une factorisation est gauche (resp. droite) si et seulement si elle vérifie une des assertions suivantes:*

1. *Elle est indécomposable (i.e. on ne peut pas l'écrire comme une composition de factorisations).*

2. *On $a =_1 \circ_2$ où $_2 = (Y_i)_{i \in I}$ est une factorisation gauche (resp. droite) telle que I admette un plus petit (resp. grand) élément i_0 et que $_1$ soit une factorisation gauche (resp. droite) de $< Y_{i_0} >$.*

En appliquant récursivement la proposition **??**, on trouve le théorème suivant qui justifie la limitation aux graphes de type H.

Théorème 51 *Le monoïde (A, θ) admet une factorisation complète localement transitive gauche*[17] *(resp. droite) si et seulement si le graphe de commutation de θ est de type H.*

Remarque 33 *Le théorème* **??** *prouve que le problème d'existence de factorisation de Lazard transitive est décidable.*

[17] Voir Viennot [**?**] pour une étude complète des factorisations localement dichotomiques gauches finies dans le cas libre.

2.3.3 Définition et propriétés des ensembles de Hall transitifs

Définition 52 *Un ensemble de* `Hall transitif` *pour la commutation θ est une famille d'arbres $(h)_{h\in H}$ de (A) totalement ordonnée par une relation d'ordre $<$ telle que la famille $(f_\theta(h))_{h\in H}$ forme une factorisation complète de (A,θ) et que les conditions suivantes sont vérifiées*

1. $A \subset H$
2. *Si* $h = (h', h'') \in H - A$ *alors* $h'' \in H$ *et* $h < h''$
3. *Si* $h = (h', h'') \in (A) - A$ *alors* $h \in H$ *si et seulement si*
   (a) $h', h'' \in H$
   (b) $h' < h''$
   (c) $(f_\theta(h'), f_\theta(h'')) \notin \theta$
   (d) *Soit* $h' \in A$ *soit* $h'' = (x, y)$ *avec* $y \geq h'$

Le résultat suivant permet de caractériser les éléments d'un ensemble de Lazard transitif d'une façon proche des ensembles de Hall.

Théorème 53 *Soient (A,θ) un alphabet à commutations et $L \subset (A)$. Alors L est un ensemble de Lazard transitif si et seulement si c'est un ensemble de Hall transitif.*

Preuve Soit L un ensemble de Lazard transitif. La partie (1) de la définition **??** est évidente.
Soit $h \in L - A$. Alors, on peut écrire h sous la forme $h = (h_1 h_2^p)$ avec $p \geq 1$ avec $h_1, h_2 \in L$ et $p > 0$. Posons $L \cap (A)^{\leq |h|} = \{s_1, \ldots, _k\}$. Alors, il existe $G_1, \ldots, G_{k+1}$ vérifiant les assertions (1), (2), (3) et (4) de la définition des ensembles de Lazard. Soit l le plus petit entier tel que $h \in A_l$. Par construction $s_{l-1} = h_2$, ceci prouve que $h_2 > h$ et l'assertion (2).
Montrons maintenant la propriété (3).
Soit $h \in L - A$. Posons $L \cap (A)^{\leq |h|} = \{s_1, \ldots, _k\}$. Alors il existe $G_1, \ldots, G_{k+1}$ vérifiant les assertions (1), (2), (3) et (4) de la définition des ensembles de Lazard. De plus h peut s'écrire sous la forme $(h_1 h_2^p)$ avec $(h_1 h_2^{p-1}) < h_2 \in L$ et $p > 0$. En effet, si on considère le plus petit entier $l \leq k$ tel que $(h_1 h_2^p) \in A_l$ alors $h_2 = s_{l-1}$, $h_1 \in A_l$ (et donc $h_1 < h_2$) et $(h_1 h_2^{p-1}) \in A_l$ (et donc

$(h_1 h_2^{p-1}) < h_2$). De plus par construction, $((h_1 h_2^{p-1}), h_2) \notin \theta_l$, ce qui implique $(f_\theta((h_1 h_2^{p-1})), f_\theta(h_2)) \notin \theta$. On a prouvé les parties (3.a), (3.b) et (3.c) de la définition **??**. Si $p = 1$, alors comme $h_2 \geq h_2$, h vérifie l'assertion (3.d) de la définition des ensembles de Hall transitifs. Si $p > 1$, supposons $h_1 \neq A$. On peut écrire h_1 sous la forme $h_1 = (h'_1 {h''}_1^q)$ avec ${h''}_1 > h_2$. En effet, si l' est le plus petit entier tel que $h_1 \in A_{l'}$ alors $h''_1 = s_{l'-1}$ et $l' < l$, ce qui implique $h''_1 > h_2$. La partie (3.d) de la définition des ensembles de Hall est donc satisfaite.
Réciproquement, considérons un arbre $h = (h_1, h_2)$ vérifiant les assertions (3.a), (3.b), (3.c) et (3.d) de la définition **??**. On peut poser $L \cap (A)^{\leq |h|} = \{s_1, ..., s_k\}$. D'après la définition de L il existe $k+1$ graphes $G_1, \ldots G_k$ vérifiant les points (1), (2), (3) et (4) de la définition des ensembles de Lazard transitifs. Par construction, il existe $i > j \in [1, k]$ tel que $h_1 = s_i$ et $h_2 = s_j$. Si $h_1 \in A$ alors comme $h_1 \in A_j$, on a nécessairement $h_1 \in A_{j+1}$. Or $(f_\theta(h_1), f_\theta(h_2)) \notin \theta$ donc $(h_1, h_2) \in A_{j+1}$ et $h \in L$. Supposons maintenant que $h_1 \notin A_j$. On peut écrire $h_1 = (s_m s_l^p)$ avec $m > l$, $p \geq 1$ et $l < i$. On a $s_l \geq h_2$, ce qui implique $l \leq j$. De plus $h_1 \in A_l$ et $i > j$ d'où $h_1 \in A_j$ et $h \in A_{j+1} \cap (A)^{|h|} \subset L$.

Montrons maintenant la réciproque. Soit H un ensemble de Hall transitif. On a besoin des lemmes suivants.

Lemme 54 *On a* $\max\{h \in H\} = c \in A$ *et* $\forall (b, a) \in \theta$ *on a* $(b, c) \in \theta$ *ou* $(a, c) \in \theta$

Preuve L'appartenance de $\max\{h \in H\}$ à A provient du fait que tout arbre de H est inférieur à son sous arbre droit.
Supposons qu'il existe $(b, a) \in \theta$ tel que $(b, c) \notin \theta$ et $(a, c) \notin \theta$. Il faut considérer quatre cas:

1. Si $(a, c) > b$ et $(b, c) > a$ alors $h_1 = (b, (a, c)), h_2 = (a, (b, c)) \in H$.
2. Si $(a, c) > b$ et $(b, c) < a$ alors $h_1 = (b, (a, c)), h_2 = ((b, c), a) \in H$.
3. Si $(a, c) < b$ et $(b, c) > a$ alors $h_1 = ((a, c), b), h_2 = (a, (b, c)) \in H$.
4. Si $(a, c) < b$ et $(b, c) < a$ alors $h_1 = ((a, c), b), h_2 = ((b, c), a) \in H$.

Dans tous les cas, $f_\theta(h_1)$ et $f_\theta(h_2)$ sont soit égaux soit conjugués, ce qui implique que $(f_\theta(h))_{h \in H}$ n'est pas une factorisation complète de (A, θ).

Lemme 55 *Soit c l'élément maximal de H. On pose*

$$X := \{(ac^n) | a \in A - c, n \geq 0, (a,c) \notin \theta\} \cup \{b/(b,c) \in \theta)\}$$

et $\theta_X := \theta_{\cap} X^2$. Alors :

1. *$H' := H \cap (X)$ est un ensemble de Hall transitif sur (X) pour la commutation θ_X*
2. *De plus $H = H' \cup \{c\}$.*

Preuve Montrons tout d'abord (1). Les points (1) et (2) de la définition des ensembles de Hall sont immédiats, il reste à prouver le point (3).Soit $h \in H' - X$ avec $h = (h', h'')$. Alors $h', h'' \in (X) \cap H = H'$, $h' < h''$ et si $h' \notin X$ alors $h' = (x,y)$ avec $y \geq h''$. Réciproquement, soient $h', h'' \in H'$ avec $h' \leq h''$ et $(h', h'') \notin \theta$. Si $h' \in X - A$ alors $h' = (x,c)$ et $c > h''$, ce qui implique $h \in H'$. Si $h' \in A$ ou $h' = (x,y)$ avec $y > h''$ alors clairement $(h', h'') \in H'$.
Pour prouver (2) il suffit de montrer que $H - \{c\} \subset H'$. Soit $h \in H - \{c\}$, raisonnons par induction sur $|h|$. Si $h \in A - \{c\}$ alors le résultat est immédiat. Si $h \notin A - \{c\}$, alors on peut écrire $h = (h', h'')$ avec $h', h'' \in H$. Si $h'' = c$ alors comme $h' < h''$, $h' \neq c$ et par induction $h' \in H'$. Comme H' est un ensemble de Hall transitif il en découle $h \in H'$. Supposons maintenant que $h'' \in H - \{c\}$. Alors $h'' < c$ et par induction $h'' \in H'$ et de la même façon $h' < h'' < c$, ce qui implique $h' \in H'$. De plus $h = (h', h'')$ vérifie les points (3.a), (3.b), (3.c) et (3.d) de la définition des ensembles de Hall transitifs. Donc $h \in H'$.

Soit E un sous-ensemble clos fini de (A). Raisonnons par récurrence sur $\sharp E$. Si $\sharp E = 1$ alors $E \subset A$ et le résultat est trivial. Supposons donc que $\sharp E > 1$. Soit $A' := (A) \cap E$. Par projection, H définit un ensemble de Hall transitif sur (A') pour la commutation $\theta_{A'}$. Posons

$$\begin{array}{rcl} c & := & max\{h \in H \cap E\}, \\ X & := & \{(ac^n) | a \in A - c, n \geq 0, (a,c) \notin \theta\} \cup \{b/(b,c) \in \theta\}, \\ \theta_X & := & \theta_{\cup} X^2, \\ H' & := & H \cap (X) \text{ et} \\ E' & := & E \cap (X). \end{array}$$

Si $E' = \emptyset$ alors $H \cap E = \{c\}$ et la définition des ensembles de Lazard transitifs est respectée. Si $E' \neq \emptyset$, alors E' est un ensemble fini clos de

(A) strictement inclus dans E. Le lemme **??** permet d'affirmer que H' est un ensemble de Hall et que $H' \cap E' = H \cap E'$. Par induction sur $\sharp E$ on trouve que $H' \cap E' = H \cap E' = \{h_1, ..., h_p\}$ et donc qu'il existe $p+1$ graphes $G_1, ..., G_{n+1}$ vérifiant les points (1), (2), (3) et (4) de la définition des ensembles de Lazard transitifs. Si on pose $G_0 = (A, \theta)$ et $h_0 = c$, alors $H \cap E = \{h_0 = c, h_1, ..., h_n\}$. De plus $G_1 = (G_0)_E^{*c}$ puisque c'est le graphe de commutation de l'alphabet $X \cap E$. Donc les $n+2$ graphes $G_0, ..., G_{n+1}$ vérifient les conditions (1),(2), (3) et (4) de la définition des ensembles de Lazard transitifs.

2.3.4 Algorithmique des séquences standards

Ce qui suit montre que la théorie trouvée en [**?**] et exposée en [**?**] s'adapte bien aux graphes de type H.
Soit H un ensemble de Hall transitif. Une séquence `standard` d'arbres de Hall est une suite finie $(h_1, ..., h_n)$ d'arbres de Hall telle que pour tout $i \in [1, n]$ on a $h_i \in A$ ou $h_i = (h'_i, h''_i)$ avec $h''_i \geq h_{i+1}, ..., h_n$.
Une `montée` est un indice i tel que $h_i < h_{i+1}$. Une montée `légale` est une montée i telle que $h_{i+1} \geq h_{i+2}, ..., h_n$. Soit s une séquence standard et i une montée légale. On écrit $s \to s'$ où $s' = (h_1, ..., h_{i-1}, (h_i, h_{i+1}), h_{i+2}, ..., h_n)$ lorsque $(f_\theta(h_i), f_\theta(h_{i+1}) \notin \theta$ et $s' = (h_1, ..., h_{i-1}, h_{i+1}, h_i, h_{i+2}..., h_n)$ dans le cas contraire.

Proposition 56 *Soient s une séquence standard et s' une autre séquence telle que $s \to s'$. Alors s' est standard.*

Preuve Soit i la montée légale associée à $s \to s'$. Si $(h_i, h_{i+1}) \notin \theta$ alors le résultat se démontre comme dans le cas non commutatif (cf. [**?**, **?**]). Si $(h_i, h_{i+1}) \in \theta$ alors $s' = (h_1, .., h_{i+1}, h_i, ..., h_n)$. Posons $h_j = (h'_j, h''_j)$ pour tout $h_j \notin A$. On a évidemment

$$h_i \notin A \Rightarrow h''_i \geq h_{i+2}, ..., h_n$$

et

$$h_{i+1} \notin A \Rightarrow h''_{i+1} \geq h_{i+2}, ..., h_n,$$

car s est standard. De plus $h''_{i+1} > h_{i+1} > h_i$ par hypothèse. Ceci implique que s' est standard.
On notera $\stackrel{*}{\to}$ la fermeture transitive de $\to$. On a alors la propriété suivante.

Proposition 57 *Soit s une séquence standard. Il existe une unique séquence standard décroissante s' telle que $s \stackrel{*}{\to} s'$.*

Preuve L'existence provient du fait que si $s \to s'$ où s' n'est pas décroissante alors s' admet une montée légale. Comme le nombre de séquences standards du même multidegré total que s est fini, on en déduit que le processus de réécriture s'arrête par une séquence standard décroissante.

Montrons l'unicité.
On a besoin du lemme suivant.

Lemme 58 *Soient w une trace et s' une séquence telles que $s(w) \xrightarrow{*} s' = (h_1, .., h_n)$. Alors $w = f_\theta(h_1)...f_\theta(h_n)$.*

Preuve Il suffit de remarquer que la réduction n'utilise que des commutations autorisées par θ, et donc ne modifie pas la trace.
Il existe une séquence de lettres t telle que $t \xrightarrow{*} s$ et cette séquence est unique aux commutations près. En effet, si $s = (h_1, \ldots, h_n)$ alors t est une séquence de lettres $(a_1, \ldots, a_n)$ telle que $a_1 \ldots a_k = f_\theta(h_1) \ldots f_\theta(h_n)$ (Lemme **??**).
À toute trace w on associe une séquence de lettres $s(w) = (a_1, ..., a_n)$ telle que $w = a_1...a_n$. Donc il existe une séquence décroissante $s'(w)$ telle que $s(w) \xrightarrow{*} s'(w)$.
Le lemme **??** et le fait que $(f_\theta(h))_{h \in H}$ soit une factorisation complète implique que $s'(w)$ est unique.

Exemple 34 *On considère l'alphabet à commutations suivant:*

$$(A, \theta) = a - b - c - d.$$

Soit H un ensemble de Hall tel que $H \cap (A)^{\leq 3}$ soit l'ensemble calculé dans l'exemple **??**. *On a les réécritures suivantes:*

$$\begin{array}{c}
(b, c, a, c, c, b, d, b, d, d, a, d) \\
\downarrow \\
(b, c, a, c, c, b, d, b, d, (d, a), d) \\
\downarrow \\
(b, c, a, c, c, b, d, b, (d, (d, a)), d) \\
\downarrow \\
(b, c, (a, c), c, b, (d, b), (d, (d, a)), d) \\
\downarrow \\
(b, c, ((a, c), c), b, (d, b), (d, (d, a)), d) \\
\downarrow \\
(b, c, b, ((a, c), c), (d, b), (d, (d, a)), d) \\
\downarrow \\
(c, b, b, ((a, c), c), (d, b), (d, (d, a)), d)
\end{array}$$

D'où

$$bcac^2bdbd^2ad = c.b.b.ac^2.db.d^2a.d.$$

Soient $s = (h_1, ..., h_n)$ une séquence standard et i une montée légale, on définit

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

et

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

On définit l'*arbre de dérivation* de la séquence s, comme étant un arbre de $T(s)$ de racine s tel que

1. Si s est décroissante alors $T(s)$ est réduit à sa racine.

2. Sinon, soit i la montée légale de s la plus à droite (elle existe puisque s n'est pas décroissante). Alors,

   (a) Si $(h_i, h_{i+1}) \in \theta$, $T(S)$ admet un seul sous arbre $T(\rho_i(s))$.

   (b) Sinon, $T(S)$ admet comme sous arbre gauche $T(\lambda_i(s))$ et comme sous arbre droit $T(\rho_i(s))$.

Posons [], l'application canonique de (A) dans $L_K(A, \theta)$ et $[s] = [h_1][h_2]\cdots[h_n]$. On a la propriété suivante.

Proposition 59

$$[s] = \sum_{s' \in F(s)} [s']$$

Où $F(s)$ est le feuillage de l'arbre $T(s)$.

Preuve Il suffit de remarquer que

$$[h_i][h_{i+1}] = \begin{cases} [(h_i, h_{i+1})] + [h_{i+1}][h_i] & \text{si } (h_i, h_{i+1}) \in \theta \\ [h_{i+1}][h_i] & \text{sinon} \end{cases}.$$

Exemple 35 *En reprenant l'exemple* **??**, *on peut calculer l'arbre de dérivation suivant.*

(13,6) (6.5,5.8)(b,c,a,c,c,b,d) *(3,5)*(b,c,c,a,c,b,d) *(1.5,4)*(b,c,c,c,a,b,d)
(1.5,3)(b,c,c,c,b,a,d) *(1.5,2)*(c,b,c,c,b,a,d) *(1.5,1)*(c,c,b,c,b,a,d)
(1.5,0)(c,c,c,b,b,a,d) *(4.5,4)*$(b,c,c,(a,c),b,d)$ *(4.5,3)*$(b,c,c,b,(a,c),d)$
(4.5,2)$(c,b,c,b,(a,c),d)$ *(4.5,1)*$(c,c,b,b,(a,c),d)$ *(10,5)*$(b,c,(a,c),c,b,d)$
(8.5,4)$(b,c,c,(a,c),b,d)$ *(8.5,3)*$(b,c,c,b,(a,c),d)$ *(8.5,2)*$(c,b,c,b,(a,c),d)$
(8.5,1)$(c,c,b,b,(a,c),d)$ *(11.5,4)*$(b,c,((a,c),c),b,d)$ *(11.5,3)*$(b,c,b,((a,c),c),d)$
(11.5,2)$(c,c,b,((a,c),c),d)$ *->(6.5,5.6)(3,5.2) ->(3,4.8)(1.5,4.2)*
->(1.5,3.8)(1.5,3.2) ->(1.5,2.8)(1.5,2.2) ->(1.5,1.8)(1.5,1.2) ->(1.5,0.8)(1.5,0.2)
->(3,4.8)(4.5,4.2) ->(4.5,3.8)(4.5,3.2) ->(4.5,2.8)(4.5,2.2) ->(4.5,1.8)(4.5,1.2)
->(6.5,5.6)(10,5.2) ->(10,4.8)(8.5,4.2) ->(8.5,3.8)(8.5,3.2) ->(8.5,2.8)(8.5,2.2)
->(8.5,1.8)(8.5,1.2) ->(10,4.8)(11.5,4.2) ->(11.5,3.8)(11.5,3.2)
->(11.5,2.8)(11.5,2.2)

Ce qui signifie

$$bcaccbd = c.c.c.b.b.a.d + 2c.c.b.b.[a,c].d + c.b.b.[[a,c],d].d.$$

La décomposition d'un polynôme de Lie dans la base de Hall transitive se fait de façon classique en utilisant l'identité de Jacobi. La méthode est résumée dans la preuve du résultat suivant.

Proposition 60 *Soit $h_1, h_2 \in H$ alors*

$$[[h_1],[h_2]] = \sum_{\substack{|h|=|h_1|+|h_2| \\ h=(h',h'') \text{ avec } h''\leq \sup(h_1,h_2)}} \alpha_h [h]$$

Preuve On va montrer le résultat par induction sur l'ensemble des couples $(|h_1|+|h_2|, \sup(h_1,h_2))$ ordonnés lexicographiquement.
On peut supposer que $h_1 < h_2$ (en effet $[[h_1],[h_2]] = -[[h_2],[h_1]]$ et $[[h],[h]] = 0$). Si $h_1 \in A$ ou $h_1 = (h_1', h_1'')$ avec $h_1'' \geq h_2$ alors le résultat est immédiat. Supposons donc que $h_1'' < h_2$. L'identité de Jacobi donne

$$[[h_1],[h_2]] = [[[h_1'],[h_1'']],[h_2]] = [[[h_1'],[h_2]]],[h_1'']] + [[h_1'],[[h_1''],[h_2]]].$$

Par induction on a

$$[[h_1'],[h_2]] = \sum \alpha_i [h_i]$$
$$[[h_1''],[h_2]] = \sum \beta_j [k_j]$$

avec $h_i = (h_i', h_i'')$, $h_i'' \leq \sup(h_1', h_2)$ et $k_j = (k_j', k_j'')$, $k_j'' \leq \sup(h_1'', h_2)$. D'où

$$[[h_1],[h_2]] = \sum \alpha_i [[h_i],[h_1'']] + \sum \beta_j [[h_1'],[k_j]].$$

Or $\sup(h_i, h_1''), \sup(k_j, h_1') < h_2 = \sup(h_1, h_2)$. On peut donc appliquer les hypothèses d'induction pour trouver le résultat.

2.4 Conclusion

Les ensembles de Hall ont de multiples applications dans le cas non commutatif. En effet, non seulement ils permettent des calculs de bases et de commutateurs basiques mais ils sont aussi reliés à des problèmes d'informatique théorique. On les retrouve, par exemple, en théorie des codes (codes synchronisants, distribution de longueur de codes circulaires...) , dans des calculs de bases de l'algèbre de mélange (base duale), les séries dérivées, séries centrales descendantes du groupe libre [**?**] ...

Certains problèmes admettent un pendant partiellement commutatif. On pourrait être amené à penser que la construction de tels ensembles pourrait aider à répondre à de multiples questions. Pour l'instant, les seuls ensembles "de type" Hall que nous connaissons sont les ensembles de Hall transitifs. Bien qu'ils n'apparaissent pas dans tous les monoïdes partiellement commutatif libres, ils pourraient être utiles pour résoudre "localement" des problèmes. Il y aurait donc une recherche à mener sur cette famille de monoïdes admettant des ensembles de Hall transitifs (notamment en théorie des codes). La première question que l'on pourrait se poser est la suivante: connaissant un ensemble de Hall transitif écrit sous forme de mots, peut-on retrouver la base de Lie correspondante (par recrochetage)? Ce type de question montre d'où risquent de venir les principales difficultés de cette voie. En effet, dans le cas libre, la preuve de l'algorithme permettant de recrocheter un mot de Hall utilise un outil qui fait défaut dans le cas partiellement commutatif : le lemme de Levi, qui malgré l'existence d'une généralisation au monoïde des traces, explique à lui seul de nombreuses différences entre les deux cas.
Un autre axe de recherche pourrait être d'étudier les propriétés des factorisations localement transitives finies, dans le but de les relier à d'autres problèmes d'informatique théorique. Malheureusement, ces objets sont encore difficiles à manipuler, faute d'outils et aussi de leur trop grande généralité (les ensembles de Hall du cas non commutatif sont beaucoup plus agréables à utiliser: on n'a pas à se soucier de l'historique des factorisations par exemple).
On peut encore essayer de généraliser complètement les ensembles de Hall en étudiant les factorisations des monoïdes du type $< \beta_Z(B) >$ lorsque B n'est pas un SATF (en utilisant une approche par la théorie des automates par exemple). Il faudra alors consentir à abandonner quelques unes des propriétés des ensembles de Hall qui nous étaient bien utiles dans le cas libre.
Pour aller plus loin, on peut se poser la question de la généralisation des

bascules (là encore le lemme de Levi risque de poser problème), ou bien de l'élimination de Lazard dans d'autres structures partiellement commutatives libres: p-algèbre de Lie, super algèbre de Lie (s'il existe un analogue partiellement commutatif de cette structure) etc...
En bref, le travail effectué sur les factorisations de Hall dans cette thèse n'est qu'une première étape dans la construction de "vraies" bases de Hall partiellement commutatives. De nombreux et intéressants problèmes nous attendent encore dans ce domaine.

Chapter 3

Support de l'algèbre de Lie partiellement commutative libre

3.1 Introduction

Un théorème de Ree [?] affirme qu'un polynôme est orthogonal à tout polynôme de Lie si et seulement si il est combinaison linéaire de mélanges propres (i.e. uv avec $u, v \neq 1$). Il est naturel de se demander quels sont les mots qui satisfont cette propriété. Plus précisément : quel sont les mots qui n'apparaissent jamais dans le support d'un polynôme de Lie développé. Cette question, posée par Schützenberger a été résolue dans [?].

Théorème *(Duchamp-Thibon)*
Un mot apparaît dans le support de l'algèbre de Lie libre si et seulement si il n'est ni une puissance > 1 d'une lettre, ni un palindrome de longueur paire.

Par exemple le mot $abba$ n'apparaît pas dans le support de $L(A)$. En effet, il peut être écrit comme

$$abba = abba - \frac{1}{2}abab.$$

Ce résultat peut aussi être vérifié en développant tous les crochets des mots de Lyndon de multidegré $(2, 2)$. Par contre, le mot aba apparaît dans le support comme le montre le développement

$$[a, [a, b]] = aab - 2aba + baa.$$

Dans ce chapitre, nous traiterons du même problème dans le cadre des commutations partielles. Ce sujet a fait l'objet d'un travail en collaboration avec G. Duchamp et E. Laugerotte et d'un exposé lors du colloque WORD'99 [**?**].

3.2 Généralités

Dans tout ce paragraphe le morphisme canonique $A^* \to (A, \theta)$ sera noté π_θ. Soit f une application de A^* dans un ensemble S. On dira que f est θ-*cohérente* si elle est constante sur les classes de commutation. Dans ce cas, on peut définir une application f_θ de (A, θ) dans S telle que $f_\theta \circ \pi_\theta = f$.

(3,3) (0.5,2.5)A^* (2.5,2.5)S (1.5,0.5)(A, θ) (1.5,2.8)f (0.5,1.5)π_θ (2.5,1.5)f_θ
->(1,2.5)(2,2.5) ->(0.5,2.2)(1.2,1) ->(1.8,1)(2.5,2.2)

Soient $f : A^* \to (A, \theta)$ et $g : A^* \to S$ deux applications θ-cohérentes . Alors $g_\theta \circ f$ est aussi θ-cohérente et on a $(g_\theta \circ f)_\theta = g_\theta \circ f_\theta$.

(3,3) (0.5,2.5)A^* (2.5,2.5)S (0.5,0.5)(A, θ) (2.5,0.5)(A, θ) (1.5,2.8)g (0.2,1.5)f
(1.5,0.2)f_θ (2.8,1.50)$g)\theta$ (2.1,1.2)π_θ (1.5,2.2)$(g_\theta \circ f)_\theta$ ->(1,2.5)(2,2.5)
->(0.5,2.2)(0.5,0.8) ->(2.5,0.8)(2.5,2.2) ->(1.2,0.5)(1.8,0.5) ->(0.6,2.2)(2.2,0.8)
->(0.6,0.8)(2.2,2.2)

Par exemple, la longueur (resp. le degré partiel par rapport à un sous alphabet $S \subseteq A$) d'un mot est une application θ-cohérente.
L'application $A^* \to \mathcal{P}(A)$ associant à tout mot l'ensemble des lettres le composant est aussi une application θ-cohérente. Dans ces cas on notera $|t|$, $|t|_S$ et t) à la place de $|t|_\theta$, $(|t|_a)_\theta$ et θ(t).
Rappelons que l'image miroir d'un mot $w = a_1 \cdots a_n$ est le mot $w = a_n \cdots a_1$ où $a_1, \ldots, a - n \in A$. La symétrie de θ implique que l'application linéaire $\pi_\theta \circ ()$ est θ-cohérente. On appellera *involution* d'une trace $t = a_1 \cdots a_n$ la trace $t = a_n \cdots a_1$. On dira qu'une trace est *involutive* si et seulement si elle est égale à son involution[1].

Lemme 61 *Il n'existe pas de trace connexe de longueur impaire de la forme $t = bwc$ avec $b \neq c \in A$ telle que bw et wc soient des traces involutives et connexes.*

[1] Il s'agit de la généralisation des palindromes. Toutes les traces involutives ne peuvent pas s'écrire comme des palindromes. En effet, si on considère l'alphabet $(A, \theta) = a - b \quad c$ alors la trace *cabc* est involutive.

Preuve Supposons qu'une telle trace existe. On peut alors la choisir de longueur minimale. Notons la $t = bwc$. Le fait que wc (resp. bw) soit involutive implique que $c \in (wc)$ (resp. $b \in (bw)$). La trace t étant de longueur impaire on a nécessairement $w \neq 1$. La trace wc étant non connexe, cela signifie qu'il existe une lettre $d \in w$) telle que $(c, d) \notin \theta$ et donc $c \in (t)$. De même, on peut montrer que $b \in (w)$. Alors $t = bcw_1bc$ où cw_1b est une trace connexe de longueur impaire (en effet $cw_1b) = t)$). Les traces wc et bw étant involutives, il en est de même pour cw_1 et w_1b. Ce sont de plus deux traces connexes car $w_1) = t)$. Il en découle que la trace cw_1b vérifie encore les hypothèses et contredit la minimalité de t.

L'application de Dynkin r de A^* dans $L(A)$ est définie par $r(a) = a$ si $a \in A$ et $r(aw) = [a, r(w)]$ pour tout mot $w \in A^+$.

Proposition 62 *L'application $\pi_\theta \circ r$ est θ-cohérente.*

Preuve On a besoin du lemme suivant.

Lemme 63 *Soient $a \in A$ et $v_1, v_2 \in A^*$ tels que $a \notin v_1)$ et $av_1 = v_1a$ alors*

$$\pi_\theta \circ r(av_1v_2) = \pi_\theta \circ r(v_1av_2).$$

Preuve Nous allons montrer ce résultat par induction sur $|v_1|$. Lorsque $|v_1| = 1$, le lemme découle directement de l'identité de Jacobi:

$$\begin{aligned}
\pi_\theta \circ r(av_1v_2) &= \pi_\theta \circ r(abv_2) \\
&= [a, [b, \pi_\theta \circ r(v_2)]] \\
&= [[a, b], \pi_\theta \circ r(v_2)] + [b, [a, \pi_\theta \circ r(v_2)]] \\
&= [b, [a, \pi_\theta \circ r(v_2)]] \\
&= \pi_\theta \circ r(bav_2).
\end{aligned}$$

Sinon, supposons $v_1 = bv_3$ avec $b \in A - \{a\}$ et $a \notin v_3)$. Par induction sur la longueur du mot on trouve

$$\begin{aligned}
\pi_\theta \circ r(av_1v_2) &= \pi_\theta \circ r(abv_3v_2) \\
&= \pi_\theta \circ r(bav_3v_2) \\
&= [b, \pi_\theta \circ r(av_3v_2)] \\
&= [b, \pi_\theta \circ r(v_3av_2)] \\
&= \pi_\theta \circ r(v_1av_2).
\end{aligned}$$

Fin de la preuve de la proposition ?? Supposons $u \equiv_\theta v$ et raisonnons par induction sur la longueur de u. Si $|u| = 1$ alors on a nécessairement $u = v$ et le résultat est immédiat. Si $|u| > 1$, on peut écrire $u = au_1$ et $v = v_1 a v_2$ avec $a \notin v_1$). Si $v_1 = 1$, alors il suffit de montrer que $\pi_\theta \circ r(u_1) = \pi_\theta \circ r(v_2)$, ce qui est vrai par induction sur la taille des mots. Si $v_1 \neq 1$, alors nécessairement $v_1 a \equiv_\theta a v_1$. Le lemme **??** nous permet de conclure.

L'application $r_\theta = (\pi_\theta \circ r)_\theta$ est bien définie grâce à la proposition **??**. Les polynômes $r_\theta(t)$ seront appelés *polynômes de Dynkin partiellement commutatifs*. Ce sont des polynômes multihomogènes.

Proposition 64 *Le $-$module $L(A, \theta)$ est engendré par les polynômes de Dynkin partiellement commutatifs.*

Preuve Par projection, puisque les polynômes de Dynkin forment un ensemble générateur de $L(A)$ en tant que -module.

La θ-cohérence de $\pi_\theta \circ r$ permet de justifier de l'existence de l'application adjointe définie par $ad_a P = [a, P]$, on a encore la formule de Leibniz

$$ad_a^n P = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} a^{n-i} P a^i.$$

Proposition 65 *Pour toute trace t on a l'égalité*

$$r_\theta(t) = (-1)^{|t|+1} r_\theta(t).$$

Preuve Soit w un mot tel que $\pi_\theta(w) = t$. Alors

$$r_\theta(t) = \pi_\theta \circ r(w) = \pi_\theta(r(w)).$$

Or dans le cas non commutatif on a

$$r(w) = (-1)^{|w+1|} r(w),$$

ce qui prouve le résultat.

Afin de résoudre le problème du support, on se propose d'étudier l'ensemble des traces apparaissant (avec un coefficient non nul) dans un polynôme de Dynkin. Le résultat suivant nous sera utile par la suite.

Lemme 66 *Soit $t \in (A, \theta)$ et $b \notin t)$ tel que $(b \times t)) \cap \theta = \emptyset$. Alors,*

1. *$(r_\theta(tb), sb) \neq 0$ si et seulement si $s = t$.*
2. *$(r_\theta(tb), bs) \neq 0$ si et seulement si $s = t$.*

Preuve Il suffit de prouver le "seulement si" de chaque assertion. Montrons-le en utilisant un raisonnement par induction sur $|t|$. Si $|t| = 0$ alors les deux assertions sont vraies. Supposons donc que $|t| > 1$. Soit $a \in (t)$ et $t' \in (A, \theta)$ tel que $t = at'$. Alors

$$r_\theta(tb), w) = r_\theta(at'b), w) = (ar_\theta(t'b), w) - (r_\theta(t'b)a, w).$$

Pour (1) cette formule donne $(r_\theta(tb), sb) = (ar_\theta(t'b), sb)$ car $ab \neq ba$. De plus, si $(ar_\theta(t'b), sb) \neq 0$ alors $s = as'$ et $(r_\theta(tb), sb) = (r_\theta(t's), s'b) \neq 1$ et par induction on trouve le résultat.
Pour (2), il suffit de constater que

$$(r_\theta(tb), bs) = -(r_\theta(t'b)a, bs)$$

et un raisonnement symétrique au précédent donne le résultat.

3.3 Support simple

Le support (A, θ) de $L(A, \theta)$ est l'ensemble des traces apparaissant avec un coefficient non nul dans un polynôme de Lie partiellement commutatif. Certaines traces particulières n'apparaissent jamais dans (A, θ). La proposition suivante en exhibe trois catégories.

Proposition 67 *Si une trace est une puissance a^n d'une lettre $a \in A$ avec $n > 1$, une trace non connexe ou une trace involutive de longueur paire, elle n'appartient pas à (A, θ).*

Preuve Si $t = a^n \in (A, \theta)$ alors $t \in (\{a\}, \emptyset)$, ceci n'est possible que dans un unique cas: $n = 1$.
Supposons maintenant que t soit non connexe. Alors t peut s'écrire sous la forme $t = uv$ avec $u) \times v) \subseteq \theta$. Alors t appartient à un polynôme multihomogène de

$$L(t), \theta_{t)}) = L(u), \theta_{u)}) \oplus L(v), \theta_{v)}),$$

ce qui implique que $u = 1$ ou $v = 1$ et contredit nos hypothèses[2].

Supposons donc que t soit une trace involutive de longueur paire. Alors $t = t$. La multi-homogénéïté de r_θ et la proposition **??** implique qu'il suffit de chercher les traces t' de longueurs paires telle que t apparaisse dans le support de $r_\theta(t')$. Or, d'après la proposition **??**, on a

$$(r_\theta(t'), t) = -(r_\theta(t'), t) = -(r_\theta(t'), t) = -(r_\theta(t'), t) = 0.$$

Ceci permet de conclure.

Exemple 36 *Si on considère le graphe de commutation*

$$a \qquad b - c.$$

La trace abca, qui est involutive de longueur paire, n'apparaît pas dans le support, comme le montre l'égalité

$$acba = acba - acab.$$

Remarque 37 *Attention, la réciproque est fausse dans le cas général. En effet, considérons le graphe de commutation*

$$a - b - c - d.$$

La trace abcda peut s'écrire sous la forme

$$abcda = bacda - badac.$$

On peut retrouver le même résultat en considérant les crochetages de traces de Lyndon de multidegré $(2, 1, 1, 1)$. *Il y a ,en effet, seulement deux traces de Lyndon de ce multidegré:* a^2cdb *et* $acadb$. *Leurs crochetages donnent:*

$$\begin{aligned}
[a, [[a, c], [d, b]]] &= a^2cdb - a^2cbd - acadb + acabd - acbac + adbca + \\
&\quad abdac - \underline{adbca} - acdba + \underline{acdba} - cadba - cabda + \\
&\quad dbaca - dbca^2 - bdaca + bdca^2 \\
[[a, c], [[a, d], b]] &= acadb - acdab - acbad + \underline{acbda} - ca^2db + cadab + \\
&\quad cabad - cabda - adbac + adbca + dabac - dabca + \\
&\quad badac - \underline{badca} - bdca^2c + bdaca
\end{aligned}$$

Dans la suite, on notera A_4 *tout graphe isomorphe à* $a - b - c - d$.

[2] On peut aussi montrer ce résultat en constatant que, sous les mêmes hypothèses, $t = uv$ et en appliquant le théorème de Ree.

Définition 68 *On notera $NS_0(A,\theta)$ l'ensemble des traces t telle que $t = a^n$ avec $n > 1$ ou non connexe, ou involutive de longueur paire.*
Si $(A,\theta) = (A,\theta) - \{1\} - NS_0(A,\theta)$, on dira que $L(A,\theta)$ admet un support simple.

On a le résultat préliminaire suivant.

Lemme 69 *Soit (A,θ) un alphabet à commutations n'ayant aucun sous-graphe de type A_4. Soit $t = bw$ une trace connexe telle que w soit non connexe. Alors la lettre b ne commute avec aucune des lettres apparaissant dans w.*

Preuve Soient $w_1, \ldots, w_n$ $(n > 1)$ les composantes connexes de w. Si chaque w_i) n'a qu'une seule lettre, l'assertion est triviale. Supposons donc le contraire et choisissons un indice $i \in [1,n]$ tel que $|w_i)| > 1$. Soit $a \in w_i$). Supposons que $(a,b) \in \theta$. Alors, il existe une lettre $c \in w_i$) telle que $(b,c) \notin \theta$ (dans le cas contraire w_i ne serait pas une composante connexe). Soient $i \neq j$ et $d \in w_j$) tel que $(d,b) \notin \theta$. Si $(a,c) \notin \theta$ alors

$$b - a - d - c$$

est un sous-graphe de θ, ce qui contredit nos hypothèses. Maintenant si $(a,c) \in \theta$, il existe un chemin de a à c dans le graphe de non commutation possédant exactement trois lettres (dans le cas contraire, il existerait un sous-graphe de type A_4). Alors, il existe $e \in w_i$) tel que $(a,e),(c,e) \notin \theta$. Si $(b,e) \notin \theta$ alors $b - a - d - e$ est un sous-graphe de θ sinon $c - a - b - e$ est un sous graphe de θ. Ceci contredit nos hypothèses et prouve que $(a,b) \notin \theta$.

3.4 Caractérisation des algèbres de Lie partiellement commutatives libres admettant un support simple

Théorème 70 *L'algèbre de Lie $L(A,\theta)$ a un support simple si et seulement si le graphe de commutation de (A,θ) n'a pas de sous-graphe isomorphe à*

$$a - b - c - d.$$

Preuve Montrons la condition nécessaire par contraposition. Supposons que $a-b-c-d$ soit un sous-graphe de θ. Alors, la trace $abcda$ n'appartient ni à $NS_0(A,\theta)$ ni à (A,θ) (cf. remarque **??**).

Réciproquement, grâce à la proposition **??**, on a

$$(A,\theta) \subseteq (A,\theta) - \{1\} - NS_0(A,\theta).$$

Il suffit de prouver l'inclusion inverse par induction sur $|t|$ avec $t \notin NS_0(A,\theta)$. Si t est une lettre, alors il est évident que $t \in (A,\theta)$. Maintenant, considérons que $t \notin A$. On peut poser $t = b^n t' b^m$ avec $b \in (t)$ et $n+m$ maximum (ce qui implique que $b \notin (t') \cap (t')$). Si $t' \notin NS_0(A,\theta)$, par induction il existe un polynôme P tel que $(P,t') \neq 0$. Cela découle de la formule de Leibniz

$$({}_b^{m+n}P, t) = (-1)^n \binom{n+m}{m} (P,t') \neq 0.$$

Supposons que $t' \in NS_0(A,\theta)$, nous devons considérer 3 cas.

1. Si $t' = a^k$ avec $a \in A$, on a nécessairement $t \in (\{a,b\}, \theta_{\{a,b\}})$ et comme t est connexe, le résultat est donné dans [**?**]

2. Si t' est une trace non connexe, alors la lettre b n'appartient pas à t') et d'après lemme **??**, aucune lettre de t') ne commute avec b. Le lemme **??** implique $(r_\theta(t'b), bt') \neq 0$). Ceci donne, d'après la formule de Leibniz

$$\begin{array}{rcl} ({}_b^{m+n-1}r_\theta(t'b), t) & = & (-1)^{n-1} \binom{m+n-1}{n-1} (r_\theta(t'b), bt') \\ & + & (-1)^n \binom{m+n-1}{n} (r_\theta(t'b), t'b). \end{array}$$

   Si $t' \neq t'$ alors par lemme **??** on a $(r_\theta(t'b), t'b) = 0$, d'où le résultat.
   Si $t' = t'$ alors un rapide calcul donne

$$({}_b^{m+n-1}r_\theta(t'b, t') = (-1)^{n-1} \binom{n+m}{n} \frac{n + (-1)^{|t'|+1}m}{n+m} (r\theta(t'b, bt').$$

   Dans les deux cas $m \neq n$ et $m = n$ (car alors $|t'| = |t| - 2n$ est impair), on a $({}_b^{m+n-1}r_\theta(t'b, t)) \neq 0$.

3. Si $t' \neq a^k$ est de longueur paire et involutive.
   Supposons tout d'abord que $n > 0$ ou $m > 1$. Alors $m \neq n$ (dans le cas

contraire t serait involutive et de longueur paire). On a $bt' \notin NS_0(A,\theta)$ et par induction il existe une trace s tel que $(r_\theta(s), bt') \neq 0$). Alors,

$$\begin{array}{rcl} {}^{n+m-1}_{b}r_\theta(s),t) & = & (-1)^{n-1}\binom{n+m-1}{n-1}(r_\theta(s),bt') \\ & + & (-1)^{n}\binom{n+m-1}{n}(r_\theta(s),t'b). \end{array}$$

Comme t'est involutive, ceci implique

$${}^{m+n-1}_{b}r_\theta(s),t) = (-1)^{n-1}\binom{n+m-1}{n-1}\frac{n+(-1)^{|t'|+1}m}{n}(r_\theta(s),bt').$$

Comme $t \notin NS_0(A,\theta)$, on a $m \neq n$ et nécessairement

$${}^{m+n-1}_{b}r_\theta(s),t) \neq 0.$$

Supposons maintenant que $n = 0$ et $m = 1$ et soit $c \in (t)$. Posons $t' = c^k t''$ avec $c \notin (t'')$. La maximalité de $m+n$ implique $c \notin (t)$. Supposons que $k > 1$. Le cas précédent implique qu'il existe un polynôme de Lie P tel que $(P, bt''c^k) \neq 0$ (car $t = bt''c$), ce qui prouve que $(P,t) \neq 0$. Si $k = 1$, on doit considérer deux cas. Si $t''b \notin NS_0(A,\theta)$ alors par induction il existe un polynôme de Lie tel que $(P, t''b) \neq 0$ et alors

$$([P,c],t) = (Pc - cP, ct''b) = (P, t''b) \neq 0.$$

Si $t''b \in NS_0(A,\theta)$, par définition de $NS_0(A,\theta)$. On a encore trois possibilités.

(a) Si $t''b = a^k$ ce implique $t'' = 1$ et le résultat.

(b) Si $t''b$ est non connexe, il suffit de remarquer, en utilisant le cas 2), qu'il existe un polynôme de Lie P tel que $(P,t) \neq 0$ et alors $(P,t) \neq 0$.

(c) Si $t''b$ est connexe et involutive, le lemme **??** est contredit (car $ct'' = t'$ est involutive et connexe et t est paire). Ceci prouve le théorème.

3.5 Pliage de graphe

Dans ce paragraphe la paire $G = (A,\theta)$ dénotera un alphabet à commutations (i.e. un graphe connexe sans boucles). Le *graphe complémentaire* de G est le graphe

$$G^c := (A, A \times A - \theta - \Delta_A)$$

où $\Delta_A = \{(a,a)/a \in A\}$. Un morphisme (resp. isomorphisme) ϕ d'un alphabet à commutations (A,θ) dans un alphabet à commutations (A',θ') est une application (resp. une bijection) de A dans A' telle que pour tout couple $(a,b) \in A^2$ tel que $\phi(a) \neq \phi(b)$ on ait

$$(a,b) \in \theta \Leftrightarrow (\phi(a),\phi(b)) \in \theta'.$$

On notera $v_G(a)$ le *voisinage propre* de a dans G, c'est à dire l'ensemble des lettres $b \neq a$ telle que $(a,b) \in \theta$. On dira que deux lettres ont le *même rôle* si et seulement si

$$v_G(a) - b = v_G(b) - a.$$

Ceci définit une relation d'équivalence sur A^3 qui sera notée $\approx$.
Lorsque $\approx_G = Id_A$ on dira que G est *pliable* sinon G sera dit *plié*.

Lemme 71 *Un alphabet à commutations est pliable si et seulement si son complémentaire l'est.*

Preuve Il suffit de remarquer que $\approx_G = \approx_{G^c}$.

Supposons G pliable. Soient a,b deux sommets ayant le même rôle. Si on note G le sous graphe de G engendré par $A - \{b\}$ (i.e. le graphe de commutation $(A - \{b\}, \theta_{A-\{b\}})$), on écrira alors $G \triangleright G'$. On peut voir facilement que $\triangleright$ définit une relation d'ordre partiel sur l'ensemble des alphabets à commutations. On notera $\overset{*}{\triangleright}$ la cloture transitive de $\triangleright$.

Exemple 38 *On considère le pliage suivant.*

(10,3) (1,2)a (1.5,1)c (2,2)b (3,2)d (3,1)e (5,1.5)a (6,1.5)d (8,1.5)a
(1.2,2)(1.8,2) (1,1.8)(1.4,1.2) (1.6,1.2)(2,1.8) (3,1.8)(3,1.2)
->(3.5,1.5)(4.5,1.5) ->(6.5,1.5)(7.5,1.5) linestyle=dashed (1.5,1.5)(0.8,0.8)
(3,1.5,0)(0.25,0.8) (5.5,1.5)(0.7,0.25) (1.5,0.6)(1.5,0.2) (1.5,0.2)(5,0.2)
->(5,0.2)(5,1.2) (3,2.4)(3,2.8) (3,2.8)(6,2.8) ->(6,2.8)(6,1.8)
(5.5,1.2)(5.5,0.2) (5.5,0.2)(8,0.2) ->(8,0.2)(8,1.2)

Le graphe ci-dessus peut donc se replier en le graphe trivial (un seul point). Ce n'est pas le cas de tous les graphes comme le montre le graphe suivant

(3,3) (2,2.5)a (1,2)b (3,2)c (1,1)d (3,1)e (1.8,2.3)(1.2,2.1)
(2.2,2.3)(2.8,2.1) (1.2,2)(2.8,2) (1.2,1)(2.8,1) (1,1.8)(1,1.2) (3,1.8)(3,1.2)

[3] Cette relation d'équivalence apparaît pour la première fois dans [**?**]

qui n'est pas pliable.

Proposition 72 *La relation $\overset{*}{\triangleright}$ est confluente (aux isomorphismes près).*

Preuve Il suffit de prouver que la relation $\triangleright$ est confluente. Soient G, G_1, G_2 trois graphes de commutations tels que $G \triangleleft G_1$ et $G \triangleleft G_2$. On notera ϕ_1 le morphisme canonique de G dans G_1 et ϕ_2 le morphisme canonique de G dans G_2. Soit (a_1, b_1) (resp. (a_2, b_2)) la paire associée au pliage élémentaire $G \triangleright G_1$ (resp. $G \triangleright G_2$). Si $\{a_1, b_1\} \cap \{a_2, b_2\} = \emptyset$ alors $\phi_2(a_1) \approx_{G_2} \phi_2(b_1)$ et $\phi_1(a_2) \approx_{G_1} \phi_1(b_2)$. Ceci nous permet d'écrire

$$\begin{array}{ccc} G & \triangleright & G_1 \\ \triangledown & & \triangledown \\ G_2 & \triangleright & G_3 = G_1 - \phi_1(b_2) = G_2 - \phi_2(b_1). \end{array}$$

Dans le cas contraire, comme $\approx_G$ est une relation d'équivalence, les graphes G_1 et G_2 sont isomorphes. Ceci prouve le résultat.

Corollaire 73 *Pour tout graphe de commutation G, il existe un unique(à un isomorphisme près) graphe plié G_m tel que $G \overset{*}{\triangleright} G_m$.*

Preuve Supposons qu'il existe deux graphes pliés G_1 et G_2 tels que $G \overset{*}{\triangleright} G_1, G_2$. La proposition **??** nous donne l'existence d'un graphe G_3 tel que

$$\begin{array}{ccc} G & \overset{*}{\triangleright} & G_1 \\ \triangledown * & & \triangledown * \\ G_2 & \overset{*}{\triangleright} & G_3. \end{array}$$

La minimalité de G_1 et G_2 implique donc que G_1, G_2 et G_3 sont isomorphes. On appellera G_m le *replié* de G. Maintenant, on va caractériser les graphes admettant $G_0 = (\{a\}, \emptyset)$ comme replié.

Proposition 74 *Supposons que G ne soit pas isomorphe à G_0 et qu'il n'admette aucun sous-graphe de type A_4. Alors G ou G^c est non connexe.*

Preuve Si $|A| = 2$ alors la propriété est triviale. Sinon, choisissons une lettre $a \in A$ et posons $G' = (A - \{a\}, \theta_{A-\{a\}})$. On doit considérer deux cas.

1. Si G' est non connexe, alors pour toute lettre $b \neq a$, il existe une lettre c telle que b et c soient dans deux composantes connexes différentes de G'. On peut supposer que G est connexe (dans le cas contraire il n'y a rien à montrer). Alors il existe un chemin dans le graphe G allant de b à c et passant par a. Considérons un tel chemin de longueur minimale. Comme G ne possède aucun sous-graphe de type A_4, cette longueur est égale à deux. Ceci prouve que $(a, b) \in \theta$ et que $\{a\}$ est une composante connexe de G^c.

2. Si G' est connexe alors, comme A_4 est isomorphe à A_4^c, les graphes G^c et G'^c n'admettent aucun sous-graphe de type A_4. Supposons alors que G^c soit connexe. Comme par induction G'^c est non-connexe, on prouve le résultat par la méthode utilisée dans le cas 1).

Corollaire 75 *Tout graphe de commutation non isomorphe à G_0 et n'admettant aucun sous-graphe de type A_4, est pliable.*

Preuve Soit $G = (A, \theta)$ un tel graphe. La propriété est aisément vérifiée lorsque la taille de l'alphabet est 2. On doit considérer deux cas.

1. Supposons G non connexe. Si aucune composante connexe de G n'a plus de une lettre, alors G est totalement déconnecté et la propriété est immédiate. Dans le cas contraire, soit G' une composante connexe de G ayant strictement plus d'une lettre, et par induction G' est pliable et donc G aussi.

2. Si G est connexe alors la proposition **??** implique que G^c est non-connexe. De plus il est facile de voir que G^c n'admet aucun sous-graphe de type A_4. Les arguments du cas 1) peuvent être donc appliqués à G^c et on en déduit que G^c est pliable. Le lemme **??** permet alors de conclure.

Ce corollaire permet de prouver le résultat principal de cette section.

Théorème 76 *Un graphe n'admet aucun sous-graphe de type A_4 si et seulement si il peut être plié en G_0.*

Preuve Par induction sur la taille de l'alphabet en utilisant le corollaire **??**.

On peut donc réécrire le théorème **??** sous la forme suivante.

Corollaire 77 *Les propriétés suivantes sont équivalentes.*

1. *L'algèbre de Lie $L(A, \theta)$ admet un support simple.*
2. *Le graphe de commutation de l'alphabet n'admet aucun sous-graphe de type A_4.*
3. *Le graphe de non commutation de l'alphabet n'admet aucun sous-graphe de type A_4.*
4. *Il existe deux lettres $a_1 \neq a_2 \in A$ telles que $a_1 \approx_{(A,\theta)} a_2$ et $L(A - \{a_2\}, \theta_{A-\{a_2\}})$ admet un support simple.*
5. *Le graphe de commutation de l'alphabet peut se plier en G_0.*

3.6 Conclusion

De nombreuses questions liées au problème du support restent encore ouvertes. Notamment, sa généralisation complète au cas partiellement commutatif. Ceci semble pour l'instant difficile, l'approche que je propose est l'étude du support sur les graphes minimaux pour le pliage (voir annexe 4 pour quelques exemples de graphes minimaux). On calcule le support pour un des graphes minimaux et on essaie de généraliser le résultat à tous les graphes qui se replient en lui (c'est cette méthode qui a, en fait, été utilisée pour montrer les résultats de ce chapitre).
Le graphe A_4 marque la limite des généralisations au cas libre. En effet, pour l'instant nous ne sommes pas arrivés à conjecturer une forme "agréable" pour les traces n'appartenant pas au support. On peut prouver que les traces du type $ac_1 \dots c_n a$ où $c_1, \dots, c_n$ sont les parties connexes de la trace $c_1 \cdots c_n$ et telle ques $c_1 = bc'$ avec $(a, b) \notin \theta$ (on appellera *c-traces* de telle traces) n'appartiennent pas au support. Mais il en existe d'autres beaucoup plus complexes comme la trace *dabcda* pour le graphe

$$a - b - c - d.$$

Cela ressemble à des "enchevêtrements" de c-traces, enfin à quelque chose de difficile à définir et encore plus à utiliser dans une preuve. Peut-être touche-t-on là les limites de l'approche combinatoire du problème? On pourra tout de même noter que ces "enchevêtrements" apparaissent dès le graphe

A_4. Bizarrement, ce graphe a des propriétés remarquables pour d'autres problèmes liés aux commutations partielles. On pourra citer par exemple le théorême du sous-groupe dû à Droms dans le cas partiellement commutatif [**?**], ainsi que la décidabilité de certains problèmes sur des langages de traces [**?**].
Il semblerait hors de portée de vouloir trouver une algorithmique rapide pour calculer le projecteur orthogonal dans le cadre des commutations partielles alors que ce problème n'a pas encore été complètement résolu dans le cas libre (on pourra se référer à un article de Duchamp [**?**] pour connaître un algorithme de construction du projecteur orthogonal, malheureusement celui-ci s'avère trop coûteux en temps pour être utilisable sur de grands polynômes). Cependant, derrière le problème du projecteur orthogonal se cache une autre question fondamentale : Qu'est ce qui remplace l'action du groupe symétrique à droite (peut être n'est ce pas un groupe?)? Moins formellement, qu'est-ce qui remplace la notion de place dans un mot ?

Chapter 4

Automates admettant un produit de mélange

4.1 Introduction et généralités

La notion de produit de mélange dans A^* a été introduite par Chen, Fox et Lyndon dans "Free differential calculus" [?]. Un mot w est un mélange de deux mots u et v si il existe un entier p tel que $u = u_1u_2...u_p$, $v = v_1v_2...v_p$ avec $v_i, u_i \in A^*$ et $w = u_1v_1...u_nv_n$. On note uv la somme

$$\sum_{\substack{w[I]=u,\\ |w|=|I|+|J|,}} \sum_{\substack{w[J]=v\\ I\cap J=\emptyset}} w.$$

Ce produit s'étend facilement par linéarité et continuité à l'algèbre des séries à coefficients dans un semi-anneau K: $K\langle\langle A\rangle\rangle$. Lorsque ce semi-anneau est , on obtient le produit de mélange de deux langages [?] [?], ce produit préservant la rationnalité, il est très utilisé pour la théorie des langages. En 1990, Schmitt [?] a généralisé cette notion aux commutations partielles et D.Krob et G.Duchamp ont donné une formule explicite pour calculer le mélange de deux traces.
Le produit de mélange peut être défini de nombreuses façons. Cependant, il existe des caractérisations remarquables. La première utilise les translations: le produit de mélange se définit par induction comme l'unique produit

d'algèbre[1] tel que

$$\begin{cases} 11 & = & 1 \\ a^{-1}(uv) & = & (a^{-1}u)v + u(a^{-1}v) \end{cases}$$

Une autre caractérisation utilise l'application duale c du produit de mélange défini comme l'unique morphisme $c : K\langle A\rangle \to K\langle A\rangle \otimes K\langle A\rangle$ tel que

$$\begin{cases} c(1) & = & 1 \otimes 1 \\ c(au) & = & (a \otimes 1 + 1 \otimes a)c(u) \end{cases}$$

On a alors $(c(w), u \otimes v) = (w, uv)$.

4.2 Séries sur un monoïde et automates

Définition 78 *Soient $f : A^* \to X$ et $\equiv$ une congruence sur A^*. On dira que f est* $\equiv$-compatible *si*

$$u \equiv v \Rightarrow f(u) = f(v).$$

Un automate à multiplicités $\mathcal{A} = (\lambda, \mu, \gamma)$ sera dit compatible avec la congruence $\equiv$ *($\equiv$-compatible) lorsque $\mu : A^* \to K^{n\times n}$ le sera.*

La congruence la moins fine compatible avec une fonction f s'appelle traditionnellement la congruence syntactique de f. Lorsque un automate $\mathcal{A} = (\lambda, \mu, \gamma)$ est $\equiv$- compatible, on peut voir facilement que son comportement

$$\mathcal{B}(\mathcal{A}) = \sum_{w\in A^*} (\lambda\mu(w)\gamma)w$$

l'est aussi. La réciproque n'est pas vraie en général (par exemple si $\lambda = 0$) mais est vraie lorsque A est un automate minimal et K un corps (commutatif ou non) ou un anneau principal.
Dans le cas des morphismes de monoïde, $f : A^* \to M$ (c'est ici le cas de μ), la $\equiv_R$-compatibilité est testable sur R, précisément

$$(\forall (u, v) \in R)(f(u) = f(v)) \Rightarrow f \text{ est } \equiv -\text{compatible.}$$

Géométriquement, la $\equiv_R$-compatibilité de μ signifie que pour tout état q de l'automate et tout couple $(u, v) \in R$ on a $q.u = q.v$ (propriété du diamant).

[1] C'est d'ailleurs cette caractérisation qui sert à interpoler entre le produit de mélange et la concaténation [?]

Proposition 79 *Soient K un corps (commutatif ou non) et $S : A^* \to K$ une série rationnelle. Les conditions suivantes sont équivalentes:*

1. *La série S est $\equiv$-compatible.*

2. *L'automate minimal de S est $\equiv$-compatible.*

Preuve Montrons que (1) implique (2). Soit $\mathcal{A} = (\lambda, \mu, \gamma)$ l'automate minimal de S.
M.Flouret a adapté dans [**?**] le théorème de Schützenberger au cas non commutatif: il existe des mots

$$u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n \in A^*$$

tels que la matrice carrée en blocs colonnes $G = (\lambda\mu(u_i))_{i\in[1,n]}$ et la matrice carrée en blocs lignes $D = (\mu(v_i)\gamma)_{i\in[1,n]}$ soient des matrices $n \times n$ inversibles. Soient $w \equiv w'$. Alors

$$\begin{aligned} L\mu(w)R &= (\lambda(u_i w v_j)\gamma)_{1\leq i,j\leq n} \\ &= (\langle S|u_i w v_j\rangle)_{1\leq i,j\leq n} \\ &= (\langle S|u_i w' v_j\rangle)_{1\leq i,j\leq n} \\ &= L\mu(w')R. \end{aligned}$$

L'inversibilité des matrices L et R donnent alors $\mu(w') = \mu(w)$. La réciproque est immédiate.

Exemple 39 *Soit la série définie par*

$$S = \sum_{w\in A^*} (\pi_1 \circ c(w), aab + baa)w$$

où π_1 est l'application linéaire de projection[2] *de $K < A > \otimes K < A >$ dans $K < A >$ telle que $\pi_1(u \otimes v) = v$. Le coefficient en w de S est en fait le nombre de fois où aab et baa sont sous-mots de w.*
Soient $R_1 = \{(a^2, a^3), (b^2, b^3)\}$ et $R_2 = \{(aab, baa)\}$. La série S est elle $\equiv_{R_1}$-compatible? $\equiv_{R_2}$-compatible? Pour répondre à cette question, il suffit de construire son automate minimal.

[2] cf **??**

(8,5) (1,2.5)10a (2,4)10b (6,4)10d (7,2.5)10e (6,1)10f (2,1)10h
[angleA=270,angleB=90,loopsize=0.5,arm=0.5,linearc=.2]->aaa + b
[angleA=90,angleB=270,loopsize=0.5,arm=0.5,linearc=.2]->eea + b ->aba
->bda ->deb ->ahb ->hfa ->fea <-(1.3,2.5)(2,2.5):U1
<-(6,2.5)(6.7,2.5):U1

Un rapide calcul matriciel nous permet alors d'observer qu'elle est $\equiv_{R_1}$ compatible mais pas $\equiv_{R_2}$ compatible.

Ce résultat peut être étendu aux anneaux principaux (comme , $/p[X]$, $[X]$ ...). Il est clair que la $\equiv$-compatibilité est stable par combinaison linéaire (i.e. si $(S_i)_{i\in I}$ est une famille de séries $\equiv$- compatible alors $\sum \alpha_i S_{i,j} \beta_j$ est encore $\equiv$-compatible) et produit de Hadamard. Ce n'est pas le cas du produit de Cauchy comme le montre l'exemple:

$$R = \{(ab, ba)\}, S = a \text{ et } T = b.$$

4.3 Mélanges d'automates à multiplicités sur des semi-anneaux

Il est possible d'adapter pour les automates le produit de mélange des langages ou des séries rationnelles.
Soient $\mathcal{A}_1 = (\lambda_1, \mu_1, \gamma_1)$ et $\mathcal{A}_2 = (\lambda_2, \mu_2, \gamma_2)$ deux automates sur le même semi-anneau K. Leur produit de mélange sera noté

$$\mathcal{A}_1\mathcal{A}_2 = (\lambda_1 \otimes \lambda_2, (\mu_1(a) \otimes I_2 + I_1 \otimes \mu_2(a))_{a\in A}, \gamma_1 \otimes \gamma_2).$$

La justification de cette définition se trouve dans [**?**]. Dans le cas des corps la compatibilité des automates avec le produit de mélange est équivalente à la compatibilité du coproduit. Ce que montre le théorème suivant.

Théorème 80 *Supposons que K soit un corps. Soit $\equiv$ une congruence à fibres finies*[3].

1. *Les assertions suivantes sont équivalentes.*
   (a) *Si $\mathcal{A}_1$ et $\mathcal{A}_2$ sont deux automates $\equiv$-compatibles alors $\mathcal{A}_1\mathcal{A}_2$ l'est aussi.*

[3]Une congruence à fibres finies est une congruence dont les classes sont finies.

(b) Le coproduit respecte $\equiv$ en le sens suivant.
Pour tout couple $(u, v) \in A^* \times A^*$, on a

$$u \equiv v \Rightarrow c(u) \equiv^{\otimes 2} c(v)$$

où $\equiv^{\otimes 2}$ désigne le carré tensoriel de $\equiv$ défini comme étant le noyau de l'application naturelle

$$K\langle A\rangle \otimes K\langle A\rangle \to K[A^*/_{\equiv}] \otimes K[A^*/_{\equiv}]$$

2. Les assertions précédentes impliquent que si S et T sont deux séries $\equiv$-compatibles alors ST l'est aussi.

Preuve Pour montrer que (1.b) implique (1.a), il suffit de remarquer que si on pose $\mathcal{A}_1 = (\lambda_1, \mu_1, \gamma_1)$, $\mathcal{A}_2 = (\lambda_2, \mu_2, \gamma_2)$ et $\mathcal{A}_1\mathcal{A}_2 = (\lambda, \mu, \gamma)$ alors $\mu = (\mu_1 \otimes \mu_2) \circ c$.
Montrons maintenant que (1.a) implique (1.b). Considérons la relation d'ordre produit sur les multidegrés $(\alpha, \beta \in^{(A)})$:

$$(\alpha \leq \beta) \Leftrightarrow (\forall a \in A)(\alpha(a) \leq \beta(a)).$$

Soit w un mot. On notera $[w] := a \to |w|_a$ son multidegré et $Cl(w)$ sa classe d'équivalence modulo $\equiv$.
Soient $w_1 \equiv w_2$ deux mots équivalents. Posons

$$t_1 = \sup_{w \in Cl(w_1)} [w].$$

Et soient $\mathcal{C}_1, \ldots, \mathcal{C}_k$ les classes contenant au moins un mot de multidegré inférieur ou égal à t_1. Posons

$$t_2 = \sup_{w \in \bigcup_{i=1}^{k} \mathcal{C}_i} [w]$$

(5,5) (0,5)(2.5,1)(5,5) linestyle=dashed (1.2,3)(3.85,3) (0.6,4)(4.4,4)
(1.6,2.4)(1.6,4)(2,4)(2,1.8) (1,3.4)(1.6,3.4) (2,3.6)(2.4,3.6)(2.4,1.2)
(2.4,2.2)(3.2,2.2) (2.4,3)(3,3)(3,2.2) (4,3.4)(3,3.4)(3,2.2)
(3,3.4)(3,3.6)(4.1,3.6) (0.4,4.4)(4.6,4.4) (1,5)(1,4.4) (3,5)(3,2.2) (4.4,3)t_1
(4.8,4)t_2 (2.5,0.5)Classes de $\equiv$ dans A^*

(t_1 et t_2 sont bien définies grâce aux hypothèses sur les fibres finies). On définit la troncature de $\equiv$ par

$$u \sim v \Leftrightarrow \begin{cases} Cl(u) \not\subseteq A^{\leq t_2} \text{ et } Cl(v) \not\subseteq A^{\leq t_2} \\ \text{ou} \\ Cl(u) = Cl(v) \end{cases}$$

Le lemme suivant est immédiat.

Lemme 81 *1. La relation d'équivalence $\sim$ est une congruence plus grossière que $\equiv$.*

2. Les classes de $\sim$ sont $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k, \mathcal{C}_{k+1}, \ldots, \mathcal{C}_{p-1}$ et

$$\mathcal{C}_p = \bigcup_{Cl(w) \not\subseteq A^{\leq t_2}} Cl(w)$$

où $\mathcal{C}_1, \ldots, \mathcal{C}_{p-1}$ sont des classes d'équivalences de $\equiv$ induites sur $A^{\leq t_2}$.

3. En particulier, si $w_1 \sim w_2$ et $[w_1] \leq t_1$ alors $w_1 \equiv w_2$.

(5,5) (0,5)(2.5,1)(5,5) linestyle=dashed (1.2,3)(3.85,3) (0.6,4)(4.4,4) (1.6,2.4)(1.6,4)(2,4)(2,1.8) (1,3.4)(1.6,3.4) (2,3.6)(2.4,3.6)(2.4,1.2) (2.4,2.2)(3.2,2.2) (2.4,3)(3,3)(3,2.2) (4,3.4)(3,3.4)(3,2.2) (4.4,3)t_1 (4.8,4)t_2 (2.5,0.5)Classes de $\sim$ dans A^*

Pour tout $a \in A$, on définit $\mu(a)$ comme la matrice (par rapport à la base $(\mathcal{C}_j)_{j\in[1,p]}$) de l'application linéaire $u \to a.u \in A^*/_\sim$, où u représente la classe de u dans $\sim$. Plus précisément,

$$\mu(w) : \mathcal{C}_j \to w.\mathcal{C}_j.$$

Alors, μ est $\equiv$-compatible et les automates $\mathcal{A}_{i,j} = (e_{\mathcal{C}_i}^T, \mu, e_{\mathcal{C}_j})$, où $(e_{\mathcal{C}_i})_{i\leq i\leq p}$ est la base canonique de $K^{p\times 1}$, sont $\equiv$-compatibles. Donc, d'après (1.a) les p^4 automates $\mathcal{A}_{i_1,j_1}\mathcal{A}_{i_2,j_2}$ sont aussi $\sim$-compatibles. Ceci implique que le morphisme $\nu : A^* \to K^{p^2\times p^2}$ défini par $\nu(a) = \mu(a) \otimes I_p + I_p \otimes \mu(a)$ pour tout $a \in A$, est $\sim$-compatible. Donc, comme $w_1 \equiv w_2$,

$$\begin{array}{rcl} \sum_{I+J=[1\ldots n]} \mu(w_1[I]) \otimes \mu(w_1[J]) & = & \nu(w_1) \\ & = & \nu(w_2) \\ & = & \sum_{I+J=[1,\ldots,n]} \mu(w_2[I]) \otimes \mu(w2[J]), \end{array}$$

ce qui prouve (en évaluant l'application linéaire sur $1 \otimes 1$) que

$$\sum_{I+J=[1,\ldots,n]} w_2[I] \otimes w_2[J].$$

Mais $[w_i[I]], [w_i[J]] \leq t_2$ et le lemme **??** implique $c(w_1) \equiv^{\otimes 2} c(w_2)$.

Maintenant, montrons que (1) implique (2). En fait on a,

$$(ST, w) = (S \otimes T, c(w)).$$

Comme S et T sont $\equiv$-compatible, l'assertion (1.b) implique la $\equiv$-compatibilité de ST.

Exemple 40 *Soient les automates,*

(10,5) (2,2)10a (5,2)10b (7,3)10c (7,1)10e (9,2)10d
[angleA=90,angleB=270,loopsize=0.5,arm=0.5,linearc=.2]->aaa ->bca
->cdb ->beb ->eda ->(1.3,2)(1.7,2) ->(4.3,2)(4.7,2) ->(9.3,2)(9.7,2)
(1,2)$\mathcal{A}_1$ *: (4,2)*$\mathcal{A}_2$ *:*

Soit $\equiv_\theta$ la congruence engendrée par les couples $\{(ab, ba)\}$. Les deux automates sont $\equiv_\theta$ compatibles donc l'automate

(2,0)(10,5) (5,2)10b (7,3)10c (7,1)10e (9,2)10d ->bca ->cdb ->beb ->eda
[angleA=90,angleB=270,loopsize=0.5,arm=0.5,linearc=.2]->dda
[angleA=270,angleB=90,loopsize=0.5,arm=0.5,linearc=.2]->bba
[angleB=180,loopsize=0.5,arm=0.5,linearc=.2]->cca
[angleB=180,loopsize=-0.5,arm=0.5,linearc=.2]->eea (3,2)$\mathcal{A}_1\mathcal{A}_2$ *:*
<-(5.3,2)(5.7,2) ->(8.7,2)(8.3,2)

l'est aussi.

En fait, (1.b) peut être formulé sans les hypothèses sur K et les fibres de $\equiv$. Dans le cas le plus général (1.b) implique (1.a). Ceci nous permet de donner la définition suivante.

Définition 82 *Soit K un semi-anneau*[4]*. Une congruence sera appelée $K-$compatible si (1.b) est vérifiée.*

[4]Nous considérons ici que les axiomes des semi-anneaux sont stables, ce qui implique que 0_K est l'élément absorbant.

Cette définition est équivalente au fait qu'il existe une application "coproduit quotient" $c_{\equiv}$ telle que le diagramme suivant commute:

$K < A > cK < A > \otimes K < A > \pi_{\equiv}\pi_{\equiv} \otimes \pi_{\equiv} K[A^*/_{\equiv}] c_{\equiv} K[A^*/_{\equiv}] \otimes K[A^*/_{\equiv}]$fig.1

Définition 83 *Soit $\equiv$ une congruence $K-$ compatible alors le diagramme précédent nous permet de définir un produit de mélange $_{\equiv}$ sur $A^*/_{\equiv}$ par $(u_{\equiv}v, w) = (u \otimes v, c_{\equiv}(w))$.*

Exemple 41 *1. Nous verrons plus loin que la congruence $\equiv$ engendrée par le couple (a^9, b^3) est $/3-$ compatible. On peut effectuer le calcul suivant*

$$a^9_{\equiv} b = \sum_{i=0}^{9} a^{9-i} b a^i + b^4.$$

2. Soit $\equiv$ la congruence engendrée par $\{(a^2b, ba^2), (ab^2, b^2a), (abab, baba)\}$ (la proposition ?? montrera qu'elle est $/2-$ compatible).

$$\begin{aligned} ab^2_{\equiv} a^2bc &= (ab^2_{\equiv} a^2b)c + (b^2a^2b)ca \\ &\quad +(a_{\equiv} a^2b)cb^2 + (1_{\equiv} a^2b)cab^2 \\ &= b^3a^3c + b^3a^2ca + ba^3cb^2 + a^2bcab^2. \end{aligned}$$

On peut remarquer que si $\equiv$ est engendrée par $\{(a^2b, ba^2), (ab^2, b^2a)\}$ le même calcul donne

$$ab^2_{\equiv} a^2bc = b^3a^3c + abababc + bababac + b^3a^2ca + ba^3cb^2 + a^2bcab^2.$$

4.4 Le cas général

Nous utiliserons par la suite de quelques propriétés élémentaires que nous allons examiner dans cette section.

Lemme 84 *(Propriétés des scalaires) Soit $\phi : K_1 \to K_2$ un morphisme de semi-anneaux. Alors*

1. *(a) Si $\equiv$ est K_1- compatible alors elle est K_2- compatible.*
   (b) Si ϕ est injective alors la réciproque est vraie.
2. *Une congruence est $K-$ compatible si et seulement si elle est $.1_K-$ compatible.*

Preuve Les assertions 1.a et 1.b proviennent du fait que l'application restreinte $.1_{K_1} \to .1_{K_2}$ est surjective.
La distributivité du produit par rapport à l'addition dans K ainsi que la formule de developpement du coproduit implique l'assertion 2.
Le lemme **??** impliquent que si une congruence est $-$ compatible alors elle est $K-$ compatible pour tout semi-anneau K. Soit K un semi-anneau, on s'intéressera dans la suite de la discussion au sous-semi-anneau[5] $.1_K = K_0$ que l'on peut caractériser par deux grandeurs:

$$\rho(K) = \inf\{e \in /\exists r \in^*, e.1_K = (e+r).1_K\}$$

et si $\rho(K) < \infty$

$$p(K) = \inf\{r \in^* /\rho(K).1_K = (\rho(K)+r).1_K\}$$

(13,6) arrowscale=1.5 (0,3)(6,3) =0.0+1.55(,3)2pt=0.0+1.5,=1.0+1.54->(,3)(¡3)|-|(0,2)(6,2)[90](3,2)$\rho(K)$(8,3)ı=0+30,=25+3012->(0,0)2ı [linestyle=dotted]<-(0,0)1.6170190 linestyle=none[c](0,0)1.2240300$p(K)$ =0+3012(2;)2pt

Remarque 42 *1. Si $\rho(K) = 0$ et $p(K) = 1$ alors K est l'anneau nul.*

2. *Si $\rho(K) = 0$ et $p(K) > 1$ alors K est un anneau de caractéristique $p(K)$.*

3. *Si $0 < \rho(K) < \infty$ alors K n'est pas un anneau.*

4. *Si $\rho(K) = \infty$ alors $.1_K$ est plongeable dans un anneau de caractéristique 0 (i.e.).*

Exemple 43 *1. Soit $T = (, \max, +)$ le semi-anneau tropical. Montrer qu'une congruence est $T-$ compatible revient à montrer qu'elle est $-$ compatible.*

2. *Soit H le corps des quaternions. Montrer qu'une congruence est $H-$ compatible revient à montrer qu'elle est $-$ compatible.*

3. *Soit n un entier. Montrer qu'une congruence est $/n[i]-$ compatible revient à montrer qu'elle est $/n-$ compatible.*

[5] L'action de sur K est définie par $0.x = 0_K$ et $(n+1).x = n.x + x$ pour tout $n \in$ et tout $x \in K$.

Lemme 85 *(Propriétés des relateurs)*

1. *Si $\equiv_1$ et $\equiv_2$ sont $K-$ compatible alors $\equiv_1 \vee \equiv_2$ et $\equiv_1 \wedge \equiv_2$ sont $K-$ compatibles.*

2. *Soit R une relation sur A^*. La congruence $\equiv_R$ est $K-$ compatible si et seulement si pour tout couple $(w_1, w_2) \in R$ on a*

$$c(w_1) \equiv_R^{\otimes 2} c(w_2).$$

3. *Soit $B \subseteq A$ un sous alphabet de A. Si $\equiv$ est $K-$ compatible alors la congruence $\equiv_B$ induite sur B^* aussi.*

Preuve Les assertions 1) et 3) sont évidentes. Montrons 2). Supposons que pour tout couple $(w_1, w_2) \in R$, $c(w_1) \equiv_R^{\otimes 2} c(w_2)$. Soient $w \equiv_R w'$ deux mots équivalents. Il existe une suite d' équivalences

$$w_0 = w \equiv_R w_1 \equiv_R \ldots \equiv_R w_{n-1} \equiv_R w_n = w'$$

telle que pour tout entier $i \in [1, \ldots, n-1]$, on ait $w_i = u_i v_i t_i$ et $w_{i+1} = u_i v_i' t_i$ avec $(v_i, v_i') \in R$. Alors,

$$\begin{array}{rcc} c(w_i) & \equiv_R^{\otimes 2} & c(u_i)c(v_i)c_k(t_i) \\ & \equiv_R^{\otimes 2} & c(u_i)c(v_i')c(t_i) \\ & \equiv_R^{\otimes 2} & c(w_{i+1}) \end{array}$$

et par transitivité $c(w) \equiv_R^{\otimes 2} c(w')$.
La réciproque est immédiate.
Nous aurons besoin du lemme suivant dont la démonstration est immédiate.

Lemme 86 *Soient $u \in A^+$ et n l'entier maximal tel que u puisse s'écrire sous la forme $u = u_1 a^n$ avec $u_1 \in A^*$ et $a \in A$. Alors, pour tout K on a*

$$(c(u), u_1 \otimes a^n) = 1$$

Lemme 87 *Toute congruence engendrée par des relateurs de la forme $a \equiv b$ (échanges) et $cd \equiv dc$ (commutations) avec $a, b, c, d \in A$ est $K-$ compatible.*

Preuve Il suffit de remarquer qu'elle est compatible.

$$c(a) = a \otimes 1 + 1 \otimes a \equiv^{\otimes 2} b \otimes 1 + 1 \otimes b = c(b)$$

pour tout $a \equiv b \in A$ et

$$c(cd) = cd \otimes 1 + c \otimes d + d \otimes c + 1 \otimes cd \equiv^{\otimes 2} dc \otimes 1 + c \otimes d + d \otimes c + 1 \otimes dc = c(dc)$$

pour tout couple de lettres (c, d) tel que $cd \equiv dc$.

4.5 Le cas $\rho(K) > 0$

Dans cette section, on considérera que K n'est pas un anneau ou un anneau de caractéristique 0 (ce qui est équivalent à $\rho(K) \neq 0$).

4.5.1 Le cas booléen

Considérons tout d'abord le cas où $K =$ le semi-anneau booléen. Les congruences $-$ compatibles sont caractérisées par la proposition suivante.

Proposition 88 *Une congruence est $-$ compatible si et seulement si elle est engendrée par des relateurs du type*

$$\begin{cases} a \equiv 1 & \textit{(EL) effacement de lettres} \\ a \equiv b & \textit{(IL) identification de lettres} \\ ab \equiv ba & \textit{(CL) commutation de lettres} \end{cases}$$

Preuve Montrons tout d'abord qu'une congruence est $-$ compatible si elle est engendrée par des relateurs de type (EL), (IL) et (CL). D'après les lemmes **??**.2 et **??**, il suffit de montrer que les relateurs de type (EL) sont $-$ compatibles. En fait, on a

$$a \equiv 1 \Rightarrow c(a) = a \otimes 1 + 1 \otimes a \equiv^{\otimes 2} (1+1).1 \otimes 1 = c(1).$$

Ceci prouve le résultat.

Montrons maintenant la réciproque. Soit

$$A' = \{a \in A / a \not\equiv 1\}$$

et $S \subseteq A'$ une section de $\equiv \cup A' \times A'$. Il est clair que si (EL) est la liste des couples $\{(a,1)\}_{a \in A - A'}$ et (IL) la liste des couples $\{(a,b)\}_{a \equiv b, a \in S, b \in A' - S}$ alors $\equiv$ est engendrée par $\equiv_S$ (la restriction de $\equiv$ à S^*), (IL) et (EL). Il suffit donc de prouver que $\equiv_S$ est engendrée uniquement par des relateurs de type (CL). Montrons tout d'abord que $\equiv_S$ est multihomogène. Notons $\equiv_m$ la partie multihomogène de $\equiv_S$ (i.e. la congruence engendrée par les couples (u,v) tels que $u \equiv_S v$ et $[u] = [v]$).
Si $\equiv_S$ n'est pas multihomogène, il existe un couple (u,v) tel que $u \equiv_S v$ et $u \not\equiv_m v$ avec $|u|$ minimum.

Supposons que $u = 1$. On a $v \neq 1$ (puisque $u \not\equiv_m v$). Posons $v = v_1 a$ avec $a \in A$. L'égalité

$$(v_1 \otimes a, c(1)) = 1$$

(où on note w la classe de w pour $\equiv_S$) entraîne $a \equiv_S 1$, ce qui contredit le fait que $\equiv_S$ sépare $S \cup 1$. Donc $u \neq 1$.
Écrivons u sous la forme $u = u_1 a$ avec $a \in A$. Comme $(c(u), u_1 \otimes a) = 1$, il existe deux sous-mots complémentaires v_I et v_J de v tels que $v_I \otimes v_J \equiv_S u_1 \otimes a$. Alors $u = u_1 a \equiv_S v_I v_J$, ce qui implique $v \equiv_m v_I v_J$. On ne peut pas avoir $v_J = 1$ sinon $a \equiv 1$. Posons $v_J = wb$ avec $b \in A$ alors

$$(w \otimes b, a \otimes 1 + 1 \otimes a) = 1$$

d'où $b \equiv a$ et $w \equiv 1$, soit $w \equiv_m 1$, ce qui implique $w = 1$ et $v_J = b$. Comme $\equiv_S$ sépare $S \cup \{1\}$, on a $a = b$. De plus, à cause de l'hypothèse de minimalité, $v_I \equiv_S u_1$ implique $v_I \equiv_m u_1$ et alors

$$v \equiv_m v_I v_J \equiv_m u_1 a = u$$

ce qui contredit notre hypothèse et prouve que $\equiv_S$ est multihomogène.

Notons $\equiv_\theta$ la congruence engendrée par les couples (ab, ba) avec $a, b \in A$ et $ab \equiv_S ba$ (c'est la partie de $\equiv_m$ engendrée par des relateurs de type (LC)). On a besoin du lemme suivant.

Lemme 89 *Soient $u \equiv_S v$ et $v \in A^*a$. Alors il existe $u_1 \equiv_\theta v$ tel que $u_1 \in A^*a$.*

Preuve De ce qui précède on a $[u] = [v]$ (l'égalité en multidegré) et en particulier $|u|_a \neq 0$. Soit $u_1 = u_2 a u_2'$ un mot tel que $u_1 \equiv_\theta u$ et $|u_2'|$ minimum (en particulier $|u_2'|_a = 0$). Si $u_2' = 1$, la proposition est démontrée. Sinon on peut écrire $u_2' = bu_3$ avec $b \in A$ et $u_3 \in A^*$. Soit $a^q b$ le sous-mot de u_1 avec q maximum. Il existe deux mots complémentaires v_I et v_J tels que

$$a^q b \otimes w \equiv_S^{\otimes 2} v_I \otimes v_J$$

où w est le sous-mot complémentaire de $a^q b$ dans u (ce qui entraîne $|w|_a = 0$). Alors $a^q b \equiv_S v_I$ et donc $v_I = a^{q-i} b a^i$. Mais $i > 0$, puisque $v \in A^*a$ et que $[w] = [v_j]$. De $a^q b \equiv_S v_I$, on déduit,

$$ab \otimes a^{q-1} \equiv_S^{\otimes 2} ab \otimes a^{q-1} + ba \otimes a^{q-1}.$$

On a donc $ab \equiv ba$. Ainsi, $u \equiv_\theta u_2abu_3 \equiv_\theta u_2bau_3$, ce qui contredit la minimalité de $|u'_2|$ et prouve le résultat.

Fin de la preuve de la proposition ?? Supposons que $\equiv_S$ n'est pas engendrée par des relations de commutations. Soit (u, v) un couple de mots tels que $u \equiv_S v$ et $u \not\equiv_\theta v$ avec $|u| + |v|$ minimal. Soit $a \in S$ une lettre telle que

$$u \equiv_\theta u_1 a^r = u' \text{ et } v \equiv v_1 a^s = v'$$

avec $r, s \neq 0$, $r + s \geq 2$ maximal (l'existence d'une telle lettre découle directement du lemme **??**). Sans perte de généralité, supposons $0 < r \leq s$. On a $(u_1 \otimes a^r c(u)) = 1$ et donc il existe deux sous-mots v'_I et v'_J de v' tels que

$$u_1 \otimes a^r \equiv_S^{\otimes 2} v'_I \otimes v'_J.$$

La multihomogénéité de $\equiv_S$ donne $v'_J = a^r$. On peut alors écrire $v'_I = v_2 a^\alpha$ où v_2 est un sous-mot de v_1.
Si $\alpha > 0$, on a $u_1 \equiv_S v_2 a^\alpha$ et, d'après le lemme **??**, il existe une trace u_2 telle que $u_1 \equiv_\theta u_2 a$. Alors $u \equiv_\theta u_2 a^{r+1}$, ce qui contredit la maximalité de $s + r$. D'où $\alpha = 0$ et $v'_I = v_2 \notin S^* a$ est un sous-mot de v_1. On a donc

$$|u|_a - r = |u_1|_a = |v'_I|_a \leq |v_1|_a = |v|_a - s.$$

Ceci entraîne $s \leq r$ et $s = r$. Comme $v'_I \notin S^* a$, on a $v'_I = v_1$ et $u_1 \equiv_\theta v_1$, ce qui implique

$$u \equiv_\theta u_1 a^r \equiv_\theta v_1 a^r \equiv_\theta v$$

et prouve le résultat.

4.5.2 Autres semi-anneaux tels que $\rho(K) \neq 0$

Théorème 90 *Soit K un semi-anneau tel que $\rho(K) > 0$. Alors une congruence $\equiv$ est $K-$ compatible si et seulement si*

1. *Si $1_K + 1_K = 1_K$, elle est engendrée par des relateurs de la forme (EL), (IL) ou (CL)*

2. *Si $1_K + 1_K \neq 1_K$, elle est engendrée par des relateurs de la forme (IL) et (CL)*

Preuve Dans le point (1) on a $\hookrightarrow K$, le résultat se montre en utilisant le lemme **??** et la proposition **??**. Montrons le cas (2), soit K un semi-anneau tel que $1_K+1_K \neq 1_K$, alors il existe un morphisme de $.1_K$ sur (ce morphisme envoie 0 sur 0 et tout élément $x \neq 0$ sur 1). Le lemme **??** implique que toute congruence $K-$ compatible est aussi $-$ compatible. Donc $\equiv$ est engendrée par des relateurs de type (EL), (IL) ou (CL). En examinant chacun de ces types, on constate que seul (EL) est impossible. Ceci prouve le résultat.

Remarque 44 *La classe des anneaux de caractéristique* 0 *et, plus généralement, de tous les semi-anneaux tels que* $\rho(K) = \infty$ *rentre dans le cadre de ce théorème (2) et on retrouve [**?**].*

4.6 Le cas des anneaux

4.6.1 Cas général

Nous analysons ici les congruences de type fini telles que $K[A^*/_{\equiv}]$ soit $K-$ compatible. On peut, sans perte de généralité, supposer A fini et c'est ce que nous ferons dans l'ensemble de ce numéro.

Définition 91 *Soit K un anneau et $\equiv$ une congruence $K-$ compatible. On dira qu'un polynôme P de $K[A^*/_{\equiv}]$ est primitif si et seulement si*

$$c_{\equiv}(P) = P \otimes 1 + 1 \otimes P$$

Proposition 92 *Le sous-ensemble des polynômes primitifs forme une algèbre de Lie pour le crochet* $[\quad,\quad]$ *défini par* $[P,Q] = PQ - QP$.

Preuve Soient P et Q deux polynômes primitifs on a alors

$$\begin{aligned} c_{\equiv}([P,Q]) &= c_{\equiv}(PQ-QP) \\ &= c_{\equiv}(P)c_{\equiv}(Q) - c_{\equiv}(Q)c_{\equiv}(P) \\ &= (P\otimes 1 + 1\otimes P)(Q\otimes 1 + 1\otimes Q) + \\ &\quad +(Q\otimes 1 + 1\otimes Q)(P\otimes 1 + 1\otimes P) \\ &= [P,Q]\otimes 1 + 1\otimes [P,Q]. \end{aligned}$$

Ceci montre que cet ensemble est stable pour le crochet de Lie. Il est évidemment stable aussi pour les combinaisons linéaires.

Remarque 45 *Si l'anneau est de caractéristique* 0*, cette algèbre est l'algèbre de Lie partiellement commutative libre (théorème de Friedrich's).*

Définition 93 *Soit* $\equiv$ *une congruence sur* A^* *finiment engendrée par un ensemble de relateurs* R*, on dira que* R *est* `clos` *si et seulement si pour tout couple* (u, v) *tel que* $u \equiv v$*,* $u \neq v$ *et* $\max\{|u|, |v|\} < max\{|u|, |v|/(u, v) \in R\}$ *on a* $(u, v) \in R$*.*

Toute congruence finiment engendrée sur A^* est engendrée par un ensemble de relateurs clos. Comme A est supposé fini, cet ensemble de relateurs peut être choisi fini.

Proposition 94 *Une congruence* $\equiv$ *sur* A^* *finiment engendrée est* $K-$ *compatible si et seulement si il existe une famille finie d'ensembles de relateurs* $(S_i)_{i\in[0,n]}$ *telle que*

1. $S_0 = \emptyset$*.*
2. *La congruence* $\equiv$ *est engendrée par l'ensemble de relateurs* $\bigcup_{i\in[1,n]} S_i$*.*
3. *Chaque ensemble* S_i *avec* $i > 0$ *est un ensemble de couples* (u, v) *de* $A^*/_{\equiv_{\bigcup_{j\in[1,i-1]} S_j}}$ *tels que* $u - v$ *est primitif dans* $K[A^*/_{\equiv_{\bigcup_{j\in[1,i-1]} S_j}}]$*.*

Preuve Par induction sur n, si une telle famille existe alors $\equiv$ est $K-$ compatible.
Montrons alors la réciproque. Considérons un ensemble de relateurs clos fini R engendrant $\equiv$. On construit la famille $(S_i)_{i\in}$ de la façon suivante.

1. On pose $S_0 = R_0 = \emptyset$
2. Pour tout $i > 0$, S_i est l'ensemble des paires $(u, v) \in R - \bigcup_{j\leq i-1} R_j$ telles que $u - v$ soit un polynôme primitif de $K[A^*/_{\equiv_{\bigcup_{j\leq i-1} S_j}}]$.
3. Et R_i est l'ensemble des paires $(u, v) \in R - \bigcup_{j\leq i-1} R_j$ telles que $u \equiv_{S_i} v$.

Pour montrer le résultat, il suffit donc de prouver que si $\equiv_R$ n'est pas engendrée par $\bigcup_{j\leq i-1} S_j$ alors $S_i \neq \emptyset$. Supposons $R - \bigcup_{j\leq i-1} R_j \neq \emptyset$ et soit $(u, v) \in R - \bigcup_{j\leq i-1} R_j$ avec $\max\{|u|, |v|\}$ minimal. Supposons que

$$c(u - v) \not\equiv^{\otimes 2}_{\bigcup_{j\leq i-1} S_j} (u - v) \otimes 1 + 1 \otimes (u - v).$$

Soit

$$Q := c(u-v)-(u-v)\otimes 1-1\otimes(u-v) = \sum_{\substack{I_1+J_1=[1,|u|]\\ I_1,J_1\neq\emptyset}} u_{I_1}\otimes u_{J_1} + \sum_{\substack{I_2+J_2=[1,|v|]\\ I_2,J_2\neq\emptyset}} v_{I_2}\otimes v_{J_2},$$

alors $Q \not\equiv^{\otimes 2}_{\bigcup_{j\leq i-1} S_j} 0$ et $Q \equiv^{\otimes 2}_{R} 0$. On en déduit trois possibilités:

1. Il existe deux paires de sous-mots propres de u, (u_{I_1}, u_{J_1}) et (u_{I_2}, u_{J_2}) telles que

$$u_{I_1}\otimes u_{J_1} \equiv^{\otimes 2} u_{I_2}\otimes u_{J_2} \text{ et } u_{I_1}\otimes u_{J_1} \not\equiv^{\otimes 2}_{\bigcup_{j\leq i-1} S_j} u_{I_2}\otimes u_{J_2}.$$

2. Il existe deux paires de sous-mots propres de v, (v_{I_1}, v_{J_1}) et (v_{I_2}, v_{J_2}) telles que

$$v_{I_1}\otimes v_{J_1} \equiv^{\otimes 2} v_{I_2}\otimes v_{J_2} \text{ et } v_{I_1}\otimes v_{J_1} \not\equiv^{\otimes 2}_{\bigcup_{j\leq i-1} S_j} v_{I_2}\otimes v_{J_2}.$$

3. Il existe une paire de sous-mots propres de u, (u_{I_1}, u_{J_1}) et une paire de sous-mots propres de v, (v_{I_2}, v_{J_2}) telles que

$$u_{I_1}\otimes u_{J_1} \equiv^{\otimes 2} v_{I_2}\otimes v_{J_2} \text{ et } u_{I_1}\otimes u_{J_1} \not\equiv^{\otimes 2}_{\bigcup_{j\leq i-1} S_j} v_{I_2}\otimes v_{J_2}.$$

Pour ces trois cas l'argument est le même, nous ne développerons donc que le premier. On doit examiner deux cas: $u_{I_1} \not\equiv_{\bigcup_{j\leq i-1} S_i} u_{I_2}$ ou $u_{J_1} \not\equiv_{\bigcup_{j\leq i-1} S_i} u_{J_2}$. Supposons que $u_{I_1} \not\equiv_{\bigcup_{j\leq i-1} S_i} u_{I_2}$ (l'autre cas étant totalement similaire). Alors on a

$$\max\{|u_{I_1}, u_{I_2}|\} < \max\{|u|, |v|\},$$

comme R est clos, ceci implique que $(u_{I_1}, u_{I_2}) \in R - \cup_{j\leq i-1} R_j$, ce qui contredit la minimalité de $\max\{|u|, |v|\}$.
Donc $R - \cup_{j\leq i-1} R_i = \emptyset$, ce qui contredit nos hypothèses.
Comme R est un ensemble fini, il existe nécessairement un entier $n \geq 0$ tel que $S_i = \emptyset$ pour tout $i \geq n$, ce qui prouve le résultat.

Exemple 46 *Posons $K = /2$ et considérons la congruence $\equiv$ engendrée par les couples $\{(a^2b, ba^2), (b^2a, ab^2), (abab, baba)\}$. Cet ensemble est clos. Si*

on cherche les couples (u, v) tels que $u - v$ soit primitif, on trouve $S_1 = \{(a^2b, ba^2), (b^2a, ab2)\}$. On a alors

$$\begin{aligned} c_{/2}(abab - baba) &= 1 \otimes abab + b \otimes a^2b + a \otimes ab^2 + \\ &\quad + abab \otimes 1 + a^2b \otimes b + ab^2 \otimes a + \\ &\quad 1 \otimes baba + a \otimes b^2a + b \otimes ba^2 + \\ &\quad + baba \otimes 1 + b^2a \otimes a + ba^2 \otimes b + \\ &\equiv_{S_1}^{\otimes 2} (abab - baba) \otimes 1 + 1 \otimes (abab - baba) \end{aligned}$$

La famille recherchée est donc $(\emptyset, \{(a^2b, ba^2), (ab^2, b^2a)\}, \{(abab, baba)\})$.
On peut remarquer qu'une telle congruence n'est pas $-$ compatible.

La proposition **??** permet de justifier les définitions suivantes.

Définition 95 *On appellera* `découpage primitif` *d'une congruence K- compatible une famille $(S_i)_{i\in[1,n]}$ d'ensembles de relateurs deux à deux disjoints vérifiant les conditions de la proposition* **??**.
La `profondeur` *d'une congruence $K-$ compatible $\equiv$ sera le plus petit entier n tel qu'il existe un découpage primitif $(S_i)_{i\in[1,n]}$ de $\equiv$, on notera $\gamma_K(\equiv)$ une telle grandeur.*
L'entier $\Gamma(K)$ représentera la borne supérieure de l'ensemble des $\gamma_K(\equiv)$ pour $\equiv K-$ compatible.

4.6.2 Congruence compatible et image miroir

Comme dans les précédents chapitres, on notera w l'image miroir du mot w. Soit α l'application linéaire de $K < A >$ dans $K < A >$ telle que $\alpha(w) = (-1)^{|w|}w$ (c'est l'antipode de $K < A >$ munie du coproduit c et de la coünité $P \to (P, 1)$).

Définition 96 *Soit $\equiv$ une congruence. On notera $\pi_\equiv : A^* \to A^*/_\equiv$ la projection naturelle et on dira qu'un monoïde $\equiv$ est* `K-compatible avec l'antipode` *si et seulement si les quatre conditions suivantes sont vérifiées:*

1. *La congruence $\equiv$ est $K-$ compatible.*
2. *Il existe une application linéaire $\alpha_\equiv$ telle que $\pi_\equiv \circ \alpha = \alpha_\equiv \circ \pi_\equiv$.*
3. *Pour tout couple $(u, v) \in ({}^*/_\equiv)^2$, $u - v$ primitif implique $\alpha_\equiv(u - v) = v - u$.*

4. *Il existe un morphisme* $s_\equiv$ *de* ${}^*/_\equiv$ *dans* K *tel que* $s_\equiv \circ \pi_\equiv(w) = (-1)^{|w|}$ *pour tout* $w \in A^*$.

On aura besoin du lemme suivant.

Lemme 97 *Soit* $\equiv$ *une congruence* K*-compatible avec l'antipode. Soit* $\equiv_2$ *une congruence* $K-$ *compatible sur* ${A^*}/_\equiv$ *telle que* $\equiv_2$ *soit engendrée par des couples* (u, v) *avec* $u - v$ *primitif. Alors la congruence* $\equiv \vee \equiv_2$ *est* K*-compatible avec l'antipode.*

Preuve La partie (1) de la définition est immédiate.
Montrons tout d'abord que si $u \equiv v$ $(u, v \in A)$ alors $u \equiv v$. Il suffit de remarquer que $u = (-1)^{|u|}\alpha(u)$. Et donc

$$\pi_\equiv(u) = s_\equiv(\pi_\equiv(u)).\alpha_\equiv(\pi_\equiv(u)) = s_\equiv(\pi_\equiv(v))\alpha_\equiv(\pi_\equiv(v)) = \pi_\equiv(v).$$

Soit $(u, v) \in {A^*}/_\equiv$ un couple tel que $u \equiv_2 v$ et $u - v$ primitif. Alors

$$v - u = \alpha_\equiv(u - v) = s_\equiv(u)u - s_\equiv(v)v.$$

On a deux possibilités: $u = u$ et $v = v$ ou bien $u = v$ et $v = u$. Dans les deux cas les relations $u \equiv_2 v$ et $u \equiv_2 v$ sont vraies, ce qui prouve que si $w \equiv_2 w'$ alors $w \equiv_2 w'$ pour tout couple $(w, w') \in ({A^*}/_\equiv)^2$. On peut donc étendre la notion d'image miroir au monoïde ${A^*}/_{\equiv\vee\equiv_2}$.
De la même façon, si $u = u$ et $v = v$ alors $s_\equiv(u) = s_\equiv(v) = -1$ et si $v = u$ et $u = v$ on a $s_\equiv(u) = s_\equiv(v) = 1$. L'application $s_\equiv$ est donc constante sur les classes d'équivalence de $\equiv_2$. Ceci prouve la partie (4) de la définition.
Maintenant, considérons un couple de mots $w \equiv_2 w'$ alors

$$\alpha_\equiv(w) = s_\equiv(w)w \equiv_2 s_\equiv(w')w' = \alpha_\equiv(w').$$

Donc, il existe une application linéaire $\alpha_{\equiv_2}$ telle que $\alpha_{\equiv_2} \circ \pi_{\equiv_2} = \pi_{\equiv_2} \circ \alpha_\equiv$ où $\pi_{\equiv_2}$ est la surjection canonique de $K[{A^*}/_\equiv]$ sur $K[{A^*}/_{\equiv\vee\equiv_2}]$ (ceci prouve aussi la partie (2) de la définition).
Soit $\tilde{c} : K\langle A\rangle \to K\langle A\rangle \otimes K\langle A\rangle$ le morphisme défini par

$$\tilde{c} = (Id \otimes \alpha) \circ c.$$

Par composition, on montre qu'il existe deux morphismes $\tilde{c}_{\equiv_1}$ et $\tilde{c}_{\equiv_2}$ tels que

$$(\pi_{\equiv_1} \otimes \pi_{\equiv_1}) \circ \tilde{c} = \tilde{c}_{\equiv_1} \circ \pi_{\equiv_1}$$

et

$$(\pi_{\equiv_2} \otimes \pi_{\equiv_2}) \circ \tilde{c}_{\equiv_1} = \tilde{c}_{\equiv_2} \circ \pi_{\equiv_2}.$$

On définit l'application linéaire $m : K\langle A\rangle \otimes K\langle A\rangle \to K\langle A\rangle$ par $m(P \otimes Q) = PQ$. On vérifie facilement que si $P \otimes Q \equiv P' \otimes Q'$ alors

$$m(P \otimes Q) = PQ \equiv P'Q' = m(P \otimes Q).$$

Ce qui permet de construire une application linéaire $m_{\equiv_1}$ vérifiant $\pi_{\equiv_1} \circ m = m_{\equiv_1} \circ \pi_{\equiv_1}$. De la même façon, on construit $m_{\equiv_2}$ telle que $\pi_{\equiv_2} \circ m_{\equiv_1} = m_{\equiv_2} \circ \pi_{\equiv_2}$. On a besoin du lemme suivant (montré dans [**?**]).

Lemme 98

$$m \circ \tilde{c}(P) = (P, 1)$$

En utilisant le lemme **??**, on trouve que $m_{\equiv_1} \circ \tilde{c}_{\equiv_1}(P) \in K$ pour tout $P \in K[A^*/_{\equiv_1}]$ et $m_{\equiv_2} \circ \tilde{c}_{\equiv_2}(P) \in K$ pour tout $P \in K[A^*/_{\equiv_1}/_{\equiv_2}]$.
Soit $(u, v) \in (A^*/_{\equiv_1}/_{\equiv_2})^2$ tel que $u - v$ primitif, alors on a

$$m_{\equiv_2} \circ \tilde{c}_{\equiv_2}(u - v) = u - v + \alpha_{\equiv_2}(u - v) \in K.$$

Ceci prouve que

$$m_{\equiv_2} \circ \tilde{c}_{\equiv_2}(u - v) = 0 \text{ et } \alpha_{\equiv_2}(u - v) = v - u.$$

Donc (3) est vérifié et le lemme est prouvé.

$a \quad K < A >$ $\qquad eK[A^*/_{\equiv_1}]$ $\qquad i \quad K[A^*/_{\equiv_1 \vee \equiv_2}]$

$bK < A > \otimes K < A >$ $\quad fK[A^*/_{\equiv_1}] \otimes K[A^*/_{\equiv_1}]$ $\quad jK[A^*/_{\equiv_1 \vee \equiv_2}] \otimes K[A^*/_{\equiv_1 \vee \equiv_2}]$

$$- > abc - > bcId \otimes \alpha$$

$cK < A > \otimes K < A >$ $\quad gK[A^*/_{\equiv_1}] \otimes K[A^*/_{\equiv_1}]$ $\quad kK[A^*/_{\equiv_1 \vee \equiv_2}] \otimes K[A^*/_{\equiv_1 \vee \equiv_2}]$

$dK < A >$ $\qquad hK[A^*/_{\equiv_1}]$ $\qquad lK[A^*/_{\equiv_1 \vee \equiv_2}]$

Remarque 47 *Si $\equiv$ est $K-$ compatible, un argument simple de minimalité montre que la classe de 1 est réduite à $\{1\}$ ainsi $\epsilon : P \to (P, 1)$ est constante sur les classes de $\equiv$.*

Théorème 99 *Toute congruence $K-$ compatible finiment engendrée est K-compatible avec l'antipode.*

Preuve D'après la proposition **??**, une telle congruence admet un développement primitif fini. En appliquant à chaque étape le lemme **??** on trouve le résultat.

Remarque 48 *L'algèbre $K[A^*/_\equiv]$ munie du coproduit $c_\equiv$ et de la coünité $\epsilon : P \to (P, 1)$ forme une bigèbre*[6]*. La preuve du lemme* **??** *montre que si $c_\equiv(w) = \sum_{i\in I} w_i \otimes w'_i$ alors*

$$\sum_i \alpha(w_i)w'_i = m_\equiv \circ (\alpha_\equiv \otimes Id) \circ c_\equiv(w) = \epsilon(w).$$

De façon symétrique

$$\sum_i w_i\epsilon(w'_i) = \epsilon(w).$$

Ceci prouve que $K[A^*/_\equiv]$ peut être munie d'une structure d'algèbre de Hopf d'antipode α.

La preuve du lemme **??** donne le résultat suivant qui nous sera utile dans la suite.

Corollaire 100 *Soit $\equiv$ une congruence $K-$ compatible, et soit $u, v \in A^*/_\equiv$ tels que $u - v$ est primitif. Alors une des conditions suivantes est satisfaite.*

1. *$u = u$, $v = v$ et $s_\equiv(u) = s_\equiv(v) = -1$.*

2. *$u = v$ et $s_\equiv(u) = s_\equiv(v) = 1$*

[6]Puisque, d'après la remarque **??**, l'application ϵ est stable sur les classes de $\equiv$, on peut définir une application $\epsilon_\equiv$ telle que $\epsilon_\equiv \circ \pi_\equiv = \pi_\equiv \circ \epsilon$. Le fait que $w \equiv 1$ si et seulement si $w = 1$, implique que $\epsilon_\equiv$ est bien une coünité.

4.6.3 Anneaux de caractéristique première

Le but de ce numéro est de montrer que, en caractéristique première p, la première étape d'un découpage primitif minimal est engendrée par des commutations (pLC) et les identifications (pLI) de p-puissances et que, de plus, cette première étape absorbe les commutations et identifications de puissances quelconques.
En vertu du lemme **??** 2, il suffit de traiter le cas où $K = /p$. Pour cela, nous avons besoin de quelques lemmes préparatoires sur les structures partiellement commutatives. On considérera d'abord le monoïde partiellement commutatif libre (A, θ). Pour chaque trace, on définit le mot standard de t, $std(t) \in A^*$, comme le mot w le plus grand lexicographiquement tel que $\pi_\theta(w) = t$, où π_θ est la surjection canonique $A^* \to (A, \theta)$. Grâce à cette notion on peut définir un ordre total sur (A, θ) par

$$t <_{std} t' \Leftrightarrow std(t) <_{lex} std(t').$$

Nous nous intéresserons, particulièrement, à une catégorie de traces définie par Lalonde et Krob dans [**?**]: les traces de Lyndon. Pour toute trace de Lyndon $l \notin A$, sa factorisation standard est le couple $\sigma(l) = (l_1, l_2) \in Ly(A, \theta)^2$ tel que $l = l_1 l_2$, $|l_2|$ maximal.
De telles traces vérifient la propriété suivante.

Lemme 101 *Soit l une trace de Lyndon alors*

1. *Le mot $std(l)$ est un mot de Lyndon*

2. *Pour tout $\alpha \geq 0$, on a $std(l^\alpha) = (std(l))^\alpha$*

Preuve La première assertion est montrée dans [**?**].
Montrons donc l'assertion (2). Supposons que $std(l^\alpha) >_{lex} (std(l))^\alpha$. Alors il existe un entier $k \geq 0$, un préfixe p de l, un suffixe s de l, un mot w et deux lettres $x < y$ tels que $std(l^\alpha) = std(l)^k.pxs.std(l)^{\alpha-k-1}$ et $(std(l))^\alpha = std(l)^k pyw$. On ne peut avoir $\alpha = k + 1$, sans quoi $\pi_\theta(pyw) = l$ et $std(l) = pxs < pyw$. Donc, $\alpha - k - 1 > 1$. Ceci implique pour la même raison que $y \in (l^\alpha) = (l)$. Donc y minore l) et donc x. Il y a contradiction avec nos hypothèses.
Lalonde a montré dans sa thèse [**?**] le résultat suivant.

Théorème*(de Lalonde) Soit* $\Lambda : Ly(A,\theta) \to L_K(A,\theta)$ *l'application définie récursivement par*

$$\begin{cases} \Lambda(a) = a & si\ a \in A \\ \Lambda(l) = [\Lambda(l_1), \Lambda(l_2)] & avec\ \sigma(l) = (l_1, l_2)\ si\ l \notin A. \end{cases}$$

Alors $(\Lambda(l))_{l \in Ly(A,\theta)}$ *forme une base de* $L_K(A,\theta)$ *en tant que* K*-module et de plus pour tout* $l \in Ly(A,\theta)$ *on a*

$$\Lambda(l) = l + \sum_{t >_{std} l} \beta_t t.$$

On peut en déduire le corollaire suivant.

Corollaire 102 *Soit* l *une trace de Lyndon et* $\alpha \in$ *alors*

$$(\Lambda(l))^\alpha = l^\alpha + \sum_{t >_{std} l^\alpha} \beta_t t.$$

Preuve Il suffit d'appliquer le théorème Lalonde et de remarquer que

$$(\Lambda(l))^\alpha = \left(l^\alpha + \sum_{t >_{std} l} \beta_t t \right)^\alpha = l^\alpha + \sum_{\substack{t >_{std} l^k \\ 0<k<\alpha}} \beta_{t,w,k} l^k t w + \sum_{t >_{std} l} \gamma_{t,w} t w.$$

Le lemme **??** nous permet alors de conclure car l'examen des monômes donne

$$\begin{array}{llll} std(l^\alpha) & = (std(l))^\alpha & < std(l^k)std(tw) & \leq std(t^k tw) \\ std(l^\alpha) & = (std(l))^\alpha & < std(t)std(w) & \leq std(tw). \end{array}$$

Exemple 49 *Considérons le graphe de commutation*

$$(A,\theta) : a - b - c - d.$$

La trace adc *est une trace de Lyndon et on a*

$$\begin{array}{rcl} [[a,d],c]^2 & = & adcadc - adc^2ad - ad^2ac - ad^2c^2 \\ & & -cadadc + cadcad + cad^2c - cad^2ca \\ & & -dacacd + dac^2ad + dacdac - dadc^2a \\ & & +dca^2cd - dcacad - dcadac + dcadca. \end{array}$$

On a besoin des lemmes suivants.

Lemme 103 *Soit $t = l^\alpha \in (A, \theta)$ une puissance non nulle d'une trace de Lyndon. Supposons que t ne puisse pas s'écrire sous la forme $t = a^\alpha$ ou $t = a^\alpha b^\beta$ avec $a, b \in A$. Alors il existe deux sous traces complémentaires u et v de t telles que pour tout semi anneau K on a:*

$$(c(t), u \otimes v) = 1 \text{ et } (c(t), u \otimes v) = 0$$

Preuve D'après le lemme **??**, il suffit de montrer le résultat pour $K =$. Comme t est une puissance d'une trace de Lyndon et est différente de a^α et $a^\alpha b^\beta$, elle peut s'écrire sous la forme

$$t = awb^\alpha c^\beta$$

avec $a, b, c \in A$, $w \in A^*$, $\alpha, \beta > 0$, $\alpha + \beta$ maximum, $c \neq b$, $a \neq c$ (puisque l est de Lyndon). Cela implique $b \notin AT(aw)$ et $c \notin (awb^\alpha)$.

Nous allons montrer que la propriété est vraie avec le choix $u = awc^\beta$ et $v = b^\alpha$.
Montrons d'abord que $(c(t), u \otimes v) = 1$.

1. Si $(b, c) \in \theta$ alors $t = awc^\beta b^\alpha$ avec α maximal et, de la même façon que dans le lemme **??**, on montre que

   $$(c(t), u \otimes v) = 1.$$

2. Si $(b, c) \notin \theta$, supposons que $(c(t), u \otimes v) > 1$. Alors on peut écrire w sous la forme

   $$w = b^{\alpha_1} w_1 b^{\alpha_2} w_2 \dots b^{\alpha_n} w_n$$

   avec $0 < \alpha' = \alpha_1 + \dots + \alpha_n < \alpha$ et $aw_1 \dots w_n b^{\alpha - \alpha'} c^\beta = u$.
   Or $t = awb^\alpha c^\beta$, $(b, c) \notin \theta$ et $b \notin AT(w_n)$, ce qui implique $\alpha' = 0$. Il y a donc une contradiction.

D'où $(c(t), u \otimes v) = 1$ et donc pour tout semi-anneau K on a $(c(t), u \otimes v) = 1$.
Montrons maintenant que $(c(t), u \otimes v) = 0$. Supposons que $(c(t), u \otimes v) \geq 1$. Alors il existe un suffixe s de longueur minimale de t contenant u. On peut écrire $ps = t$ ($p = b^\gamma$). Considérons deux cas.

1. Si $(c, b) \notin \theta$, puisque $|s|_c = |t|_c$ on a $p = 1$. En ce cas, $a \in (s)$ car $a \in (u)$ et donc $a \in (t)$, ce qui est impossible par hypothèse.

2. Si $(c,b) \in \theta$, dans ce cas on a $a \neq b$ (car pour un mot de Lyndon $l \notin A$, $(l) \cap (l) = \emptyset$) ainsi que l'égalité

$$ps = (b^\alpha c^\beta)(wa).$$

Le lemme de Levi nous donne l'existence de quatre traces p', s', r, q telles que $(s', r) \in \theta$, $p = p's'$, $s = rq$, $b^\alpha c^\beta = p'r$ et $wa = s'q$. Le fait que t soit une puissance d'une trace de Lyndon et que $(c,b) \in \theta$ implique que $AI(u) = \{a\} \neq \{b\}$. La minimalité de s donne $AI(s) = \{a\}$. Si $r \neq 1$, on a $a \in Alph(r) \subseteq \{c,b\}$ ce qui est impossible. Donc $r = 1$, ce qui implique $bwa = s's$. Or $|s|_b \geq |bwa|_b$ d'où $|s'|_b = 0$ mais comme $s') = \{b\}$, $s' = 1$. Donc $p = p' = b^\alpha c^\beta$, mais $p) = \{b\}$ prouve la contradiction.

Nous utilisons ici un lemme très général dont la preuve est reportée en annexe.

Lemme 104 *Soit p un nombre premier et $(b_i)_{i\in I}$ une base de $L_{/p}(A,\theta)$. Alors l'algèbre de Lie des élèments primitifs de $/p < A,\theta >$ a pour base $(b_i^{p^e})_{\substack{i\in I \\ e\geq 0}}$.*

Exemple 50 *Posons $K = /3[i]$ et*

$$(A,\theta) = a - b - c - d.$$

Alors le polynôme de Lie $P = i[a,[b,d]]^3 + 2 * [c,[a,d]]$ est primitif. En effet,

$$\begin{aligned} c(P) &= i * c([a,[b,d]])^3 + 2 * c([c,[a,d]]) \\ &= i[a,[b,d]]^3 \otimes 1 + 3i[a,[b,d]] \otimes [a,[b,d]] + 3i[a,[b,d]]^2 \otimes [a,[b,d]] \\ &\quad + i * 1 \otimes [a,[b,d]]^3 + 2[c,[a,d]] \otimes 1 + 2 * 1 \otimes [c,[a,d]]. \\ &= P \otimes 1 + 1 \otimes P \end{aligned}$$

Lemme 105 *Les seules traces de $/p < A,\theta >$ (avec p premier) qui sont des éléments primitifs sont les puissances p^α de lettres.*

Preuve En utilisant le lemme **??**, le théorème Lalonde et le corollaire **??** on a

$$u = \sum_{\substack{l\in Ly(A,\theta) \\ \alpha\in}} \beta_{\alpha,l}(\Lambda(l))^{p^\alpha} = \sum_{\substack{l\in Ly(A,\theta) \\ \alpha\in}} \beta_{\alpha,l} \left(l^{p^\alpha} + \sum_{t>_{std} l^{p^\alpha}} \gamma_{t,l,\alpha} t \right).$$

Si on pose $l^{p^\alpha} = inf_{std}\{l_1^{p^{\alpha_1}} \in Ly(A,\theta) | \beta_{\alpha_1,l_1} \neq 0\}$, on a nécessairement $u = l^{p^\alpha}$. Or si $l \notin A$, on peut écrire $l^{p^\alpha} = ta^n$ avec n maximal, $a \in A$ et $t \neq 1$. Dans ce cas $(c(l^{p^\alpha}), t \otimes a^n) = 1$, ce qui est impossible et prouve le résultat.
On aura par la suite besoin de quelques résultats arithmétiques.
On définit pour tout $n \in$ l'entier

$$\xi_p(n) = \sum_{j=0}^{k} q_j \frac{p^j - 1}{p - 1}$$

où $n = \sum_{j=0}^{k} q^j.p^j$ est l'écriture en base p de n.

Lemme 106 *Soit p un nombre premier.*

1. *Soit $n > 0$ un entier alors*

$$n! = p^{\xi_p(n)}.r_n$$

où $r_n \not\equiv 0 \quad [p]$.

2. *Soit $n \in^* $ tel que $\binom{n}{i} \equiv 0 \quad [p]$ pour tout $i \in [1, n-1]$. Alors n est une puissance entière de p.*

3. *Pour tout $\alpha \geq 1$ on a*

$$\binom{p^\alpha}{p^{\alpha-1}} = pr$$

lorsque $r \not\equiv 0 \quad [p]$.

Preuve Calcul simple à partir du théorème de Legendre

$$\xi_p(n) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots + \lfloor \frac{n}{p^i} \rfloor + \cdots$$

d'où on déduit les points 2 et 3.
Le résulat suivant nous sera utile pour caractériser les congruences $/p-$ compatibles $\equiv$ telles que $\gamma_{/p}(\equiv) = 1$.

Proposition 107 *Soit $u - v$ un polynôme primitif de $/p < A, \theta >$ tel que $u, v \in (A, \theta)$. Alors $u = a^{p^\alpha}$ et $v = b^{p^\beta}$ ou $u = a^{p^\alpha} b^{p^\beta}$ et $v = b^{p^\beta} a^{p^\alpha}$.*

Preuve Soit $u - v$ un tel polynôme. Sans perte de généralité, quitte à multiplier par -1, on peut supposer $u <_{std} v$. Alors, d'après le lemme **??**, $u - v \in L^{(p)}_{/p}(A, \theta)$ qui admet comme base (en tant que $/p$-module) les p^n puissances des polynômes de Lyndon. On peut donc écrire

$$u - v = \sum_{\substack{l \in Ly(A,\theta) \\ n \in}} \alpha_{l,n} (\Lambda(l))^{p^n} = \sum_{\substack{l \in Ly(A,\theta) \\ n \in}} \alpha_{l,n} \left(l^{p^n} + \sum_{t >_{std} l^{p^n}} \gamma_{l,n,t} t \right).$$

Soit $l^{p^n} = \min_{std}\{l'^{p^m} / \alpha_{l',m} \neq 0\}$. Nécessairement $l^{p^n} = u$. Le corollaire **??** implique que si $u - v$ est primitif alors $u = u$ et $v = v$ ou $u = v$. Si $u = u$, comme l est une trace de Lyndon, $l = l$ implique $l = a$ (en effet si $l \in Ly(A, \theta) - A$ alors $(l) \cap AT(l) = \emptyset$) et donc v est primitif. Le lemme **??** implique alors $v = b^{p^\beta}$ et prouve le résultat. Si $u = v$ alors $u - v = l^{p^n} - l^{p^n}$. Le lemme **??** implique que si $l^{p^n} \neq a^\alpha$ et $l^{p^n} \neq a^\alpha b^\beta$ alors $u - v$ n'est pas primitif. Si $l = a$ alors $u - v = 0$. Supposons donc que $n = 0$ et $l = a^\alpha b^\beta$. On a alors

$$\begin{aligned} c(u - v) &= c(a^\alpha b^\beta - b^\beta a^\alpha) \\ &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \binom{\alpha}{i} \binom{\beta}{j} a^{\alpha - i} b^{\beta - j} \otimes a^i b^j - \\ &\quad \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \binom{\alpha}{i} \binom{\beta}{j} b^{\beta - j} a^{\alpha - i} \otimes b^j a^i \end{aligned}$$

et

$$c(u - v) = (a^\alpha b^\beta - b^\beta a^\alpha) \otimes 1 + 1 \otimes (a^\alpha b^\beta - b^\beta a^\alpha).$$

Ceci implique que pour tout $i \in \{1, \ldots, \alpha - 1\}$ et pour tout $j \in \{1, \ldots, \beta - 1\}$ on a $\binom{\alpha}{i} \equiv \binom{\beta}{j} \equiv 0 \quad [p]$. Le lemme **??** permet de conclure.

Théorème 108 *Soient p un nombre premier et $\equiv$ une congruence $/p-$ compatible. Alors $\gamma_{/p}(\equiv) = 1$ si et seulement si $\equiv$ est engendrée par des couples de la forme $(a^{p^\alpha}, b^{p^\beta})$ ou $(a^{p^\alpha} b^{p^\beta}, b^{p^\beta} a^{p^\alpha})$.*

Preuve C'est une conséquence directe de la proposition **??** et du lemme **??**.

Nous montrons que les relateurs de commutation et d'identification d'exponentielles (c'est à dire de la forme $a^\alpha \equiv b^\beta$ et $a^\alpha b^\beta \equiv b^\beta a^\alpha$) sont absorbés dans la profondeur 1.

Théorème 109 *Soit $\equiv$ une congruence /p− compatible alors*

1. *La congruence $\equiv_c$ engendrée par les commutations $a^\alpha b^\beta \equiv b^\beta a^\alpha$ l'est par des commutations de la forme $a^{p^\alpha} \equiv b^{p^\beta} = b^{p^\beta} a^{p^\alpha}$ (pLC).*

2. *La congruence $\equiv_l$ engendrée par les identifications $a^\alpha \equiv b^\beta$ l'est par des identifications de la forme $a^{p^\alpha} \equiv b^{p^\beta}$(pLI).*

Preuve (1) On notera $\equiv_{pLC}$ la congruence engendrée par les paires $(a^{p^{k_1}} b^{p^{k_2}}, b^{p^{k_2}} a^{p^{k_1}})$ telles que $a^{p^{k_1}} b^{p^{k_2}} \equiv b^{p^{k_2}} a^{p^{k_1}}$. Il suffit de prouver que si $a^\alpha b^\beta \equiv_c b^\beta a^\alpha$ on a nécessairement $a^\alpha b^\beta \equiv_{pLC} b^\beta a^\alpha$. Supposons qu'il existe des paires $a^\alpha b^\beta \equiv_c b^\alpha a^\beta$ et $a^\alpha b^\beta \not\equiv_{pLC} b^\beta a^\alpha$. Considérons une telle paire avec $\alpha + \beta$ minimal. Alors la K- compatibilité de $\equiv$ donne

$$\sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \binom{\alpha}{i} \binom{\beta}{j} a^{\alpha-i} b^{\beta-j} \otimes a^i b^j \equiv_c^{\otimes 2} \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \binom{\alpha}{i} \binom{\beta}{j} b^{\beta-j} a^{\alpha-i} \otimes b^j a^i.$$

Comme $\equiv_c$ est multihomogène, la minimalité de $\alpha + \beta$ implique

$$\binom{\alpha}{i} \binom{\beta}{j} \equiv 0 \quad [p]$$

pour toute paire

$$(i, j) \notin \{(0, 0), (\alpha, 0), (0, \beta), (\alpha, \beta)\}.$$

Alors en posant $j = 0$, on obtient $\binom{\alpha}{i} \equiv 0 \quad [p]$ pour tout $i \in \{1, \ldots, \alpha - 1\}$ et de façon similaire $\binom{\beta}{j} \equiv 0 \quad [p]$ pour tout $j \in \{1, \ldots, \beta - 1\}$. Le lemme **??** entraîne la conclusion.

Pour le point suivant nous avons besoin du résultat ci-dessous.

Théorème *(Cauchy-Lucas-1830[?]) Soit p un nombre premier. Soit $\alpha = \sum_{m \leq i \leq M} \alpha_i p^i$ le développement de α dans la base p. Considérons un entier $\gamma = \sum_{m \leq i \leq M} \gamma_i p^i$ tel que pour tout $i \in \{m, \ldots, M\}$, $\gamma_i \leq \alpha_i$. Alors*

$$\binom{\alpha}{\gamma} \equiv \prod_{m \leq i \leq M} \binom{\alpha_i}{\gamma_i} [p]$$

Suite de la preuve du théorème ?? (2) Le fait que $\equiv_l$ soit $/p-$ compatible provient du fait que la compatibilité est stable par restriction aux sous-alphabets (cf. lemme **??**.3). On aura besoin du lemme suivant.

Lemme 110 *Toute congruence $K-$ compatible $\equiv$ sépare A^+ et 1 (autrement dit $w \equiv 1 \Rightarrow w = 1$).*

Preuve Supposons que cela ne soit pas le cas. Soit $w \in A^+$ tel que $w \equiv 1$ de longueur minimale. Comme $w \neq 1$, on a

$$\sum_{\substack{I+J=[1,|w|]\\ I,J\neq\emptyset}} w_I \otimes w_J \equiv^{\otimes 2} -1 \otimes 1.$$

Ceci contredit la minimalité de w.
Fin de la preuve du théorème ?? Le lemme **??** montre que $\equiv$ sépare nécessairement A^+ et 1. Nous nous intéresserons donc uniquement aux couples (a^α, b^β) avec $\alpha, \beta \neq 0$.
On notera $\equiv_{pLI}$ la congruence engendrée par les paires $(a^{p^{k_1}}, b^{p^{k_2}})$ avec $a^{p^{k_1}} \equiv_l b^{p^{k_2}}$. Supposons que l'ensemble

$$P = \{(a^\alpha, b^\beta) | a^\alpha \equiv_l b^\beta \text{ et } a^\alpha \not\equiv_{pLI} b^\beta\}$$

ne soit pas vide et considérons $(a^\alpha, b^\beta) \in P$ tel que $(\max\{\alpha, \beta\}, \alpha + \beta)$ soit minimal pour l'ordre lexicographique sur ^{2}. Sans restriction de généralité, on peut supposer $\alpha \leq \beta$. Nécessairement α ou β n'est pas une puissance de p.
Supposons que α ne soit pas une puissance de p. Le théorème de Cauchy implique qu'il existe α_1 $(0 < \alpha < \alpha_1)$ tel que

$$(c(a^\alpha), a^{\alpha_1} \otimes a^{\alpha-\alpha_1}) \not\equiv 0 \quad [p].$$

Si $a^{\alpha_1} \otimes a^{\alpha-\alpha_1}$ ne figure pas dans le support de $c_\equiv(a^\alpha)$ c'est qu'il existe α_2 $(0 < \alpha_1 < \alpha,\ \alpha_1 \neq \alpha_2)$ tel que $a^{\alpha_1} \otimes a^{\alpha-\alpha_1} \equiv_l^{\otimes 2} a^{\alpha_2} \otimes a^{\alpha-\alpha_2}$. Supposons que $\alpha_1 < \alpha_2$ (l'autre cas étant similaire). On a alors $a^{\alpha-\alpha_2+\alpha_1} \equiv_l a^\alpha$, or

$$\max\{\alpha, \alpha - \alpha_2 + \alpha_1\} \leq \max\{\alpha, \beta\} \text{ et } 2\alpha - \alpha_2 + \alpha_1 < \alpha + \beta$$

donc les hypothèses de minimalité donnent $a^{\alpha-\alpha_2+\alpha_1} \equiv_{pLI} a^\alpha$. Ceci implique $a^{\alpha-\alpha_2+\alpha_1} \equiv_l b^\beta$. De plus

$$\max\{\alpha - \alpha_2 + \alpha_1, \beta\} = \beta = \max\{\alpha, \beta\} \text{ et } \alpha - \alpha_2 + \alpha_1 + \beta < \alpha + \beta.$$

En utilisant les hypothèses de minimalité on trouve $a^{\alpha-\alpha_2+\alpha_1} \equiv_{pLI} b^{\beta}$, ce qui contredit nos hypothèses.
Donc $a^{\alpha_1} \otimes a^{\alpha-\alpha_1}$ ne figure pas dans le support de $c_{\equiv}(a^{\alpha})$. Alors il existe β_1 $(0 < \beta_1 < \beta)$ tel que

$$a^{\alpha_1} \otimes a^{\alpha-\alpha_1} \equiv^{\otimes 2} b^{\beta_1} \otimes b^{\beta-\beta_1}.$$

Or

$$\max\{\alpha_1, \beta_1\}, \max\{\alpha-\alpha_1, \beta-\beta_1\} < \max\{\alpha, \beta\}.$$

La minimalité montre alors que

$$a^{\alpha} = a^{\alpha_1} a^{\alpha-\alpha_1} \equiv_{pLI} b^{\beta_1} b^{\beta-\beta_1} = b^{\beta},$$

ce qui contredit nos hypothèses.
Donc $\alpha = p^k$ et β n'est pas une puissance de p. Alors le théorème de Cauchy implique qu'il existe β_1, β_2 $(0 < \beta_1 < \beta_2 < \beta)$, tel que $b^{\beta_1} \otimes b^{\beta-\beta_1} \equiv^{\otimes 2} b^{\beta_2} \otimes b^{\beta-\beta_2}$. Comme $\max\{\beta_1, \beta_2\} < \max\{\alpha, \beta\}$, on a $b^{\beta_1} \equiv_{pLI} b^{\beta_2}$ et donc $b^{\beta} \equiv_{pLI} b^{\beta-\beta_2+\beta_1}$. Ceci implique $a^{\alpha} \equiv_l b^{\beta}$, $\max\{\alpha, \beta-\beta_2+\beta_1\} \leq \max\{\alpha, \beta\}$ et $\alpha+\beta-\beta_2+\beta_1 < \alpha+\beta$. Les hypothèses de minimalité donnent $a^{\alpha} \equiv_{pLI} b^{\beta-\beta_2+\beta_1}$ et $a^{\alpha} \equiv_{pLI} b^{\beta}$ contredisant l'appartenance de (a^{α}, b^{β}) à P. Ceci entraîne la conclusion.

La proposition suivante montre qu'il existe une famille infinie $(\equiv_i)_{i\in I}$ de congruences $/2-$ compatibles de profondeur 2 et telle que pour tout couple $(i,j) \in I^2$, $i \neq j$ on a $\equiv_i \not\subset \equiv_j$ et $\equiv_j \not\subset \equiv_i$.

Proposition 111 *Soient n et m deux entiers alors la congruence engendrée par*

$$R = \begin{cases} a^{2^n} b^{2^m} a^{2^n} b^{2^m} = b^{2^m} a^{2^n} b^{2^m} a^{2^n}, \\ a^{2^{n+1}} b^{2^m} = b^{2^m} a^{2^{n+1}}, \\ b^{2^{m+1}} a^{2^n} = a^{2^n} b^{2^{m+1}}. \end{cases}$$

est $/2-$ compatible.

Preuve On a l'égalité

$$c(a^{2^n} b^{2^m} a^{2^n} b^{2^m}) = \sum_{i,j,k,l} \binom{2^n}{i} \binom{2^m}{j} \binom{2^n}{k} \binom{2^m}{l} a^{2^n-i} b^{2^m-j} a^{2^n-k} a^{2^m-l} \otimes a^i b^j a^k b^l.$$

Donc

$$c(a^{2^n}b^{2^m}a^{2^n}b^{2^m}) = \sum_{(i,j,k,l)\in\{0,1\}^4} a^{2^n i}b^{2^m j}a^{2^n k}b^{2^m l}\otimes a^{2^n(1-i)}b^{2^m(1-j)}a^{2^n(1-k)}b^{2^m(1-l)}.$$

De même

$$c(b^{2^m}a^{2^n}b^{2^m}a^{2^n}) = \sum_{(i,j,k,l)\in\{0,1\}^4} b^{2^m j}a^{2^n k}b^{2^m l}a^{2^n i}\otimes b^{2^m(1-j)}a^{2^n(1-k)}b^{2^m(1-l)}a^{2^n(1-i)}.$$

$$\begin{aligned} P &= c(a^{2^n}b^{2^m}a^{2^n}b^{2^m}) + c(b^{2^m}a^{2^n}b^{2^m}a^{2^n}) \\ &= a^{2^n}b^{2^m}a^{2^n}b^{2^m}\otimes 1 + a^{2^{n+1}}b^{2^m}\otimes b^{2^m} + a^{2^n}b^{2^{m+1}}\otimes a^{2^n} \\ &\quad + b^{2^m}\otimes a^{2^{n+1}}b^{2^m} + a^{2^n}\otimes a^{2^n}b^{2^{m+1}} + 1\otimes a^{2^n}b^{2^m}a^{2^n}b^{2^m} \\ &\quad + b^{2^m}a^{2^n}b^{2^m}a^{2^n}\otimes 1 + b^{2^m}a^{2^{n+1}}\otimes b^{2^m} + b^{2^{m+1}}a^{2^n}\otimes a^{2^n} \\ &\quad + b^{2^m}\otimes b^{2^m}a^{2^{n+1}} + a^{2^n}\otimes b^{2^{m+1}}a^{2^n} + 1\otimes b^{2^m}a^{2^n}b^{2^m}a^{2^n} \end{aligned}$$

Soit $\equiv_1$ la congruence engendrée par $(a^{2^{n+1}}b^{2^n}, b^{2^n}a^{2^{n+1}})$ et $(a^{2^n}b^{2^{n+1}}, b^{2^{n+1}}a^{2^n})$. Alors

$$P \equiv_1^{\otimes 2} (a^{2^n}b^{2^m}a^{2^n}b^{2^m} + b^{2^m}a^{2^n}b^{2^m}a^{2^n})\otimes 1 + 1\otimes(a^{2^n}b^{2^m}a^{2^n}b^{2^m} + b^{2^m}a^{2^n}b^{2^m}a^{2^n}).$$

Ceci prouve que $a^{2^n}b^{2^m}a^{2^n}b^{2^m} + b^{2^m}a^{2^n}b^{2^m}a^{2^n}$ est un polynôme primitif de $/2[A^*/_{\equiv_1}]$. Donc R est $/2-$ compatible.

4.6.4 Anneaux de caractéristique non première

Ce numéro est consacré à montrer que le cas de la caractéristique non première se comporte comme celui de la caractéristique 0.

Lemme 112 *Soient K_1 et K_2 deux anneaux et $\equiv$ une congruence K_1- compatible et K_2- compatible. Si il existe un morphisme $K_1 \to K_2$, alors tout polynôme primitif dans $K_1[A^*/_{\equiv}]$ est primitif dans $K_2[A^*/_{\equiv}]$.*

Preuve Évident, car $.1_{K_1} \to .1_{K_2}$ est surjectif.

Théorème 113 *Soit $n > 0$ un entier non premier. Toute congruence $/n-$ compatible est engendrée par des relateurs de la forme (a, b) ou (ab, ba) avec $a, b \in A$ ((IL) et (CL)).*

Preuve On doit ici différencier deux cas:

1. Si $n \neq p^\alpha$ avec p premier, alors on peut écrire $n = p_1 p_2 m$ avec $p_1, p_2, m \in$ et $p_1 \neq p_2$ premier. Il existe donc deux morphismes $\phi_1 : /n \to /p_1$ et $\phi_2 : /n \to /p_2$, ce qui implique, d'après le lemme **??**, que les polynômes primitifs dans $/n < A >$ sont primitifs dans $/p_1 < A >$ et $/p_2 < A >$. Donc d'après le lemme **??**, si $u - v$ est primitif dans $/n < A >$, alors

$$u = a^{p_1^{\alpha_1}} = a^{p_2^{\alpha_2}} \text{ et } v = b^{p_1^{\beta_1}} = b^{p_2^{\beta_2}}$$

ou

$$u = a^{p_1^{\alpha_1}} b^{p_1^{\beta_1}} = a^{p_2^{\alpha_2}} b^{p_2^{\beta_2}} \text{ et } v = b^{p_1^{\beta_1}} a^{p_1^{\alpha_1}} = b^{p_2^{\beta_2}} a^{p_2^{\alpha_2}}.$$

Comme p_1 et p_2 sont premiers ceci implique $\alpha_1 = \alpha_2 = \beta_1 = \beta_2 = 0$. On vient donc de prouver que $\gamma_{/n}(\equiv) = 1$ si et seulement si $\equiv$ est engendrée par des relateurs de la forme (a, b) ou (ab, ba) avec $a, b \in A$. Montrons maintenant que $\gamma_{/n}(\equiv) = 1$ pour toute congruence $/n-$ compatible. Il suffit, en fait, de prouver que les seuls polynômes primitifs dans $/n < A, \theta >$ de la forme $u - v$ avec $u, v \in (A, \theta)$ sont $a - b$ et $ab - ba$ avec $a, b \in A$. Cela se fait en appliquant à nouveau le raisonnement précédent mais dans le cadre des commutations partielles.

2. Si $n = p^m$ avec $m > 1$. Alors il existe deux morphismes

$$/p^m \to /p^2 \to /p.$$

Le lemme **??** montre qu'il suffit de prouver la proposition dans le cas où $m = 2$. Plus précisément, on s'intéressera tout d'abord aux polynômes de $/p^2 < A >$ qui sont de la forme $a^{p^\alpha} - b^{p^\beta}$ ou $a^{p^\alpha} b^{p^\beta} - b^{p^\beta} a^{p^\alpha}$ qui d'après la proposition **??** et le lemme **??** sont les seuls candidats possibles à la primitivité dans $/p^2 < A >$.
Montrons tout d'abord que $a^{p^\alpha} - b^{p^\beta}$ est primitif si et seulement si $\alpha = \beta = 0$. Examinons deux cas

   (a) Si $a \neq b$ et $(\alpha, \beta) \neq (0, 0)$, supposons par exemple que $\alpha > 0$. Le lemme **??** implique que

$$(c_{/p^2}(a^{p^\alpha} - b^{p^\beta}), a^{p^{\alpha-1}} \otimes a^{p^{\alpha-1}(p-1)}) = \binom{p^\alpha}{p^{\alpha-1}} \not\equiv 0 \quad [p^2].$$

   Ceci contredit la primitivité de $a^{p^\alpha} - b^{p^\beta}$ et prouve que $\alpha = \beta = 0$.

(b) Si $a = b$, si $(\alpha, \beta) \neq (0,0)$ alors $\alpha \neq \beta$ et sans restriction de généralité on peut supposer $\alpha > \beta$. Encore une fois le lemme **??** implique que $a^{p^\alpha} - a^{p^\beta}$ n'est pas primitif. D'où $\alpha = \beta = 0$.

Montrons maintenant que $a^{p^\alpha} b^{p^\beta} - b^{p^\beta} a^{p^\alpha}$ est primitif si et seulement si $\alpha = \beta = 0$. Supposons $(\alpha, \beta) \neq (0,0)$. Si $\alpha = \beta = 1$ alors on a

$$(c_{/p^2}(a^p b^p - b^p a^p), a^{p-1} b^p \otimes a) = p \not\equiv 0 \quad [p^2],$$

ce qui prouve que $a^p b^p - b^p a^p$ n'est pas primitif. Sinon on peut supposer sans perte de généralité que $\alpha > 0$, dans ce cas le lemme **??** implique que

$$(c_{/p}(a^{p^\alpha} b^{p^\beta} - b^{p^\beta} a^{p^\alpha}), a^{p^{\alpha-1}} b^p \otimes a^{p^{\alpha-1}(p-1)}) = \binom{p^\alpha}{p^{\alpha-1}} \not\equiv 0 \quad [p^2].$$

On vient de montrer que $\gamma_{/p^2}(\equiv) = 1$ si et seulement si $\equiv$ est engendrée par des couples de la forme (a, b) ou (ab, ba). Pour montrer que $\gamma_{/p^2}(\equiv) = 1$ pour toute congruence $/p^2-$ compatible, il suffit de prouver que les seuls polynômes primitifs de la forme $u - v$ avec $u, v \in (A, \theta)$ sont du type $a - b$ ou $ab - ba$ avec $a, b \in A$. Pour cela, il suffit de remarquer que le raisonnement précédent est indépendant des commutations. En l'appliquant encore une fois on trouve le résultat.

Corollaire 114 *Soit K un semi-anneau. Les assertions suivantes sont équivalentes.*

1. *On a $\Gamma(K) = 1$.*
2. *L'anneau K_0 n'est pas isomorphe à $/p$ avec p premier.*

4.6.5 Homogenéité et profondeur

Le but de cette section est l'examen des congruences compatibles homogènes pour un poids $l : A \to^+$ (i.e. une graduation totale non dégénérée). La fonction l s'étend à A^* par $l(w) = \sum_{a \in Alph(w)} |w|_a l(a)$. Cette classe de monoïdes admet une transformation de Magnus injective et nous verrons que les autres monoïdes compatibles et de profondeur 1 ne sont pas simplifiables.

Montrons d'abord que toutes les congruences $K-$ compatibles admettent une transformation de Magnus quotient.
Soit donc μ, l'unique endomorphisme de $K\langle A\rangle$ tel que $\mu(a) = 1 + a$ pour toute lettre $a \in A$. On a le

Lemme 115 *Soient K un semi-anneau et $\equiv$ une congruence $K-$ compatible. Alors il existe un unique morphisme $\mu_{\equiv}$ tel que le diagramme suivant commute.*

$$K < A > \mu K < A > \pi_{\equiv}\pi_{\equiv} K[A^*/_{\equiv}]\mu_{\equiv} K[A^*/_{\equiv}]$$

Preuve Il suffit de remarquer que $\mu = (Id \otimes ev) \circ c$ où ev est l'application linéaire de $K < A >$ dans K telle que $ev(u) = 1$ pour tout mot $u \in A^*$. Cette application est constante sur A^*, elle passe donc au quotient en une application $ev_{\equiv}$. Comme $\equiv$ est $K-$ compatible $c_{\equiv}$ existe. Le morphisme recherché est donc $\mu_{\equiv} = (Id \otimes ev_{\equiv}) \circ c_{\equiv}$ rendant le diagramme suivant commutatif.

$$K < A > cK < A > \otimes K < A > Id \otimes evK < A > \pi_{\equiv}\pi_{\equiv} \otimes \pi_{\equiv}\pi_{\equiv} K[A^*/_{\equiv}]c_{\equiv} K[A^*/_{\equiv}] \otimes K[A^*/_{\equiv}] Id \otimes ev_{\equiv} I$$

Le lemme suivant est immédiat en remarquant que l est un morphisme.

Lemme 116 *Soit $R \subset A^* \times A^*$ et l une longueur. Alors les conditions suivantes sont équivalentes:*
i) Pour tout $(u, v) \in R$, $l(u) = l(v)$.
ii) Pour tout $u, v \in A^*$, $u \equiv v \Longrightarrow l(u) = l(v)$.

Définition 117 *On dira que $\equiv$ (resp. R) est homogène (pour l) si et seulement si elle vérifie les conditions équivalentes du lemme* **??**.

Nous avons alors l'alternative suivante:

Théorème 118 *Soient A un alphabet fini et $\equiv$ une congruence compatible de profondeur* 1. *Alors une seule des deux propriétés suivantes est vraie.*
1) Le monoïde $A^*/_{\equiv}$ est non simplifiable.
2) Il existe une fonction de longueur pour laquelle $\equiv$ est homogène et $A^*/_{\equiv}$ se plonge dans un groupe.

Preuve Si $ch(K)$ est non première alors la congruence est engendrée par des commutations partielles. Sinon posons $p = ch(K)$, d'après ce qui précède une telle congruence est engendrée par des couples (pLC) et (pLI). Les premiers sont multihomogènes et donc sont homogènes pour toutes les fonctions de longueur. Il suffit donc de montrer, dans le cas simplifiable, l'existence d'une longueur rendant les couples (pLI) homogènes. Si l'on note, pour une lettre x, x^p, l'ensemble de ses p-puissances, posons

$$G = \{(a, b) \in (A^*)^2 | \equiv \cap (a^{p \times b^{p)} \neq \emptyset}\}$$

c'est à dire les couples de lettres supports des relations engendrées par (pLI). Il n'est pas difficile de voir que G est le graphe d'une relation d'équivalence. Soient deux relations $a^{p^{\alpha_i}} \equiv b^{p^{\beta_i}}$; $i = \{1, 2\}$. Supposons, sans perte de généralité, que $\alpha_1 \leq \alpha_2$, nous avons aussi

$$a^{p^{\alpha_2}} = [a^{p^{\alpha_1}}]^{p^{\alpha_2-\alpha_1}} \equiv [b^{p^{\beta_1}}]^{p^{\alpha_2-\alpha_1}} = b^{p^{\beta_1+(\alpha_2-\alpha_1)}} \equiv b^{p_2^{\beta}}.$$

Supposons dans la suite le monoïde quotient simplifiable. On a, en vertu de ce qui précède (et avec les mêmes notations) $b^{p^{\beta_1+\alpha_2-\alpha_1}} \equiv b^{p^{\beta_2}}$. Comme le monoïde est simplifiable, ceci entraîne $b^{|p^{\beta_1+\alpha_2-\alpha_1}-p^{\beta_2}|} \equiv 1$. D'où $p^{\beta_1-\alpha_2+\alpha_1} = p^{\beta_2}$ comme cela résulte du lemme **??**. Ceci entraîne $\alpha_2 - \beta_2 = \alpha_1 - \beta_1$. Pour tout $(a, b) \in G$, notons $d_{a,b}$ la différence commune $\alpha - \beta$ pour tous les couples $a^{p^{\alpha}} \equiv b^{p^{\beta}}$ l'existence de la longueur résulte du fait suivant.

Lemme 119 *(Fonction potentiel) Soit G le graphe (non orienté) d'une relation d'équivalence dans un ensemble A. Soit $d : G \rightarrow$ une fonction telle que $(a, b), (a, c) \in G \Longrightarrow d(a, b) + d(b, c) + d(c, a) = 0$. Alors:*

1. *Il existe une fonction $h :\ A \rightarrow$ telle que $d(a, b) = h(b) - h(a)$.*
2. *De plus, si A est fini, on peut choisir h positive.*

Preuve (1) Il suffit de prendre un point distingué dans chaque classe d'équivalence et de lui attribuer le potentiel 0.
(2) Comme h est définie à une constante additive près, lorsque X est fini, il suffit d'ajouter une constante convenable.
Fin de la preuve du théorème ?? Dans le cas où le monoïde quotient est simplifiable, il suffit de prouver que la condition cyclique est satisfaite. Soient $(a, b), (b, c) \in G$. On a trois congruences:

$$a^{p^{\alpha_1}} \equiv b^{p^{\beta_1}},\ b^{p^{\beta_2}} \equiv c^{p^{\gamma_2}},\ c^{p^{\gamma_3}} \equiv a^{p^{\alpha_3}}.$$

Comme $x^{p^u} \equiv y^{p^v} \Longrightarrow x^{p^{u+t}} \equiv y^{p^{v+t}}$, on peut supposer que $\beta_1 = \beta_2,\ \gamma_2 = \gamma_3$. Alors $a^{p^{\alpha_1}} \equiv a^{p^{\alpha_3}}$ et donc, à cause de la simplifiabilité, $\alpha_1 = \alpha_3$. Le calcul des différences donne alors la condition cyclique.
Soit donc h une fonction potentiel positive (d'après le lemme **??** cette fonction existe et est telle que $d_{a,b} = h(a) - h(b)$), la fonction $l := p^h$ rend les relateurs (pLI) homogènes.

Montrons maintenant que le monoïde se plonge dans un groupe. L'image de $A^*/_{\equiv}$ par $\mu_{\equiv}$ est dans $1 + \mathcal{M}(A^*/_{\equiv})$ où $\mathcal{M}(A^*/_{\equiv})$ est l'idéal des séries dont

le terme constant est 0. Or $1 + \mathcal{M}(A^*/_{\equiv})$ est un groupe (puisque l rend $\equiv$ homogène). Il reste à montrer que $\mu_{\equiv} : A^*/_{\equiv} \to 1 + \mathcal{M}(A^*/_{\equiv})$ est injective. Ce qui découle de la formule

$$\mu_{\equiv} w = w + \sum_{l(u)<l(w)} n_u u$$

où $w \in A^*/_{\equiv}$.

Remarque 51 *La preuve du théorème* **??** *montre que si un monoïde $A^*/_{\equiv}$ (où $\equiv$ est $K-$ compatible de profondeur quelconque) admet une graduation totale non dégénérée alors il se plonge dans un groupe. C'est en particulier le cas lorsque $\equiv$ est homogène et pas nécessairement de la profondeur 1 (cf. proposition* **??***).*

4.7 Tableau récapitulatif

$\rho(K)$	$p(K)$	exemple	EL	IL	CL	Autres	$\Gamma(K)$
1	1	$,(,max,+)$	oui	oui	oui	non	-
1	>1	-	non	oui	oui	non	-
>1	-	-	non	oui	oui	non	-
0	1	Anneau nul (que lorsque $A = \emptyset$)	-	-	-	-	-
0	$n > 1$ non premier	$/n$	non	oui	oui	non	1
0	2	$/2$	non	oui	oui	2-commutations 2-echanges voir prop.?? etc...?	≥ 2
0	p>2 premier	$/p$ $/p[i]$ $p \equiv 3[4]$	non	oui	oui	p-commutations p-échanges etc...?	≥ 1
∞	0	, , ,	non	oui	oui	non	1

4.8 Conclusion

Le problème de la caractérisation des monoïdes admettant un produit de mélange est encore ouvert lorsque K est un anneau de caractéristique première (K_0 est un corps fini). On peut tout de même conjecturer l'assertion suivante.

Conjecture 120 *Toute congruence $/p-$ compatible est le suprémum de deux congruences $\equiv_1$ et $\equiv_2$ telles que $\equiv_1$ soit uniquement engendrée par des relateurs de type $(a^{p^\alpha}, b^{p^\beta})$ et $\equiv_2$ multihomogène. De plus, si $p = 2$, alors la profondeur de la congruence est inférieure ou égale à deux, sinon elle est inférieure ou égale à un (ce qui signifie que $\equiv_2$ est engendrée par des relateurs de la forme $(a^{p^\alpha} b^{p^\beta}, b^{p^\beta} a^{p^\alpha})$.*

La première étape pour montrer ceci pourrait être d'étudier les algèbres de Lie des polynôme primitifs de $K[A^*/_\equiv]$, en extraire des bases et essayer d'adapter les calculs vus précédemment.
Pour l'instant, on ne peut pas dire si la $K-$ compatibilité est calculable, le découpage primitif est un outil théorique et ne donne pas un algorithme. En effet, on a besoin de forme normale sur le monoïde pour pouvoir décider si un polynôme est primitif, de plus, on ne sait pas si la profondeur des congruences $K-$ compatible est bornée.
L'étude des monoïdes à p-commutation semble être un sujet intéressant, c'est une généralisation du cadre partiellement commutatif qui conserve des propriétés agréables (groupe sous-jacent, algèbre de Lie, conservation de la multihomogénéité). On pourrait se pencher par exemple sur l'étude de la liberté des algèbres de Lie et groupes associés, sur le calcul de factorisations et de bases, la généralisation de la notion de code, de classe de conjugaison dans le monoïde et dans le groupe, la rationnalité et la reconnaissabilité de série formelle, la combinatoire de ce monoïde (a-t-on encore un lemme de Levi? Peut-on résoudre des équations en "p-traces"?) etc ...
Ce qui ouvre de nouvelles perspectives passionnantes...

Chapter 5

Contribution au logiciel SEA

L'ensemble des procédures expliquées dans ce chapitre s'insère dans le projet SEA ainsi que dans un projet commun avec l'Université du Havre sur la parallélisation des automates à multiplicités.

La première partie de ce chapitre est consacrée à l'étude de l'algorithmique de la minimisation dans un anneau principal. Cet algorithme permet de donner une démonstration calculatoire d'un théorème de Fliess [**?**]. Ce procédé a été implémenté en Maple, nous en donnerons quelques exemples.
Puis, afin de pouvoir tester les propriétés de compatibilité des automates, G.Duchamp m'a demandé de programmer les divers algorithmes (minimisation, produits...) sur différents corps (et anneaux principaux). Comme beaucoup de ces algorithmes sont communs à tous les corps, par souci de minimiser la taille du programme, nous avons créé un type de donnée permettant de représenter un corps (et même plus généralement un semi-anneau). Cette structure est passée en paramètre dans chaque automate qui, de cette façon, sait effectuer les opérations élémentaires (addition, multiplication, inverse, test d'égalité...) sur son corps (par exemple une extension). Il n'est pas seulement agréable de disposer d'extensions formelles de corps pour les multiplicités. Par exemple, la décomposition en éléments simples montre que les séries rationnelles d'une variable peuvent se décomposer en séries de rang plus petit dès que l'on dispose des racines d'un polynôme. Par exemple:

$$\frac{1}{1+ix}+\frac{1}{1-ix}=\sum_{n \text{ pair}} 2i^n x^n = \frac{1}{1+x^2}=\sum_{n\geq 0}(-x^2)^n$$

5.1 Minimisation des automates à multiplicités dans un anneau principal

M.P. Schützenberger avait inauguré l'étude des automates à multiplicités pour $K = [?]$. Par la suite la minimisation a été démontrée dans $K =$ (pour les automates déterministes) et lorsque K est un corps. Fliess [?] montre que si K est un anneau principal, toute série rationnelle admet une représentation minimale à coefficients dans K. Pour la démonstration du processus que nous proposons ici, nous avons utilisé une adaptation de [?] (avec toutes les précautions supplémentaires que réclame une structure plus faible). Le procédé de calcul ne donne effectivement un algorithme que si la détermination des coefficients de Bézout est algorithmique. C'est le cas, en particulier, des anneaux euclidiens. Cependant, dans le cas général, ce calcul redémontre le résultat classique[1].
L'algorithme de minimisation d'un automate à multiplicités (λ, μ, γ) dans un tel anneau K se déroule (comme dans le cas des corps) en deux parties: une réduction à gauche puis une réduction à droite. Comme ces deux étapes sont symétriques, nous traiterons seulement de la réduction à gauche. Le principe de cet algorithme est de parcourir une partie préfixielle (parcours en largeur) et de construire une matrice en utilisant à chaque étape uniquement des opérations conservant la multiplicité sur l'anneau K. De cette façon, les lignes de la matrice ainsi calculée forment une base de $\lambda\mu(K < A >)$.
Soit S une série de représentation linéaire (λ, μ, γ) de dimension n.
L'algorithme proposé prend en paramètre une représentation (λ, μ, γ) de S et retourne un triplet (I, T, X), où I est une matrice de $K^{1\times r}$, $T \in K^{r\times n}$ et X un ensemble préfixe (nous verrons plus bas comment utiliser ces données pour calculer une représentation minimale)[2]. Il comporte deux boucles imbriquées. Dans la plus grande (décrite par l'algorithme `reduireGauche`), on utilisera en plus une variable Y désignant un ensemble contenant les mots restants à traiter. Dans cette boucle l'indice i permettra de représenter l'état des variables après i tours de boucle (ainsi nous nous intéresserons aux quadruplets (I_i, T_i, X_i, Y_i). La variable y représentera le mot courant.
La plus petite boucle (décrite dans l'algorithme `traiterLigne`), permettra

[1] Dont la démonstration usuelle repose sur un argument de borne des dénominateurs et un argument d'existence de bases. Ici, on utilise seulement le caractère "noethérien" des factorisations sans avoir à borner les facteurs.

[2] Ici r est le rang de $\lambda\mu(F < A >)$ où F est le corps des fractions de K.

d'intégrer la ligne $\lambda\mu(y)$ (après d'éventuelles transformations) dans la matrice T et de modifier les autres variables en conséquence. Afin de respecter la multiplicité dans K nous utiliserons un algorithme de Gauss modifié, faisant appel à l'égalité de Bézout. Les variables les plus importantes de cet algorithme sont:

- une matrice ligne J qui au départ sera la matrice I augmentée d'une coordonnée, et qui sera modifiée au fur et à mesure de l'avancement de l'algorithme,
- une matrice M, qui au départ sera la matrice T augmentée de la ligne $\lambda\mu(y)$.

De la même façon que pour l'algorithme `reduireGauche`, le couple (J_i, T_i) représentera l'etat des variables J et T après i étapes (2) exécutées.
Voici donc les algorithmes.

Algorithme 52 `reduireGauche`
Entrée: Une représentation linéaire (λ, μ, γ).
Sortie: Le triplet (I, T, X)
Début

1. *Initialisation.*
$$(I_0, T_0, X_0, Y_0) := ([], [], \emptyset, \{1\})$$
2. *Si* $Y_i \neq \emptyset$ *alors*
On choisit y *minimal en longueur dans* Y_i.
$(I_{i+1}, T_{i+1}, X_{i+1}, Y_{i+1})$:=`traiterLigne`$((I_i, T_i, X_i, Y_i, y), (\lambda, \mu, \gamma))$
3. *Retourner(I,T,X)*

Fin.

Algorithme 53 `traiterLigne`
Entrée: Le quintuplet (I, T, X, Y, y) *et la représentation* (λ, μ, γ)
Sortie: Un quadruplet (I', T', X', Y').
Début
Soit m *le nombre de ligne de* T.

1. *Initialisation:* $(J_0, M_0) := ((I, 0), \begin{pmatrix} T \\ \lambda\mu(y) \end{pmatrix})$.

2. *On pose* $M_i = \begin{pmatrix} T' \\ l \end{pmatrix}$ *et* $J_i = (J'|\alpha)$ *avec* $l \in K^{1\times n}$ *et* $\alpha \in K$.

   (a) *Si* $l = 0$ *alors*

      i. *Si* $T = T'$ *alors Retourner* $(I, T, X, Y - \{y\})$.

      ii. *Si* $T \neq T'$ *alors Retourner* $(J', T', X \cup \{y\}, Y \cup yA - \{y\})$

   (b) *Si* $l \neq 0$ *alors soit* j *le plus petit entier tel que* $l_j \neq 0$.

      i. *Gauss:*
      Si il existe une ligne $(M_i)_k$ *dont la plus petite coordonnée non nulle est*
      j.
      $a := (M_i)_{k,j}$
      $b := l_j$
      $d := pgcd(a, b)$
      et soient α, β *tels que* $\alpha a + \beta b = d$ *(si* $b \equiv 0 \quad [a]$ *on prendra* $\alpha = 1$ *et* $\beta = 0$*).*
      $$G := \begin{pmatrix} Id_{k-1} & 0 & 0 & 0 \\ 0 & \alpha & 0 & \beta \\ 0 & 0 & Id_{n-k} & 0 \\ 0 & -\frac{b}{d} & 0 & \frac{a}{d} \end{pmatrix}$$
      $(J_{i+1}, M_{i+1}) := (J_i G^{-1}, G M_i)$
      Recommencer (2)

      ii. *Insertion:*
      Si une telle ligne n'existe pas alors on considère le plus petit entier k *tel que la plus petite coordonnée non nulle de* $(M_i)_k$ *soit supérieure à* j.
      $$G := \begin{pmatrix} Id_{k-1} & 0 & 0 \\ 0 & 0 & Id_{n-k} \\ 0 & 1 & 0 \end{pmatrix}$$
      $Retourner(J_i G^{-1}, G.M_i, X \cup \{y\}, (Y - \{y\}) \cup yA)$

Fin

Montrons que cette méthode nous permet de réduire à gauche.
Dans la suite, on notera $Lin_K(P)$ le sous-module engendré par P. Nous aurons besoin du résultat suivant.

Proposition 121 *On a les assertions suivantes.*

1. *L'ensemble X est un sous-ensemble préfixe.*
2. *L'algorithme* `reduireGauche` *termine.*
3. *On a $Lin_K(lignes(T)) = \lambda\mu(K < A >)$.*
4. *Si $S \neq 0$ alors $\lambda = IT$.*

Preuve 1) Une induction sur i montre que tout X_i est un sous-ensemble préfixe.

2) Pour toute matrice T en échelons, on notera $lg(T)$ le nombre de facteurs premiers des éléments diagonaux (en comptant les multiplicités).
Soit $Ind(i) = (n - h(T_i), lg(T_i), \sharp Y_i)$ où $h(T_i)$ est le nombre de lignes de T_i.
Il est clair qu'à chaque appel de l'algorithme `traiterLigne` la fonction Ind diminue strictement dans [3] ordonné lexicographiquement. Comme ce dernier est noethérien, l'algorithme s'arrête.

3) Pour montrer que les lignes de T engendrent $\lambda\mu(K)$, il suffit de montrer que pour tout $m \in$ et pour chaque mot w de XA^m, $\lambda\mu(w)$ est une combinaison linéaire de lignes de T. Nous procéderons par induction sur m.

Remarquons tout d'abord, qu'à chaque pas, on a

$$Lin_K(\lambda\mu(X_i)) = Lin_K(lignes(T_i)),$$

donc

$$Lin_K(\lambda\mu(X)) = Lin_K(lignes(T)). \tag{5.1}$$

Ceci prouve notre résultat pour $m = 0$.
Si $xa \in XA - X$, alors il existe i tel que $xa \in Y_i$ et $xa \notin Y_{i+1}$. Par construction, il est clair que $\lambda\mu(xa) \in Lin_K(lignes(T_{i+1}))$ et donc $\lambda\mu(xa) \in Lin_K(lignes(T))$.
Si $xa_1 \dots a_k \in XA^k - \bigcup_{l<k} XA^l$ alors par induction et en utilisant **??**, on peut écrire

$$\lambda\mu(xa_1 \dots a_k) = \sum_{x'a_k \in X \cup XA} \alpha_{x'} \lambda\mu(x'a_k).$$

Les cas initiaux de la récurence nous permettent alors de conclure.

4) Si $S \neq 0$ alors l'algorithme `reduireGauche` effectue au moins un tour

boucle et clairement $\lambda = I_1 T_1$.
Montrons que le produit $I_i T_i$ est constant. Soit $0 < i$, on a alors deux possibilités.
Si $|T_{i+1}| = |T_i|$ (cela correspond au cas 2.a de l'algorithme `traiterLigne`) alors il existe une matrice de Gauss G, un élément $\alpha \in K$ et $y \in X \cup XA$ tel que $(I_i|0) = (I_{i+1}|\alpha)G$ et $\begin{pmatrix} T_i \\ \lambda\mu(y) \end{pmatrix} = G^{-1} \begin{pmatrix} T_{i+1} \\ 0 \end{pmatrix}$. D'où, $I_i T_i = I_{i+1} T_{i+1}$.
Si $|T_{i+1}| = |T_i|+1$ (cela correspond au cas 2.b.ii de l'algorithme `traiterLigne`) alors il existe une matrice de Gauss G telle que $(I_i|0) = I_{i+1} G$ et $\begin{pmatrix} T_i \\ \lambda\mu(y) \end{pmatrix} = G^{-1} T_{i+1}$. D'où le résultat.

Supposons (I, T, X) calculé par l'algorithme `reductionGauche`. L'assertion (3) de la proposition **??** implique que pour tout $a \in A$, il existe une matrice $\mu_r(a) \in K^{r \times r}$ telle que

$$T\mu(a) = \mu_r(a)T. \tag{5.2}$$

Remarque 54 *Pour le calcul, on peut écrire R sous la forme $T = (T'|M)P$ où $T' \in K^{r \times r}$ est une matrice carrée triangulaire supérieure (inversible dans F), $M \in K^{r \times (n-r)}$ et $P \in K^{n \times n}$ une matrice de permutation des colonnes. Soient $M_a \in K^{n \times r}$ et $M'_a \in K^{n \times (n-m)}$ deux matrices telles que $\mu(a) = (M_a|M'_a)P$. Alors on a*

$$T(Ma|Ma')P = \mu_r(a)(T'|M)P,$$

comme P est inversible, ceci implique $TM_a = \mu_r(a')$. La matrice T' étant inversible dans $F^{r \times r}$, $\mu_r(a)$ est donnée par la formule

$$\mu_r(a) = TM_a T'^{-1},$$

*mais $\mu_r(a) \in K^{r \times r}$ à cause de la triangularité de T et de l'existence d'une solution de (**??**).*

De plus, pour tout $w \in A^*$,

$$\lambda\mu(w\gamma) = IT\mu(w)\gamma = I\mu_r(w)T\gamma.$$

En posant $\lambda_r := I$ et $\gamma_r := T\gamma$, la représentation $(\lambda_r, \mu_r, \gamma_r)$ est réduite à gauche.

Pour effectuer la réduction à droite d'une représentation linéaire (λ, μ, γ), il suffit d'effectuer la réduction à gauche de l'automate $(\gamma^t, \mu^t, \lambda^t)$ à multiplicités dans l'anneau K' dont le produit est défini par $\alpha._{K'}\beta = \beta._K\alpha$.
On a, comme dans le cas des multiplicités sur un corps, le résultat suivant.

Théorème 122 *Soient A un alphabet et K un anneau euclidien. Soit S une série de $K << A >>$ et (λ, μ, γ) une représentation linéaire de dimension n de S. La représentation matricielle $(\lambda_r, \mu_r \gamma_r)$ obtenue par réduction à droite puis à gauche est une représentation matricielle réduite de S.*

Preuve En appliquant la minimisation à gauche puis à droite, on trouve une représentation de même rang que celle obtenue lors de la minimisation dans F. Ceci prouve qu'elle est minimale.

Voici quelques exemples. Considérons tout d'abord cet automate à multiplicités dans .

```
> A;
```

$$[[4 \quad 10 \quad 10 \quad 25],\ [a = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 3 & 4 & 6 & 8 \\ 3 & 6 & 4 & 8 \\ 9 & 12 & 12 & 16 \end{bmatrix}],\ \begin{bmatrix} 1 \\ 2 \\ 2 \\ 4 \end{bmatrix}]$$

Après minimisation dans on obtient l'automate.

```
> minimization(A);
 [[-113253    -42883    -239575],

         [      361567393          137666640           769104200]
         [                                                       ]
    [a = [-17161437408683    -6534210426343    -36504767477325]],
         [                                                       ]
         [  3071660114005     1169533359307      6533848858977]

    [    -6143]
    [         ]
    [291571395]]
    [         ]
```

```
    [-52187250]
```

La programmation peut être étendue à d'autres anneaux principaux. Ici par exemple, $[X]$.

```
>A;

                                    [2    1]      [X    X]   [1]
       [[2 + 6 X    1 + X], [a = [      ], b = [      ]], [ ]]
                                    [1    2]      [X    X]   [X]

>minimization(A);
 [

    [1499   183     1419  2   117  3
    [---- + --- X - ---- X  - --- X  ,
    [700    28      700       20

                     2       3          4]
    9/2 + 33 X + 48 X  - 33 X  - 105/2 X ], [a =
                                          ]

    [793   305     473  2   273  3
    [--- + --- X - --- X  - --- X  ,
    [160   32      160      32

    105                 2          3   1225  4]
    --- + 385/8 X + 70 X  - 385/8 X  - ---- X ]
    16                                  16    ]

    [1521  2   429      66043     305     473  2   273  3   153]
    [---- X  + ---- X - ----- , - --- X + --- X  + --- X  - ---], b
    [1600      7000     56000     32      160      32       160]

     =

    [633     305  2   473  3   273  4
```

```
[--- X + --- X  - --- X  - --- X  ,
[160     32       160      32

  35                   2       3       4   ]
- -- (-3 - 22 X - 32 X  + 22 X  + 35 X ) X]
  16                                       ]

[                 2
[1/56000 (53235 X  + 3432 X - 66043) X ,
[

                                          [                     2]
  305  2   473  3   273  4   313  ]   [2 + 11/2 X + 35/2 X ]
- --- X  + --- X  + --- X  - --- X]], [                      ]]
  32       160      32       160  ]   [      11    39      ]
                                      [    - --- - -- X    ]
                                      [      175   20      ]
```

5.2 Représentation d'un semi-anneau

Afin de représenter un semi-anneau, nous avons retenu quelques opérations élémentaires qui le caractérisent: somme, produit, calcul de l'inverse, calcul de l'opposé, test d'égalité de deux éléments, test d'égalité à 0 et à 1 (au cas où l'égalité ne soit pas décidable) et caractéristique.
Un semi-anneau est donc représenté par une table dont les éléments sont des procédures permettant d'effectuer les opérations élémentaires. Les procédures permettant de renseigner ces champs et de les lire sont les suivantes.

```
%test d egalite
setisequal:=proc(K,p)K[‘isequal‘]:=p;end;
getisequal:=proc(K) RETURN(K[‘isequal‘]);end;
%egalite a 0
setiszero:= proc(K,p) K[‘iszero‘]:=p end;
getiszero:= proc(K) RETURN(K[‘iszero‘])end;
%egalite a 1
setisone := proc(K,p) K[‘isone‘]:=p end;
```

```
getisone := proc (K) RETURN(K[‘isone‘]) end;
% Calcul du produit
setprod:=proc(K,p) K[‘*‘]:=p;end;
getprod:=proc(K) RETURN(K[‘*‘]);end;
% Calcul de la somme
getadd:=proc(K) RETURN(K[‘+‘]) end;
setadd:=proc(K,p) K[‘+‘]:=p end;
% Calcul de l’oppose
setopp:=proc(K,p) K[‘-‘]:=p end;
getopp:=proc(K) RETURN(K[‘-‘]) end;
% Calcul de l’inverse
setinverse:=proc(K,p) K[‘inverse‘]:=p end;
getinverse:=proc(K) RETURN(K[‘inverse‘]); end;
% caracteristique (lorsqu’il s’agit d’un anneau)
setcharact:=proc(K,p) K[‘caract‘]:=p; end;
getcharact:=proc(K) RETURN(K[‘caract‘]) end;
```

Les procédures par défaut représenteront le corps des complexes.

```
defaultiszero:=proc(a) RETURN(evalb(a=0));end;
defaultisequal:=proc(a,b) RETURN(evalb(a=b));end;
defaultisone:=proc(b) RETURN(evalb(b=1));end;
defaultinverse:=proc(a) RETURN(1/a);end;
defaultprod:=proc(a,b) RETURN(a*b);end;
defaultadd:=proc(a,b) RETURN(a+b);end;
defaultopp := proc(a) RETURN(-a);end;
```

La création d’un nouveau semi-anneau sera faite grâce à la procédure `newsemiring` qui crée une nouvelle table et initialise les champs de façon à représenter le corps des complexes.

```
> K:=newsemiring();

                                        K := T

> eval(K);

                            table(sparse,[
                                isone = defaultisone
```

```
        + = defaultadd
        * = defaultprod
        isequal = defaultisequal
        - = defaultopp
        iszero = defaultiszero
        inverse = defaultinverse
        caract = 0
])
```

Pour effectuer les opérations élémentaires du corps, on utilise les procédures suivantes:

```
iszero:=proc(K,a) RETURN(K[‘iszero‘](a,K));end;
isone:=proc(K,a) RETURN(K[‘isone‘](a,K));end;
addition:=proc(K,a,b) RETURN(K[‘+‘](a,b,K));end;
prod:=proc(K,a,b) RETURN(K[‘*‘](a,b,K));end;
inverse:=proc(K,a) RETURN(K[‘inverse‘](a,K));end;
opp:=proc(K,a) RETURN(K[‘-‘](a,K));end;
isequal:=proc(K,a,b) RETURN(K[‘isequal‘](a,b,K));end;
```

Plusieurs corps sont implémentés notamment le corps $/p$ lorsque p est premier. Pour créer un tel corps il faut utiliser la commande `newpfield(p)`, comme le montre l'exemple

```
> K:=newpfield(5);

                                    K := T

> addition(K,3,2);

                                      0

> inverse(K,3);

                                      2
```

et les corps du type $/p[i]$ lorsque p est un nombre premier congru à 3 modulo 4, on utilise la procédure `newpcomplexfield` pour leurs créations.

```
> K:=newpcomplexfield(3);

                                        K := T
> prod(K,2*I,1+I);

                                      1 + 2 I
> inverse(K,1+2*I);

                                      2 + 2I
```

5.3 Représentation des matrices

Pour gagner de la place en mémoire les matrices seront représentées par des tables (matrices creuses).

```
‘print/sm‘:=proc(T)
‘MATRIX‘([seq([seq(T[i,j],j=1..getcoldim(T))],i=1..getrowdim(T))]);
 end;

smatrix := proc ()
local T;
if nargs = 2 then
    T := newsmatrix(args[1],args[2])
else
     T := newsmatrix(args[1],args[2],args[3])
fi;
sm(T);
end;


newsmatrix := proc()
local row, col, t, L, i;
row := args[1];
col := args[2];
t := table(sparse);
t[r] := row;
t[c] := col;
if nargs = 3 then
```

```
  L := args[3];
  for i to nops(L) do
  putat(t,
  iquo(i-1,col)+1,((i - 1) mod col) + 1,
          L[i])
  od
fi;
RETURN(t);
end;
```

La procédure ‘`print/sm`‘ permet d'afficher proprement les matrices.

```
> A:=smatrix(3,3,[1,2,3,3+5*I,2,3,I,1+I,1]);
```

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 3 + 5\,I & 2 & 3 \\ I & 1 + I & 1 \end{bmatrix}$$

Une procédure `znormal` permet de faire le "ménage" dans la matrice en enlevant les indices qui contiennent des éléments égaux au 0 du corps.
De nombreuses procédures du package `linalg` ont été reprogrammées afin qu'elles puissent être effectuées dans n'importe quel corps. Quelques exemples:

```
> sinverse(newpcomplexfield(3),A);
```

$$\begin{bmatrix} 2 + I & 1 + 2\,I & 0 \\ 1 + I & 1 + 2\,I & 0 \\ 1 + 2\,I & 2\,I & 1 \end{bmatrix}$$

```
> sinverse(COMPLEXFIELD,A);
```

$$\begin{bmatrix} -\frac{2}{29} + \frac{5}{29}\,I & \frac{2}{29} - \frac{5}{29}\,I & 0 \\ & & \end{bmatrix}$$

```
[    17    59          23    14                    ]
[   --- + --- I    - --- + --- I  3/10 - 9/10 I ]
[   290   290         145   145                    ]
[                                                  ]
[    46    28        12                            ]
[   --- - --- I    --- - 1/145 I  - 1/5 + 3/5 I ]
[   145   145       145                            ]
```

```
> smproduct(newpcomplexfield(3),A,"");
```

```
[ 1  0  0 ]
[         ]
[ 0  1  0 ]
[         ]
[ 0  0  1 ]
```

5.4 Programmation des automates à multiplicités dans un corps.

Les automates seront représentés par trois champs:

1. Un corps.
2. Une liste du type $[\lambda, \mu, \gamma]$ où λ et γ sont des matrices et μ une table indéxée par les lettres de l'alphabet et contenant des matrices.
3. Une table contenant des procédures communes à cette famille d'automates, par exemple le procédé de minimisation est commun à tous les automates à multiplicités dans un corps.

De la même façon que pour les matrices on utilisera une procédure `'print/Aut'` pour afficher les automates de façon propre, on affichera uniquement la liste des matrices de sa représentation. Par exemple, l'automate suivant est à multiplicités sur $/3[i]$.

```
> A;
```

```
                          [ I  2 I ]      [ 1  2 ]   [ I ]
        [[ 1  1 ], [a = [        ], b = [      ]], [   ]]
                          [ I   I  ]      [ I  I ]   [ 0 ]
```

J'ai réécrit les différentes procédures sur les automates présentés dans SEA afin de les adapter à la nouvelle structure de données. En voici quelques exemples.

```
> Hadamard(A,A);
[[ 1  1  1  1 ],
          [ 2  1  1  2 ]      [ 1   2    2    1  ]   [ 2 ]
          [            ]      [                  ]   [   ]
          [ 2  2  1  1 ]      [ I   I   2 I  2 I ]   [ 0 ]
     [a = [            ], b = [                  ]], [   ]]
          [ 2  1  2  1 ]      [ I  2 I   I   2 I ]   [ 0 ]
          [            ]      [                  ]   [   ]
          [ 2  2  2  2 ]      [ 2   2    2    2  ]   [ 0 ]
> minimization(");

                     [ 0  0   2I  ]     [ 0 2+2I 2I   ]  [ 1 ]
                     [            ]     [             ]  [   ]
  [[ 2  I  1 ], [a = [ 0  2I 1+2I ],b = [ 1 2+2I 1+2I ]],[ 0 ]]
                     [            ]     [             ]  [   ]
                     [ 0  1  1+I  ]     [ 0  1   1+I  ]  [ 0 ]
```

5.5 Un exemple complet d'utilisation

Supposons que nous voulions minimiser l'automate sur une lettre et à valeur dans le corps des quaternions suivant:

(0,2)(9.5,8.5)
(2,7)10A (6,7)10B (6,4)10D (2,4)10C ->AB41k ->BA$i+k$
[angleB=180,loopsize=0.5,arm=.5,linearc=.2]->AA2 + 2i
[angleB=180,loopsize=0.5,arm=.5,linearc=.2]<-BB2 + 2i + 2j ->BD41k ->DB41k
[angleB=180,loopsize=-0.5,arm=0.5,linearc=.2]<-DD2 + 4i + 2j ->DC41k
->CD$i+k$ [angleB=180,loopsize=-0.5,arm=0.5,linearc=.2]->CC2 + 2i + 2j

$$\text{->CA41}k\ \text{->AC41}k\ \text{->(1,6)(1.8,6.8) :U1 <-(6.2,6.8)(9,5.4):U1} + i + j + k$$
$$\text{->(0,3)(1.8,4.2):U1} + i + j + k\ \text{<-(6.2,4.2)(9.2,4.2):U}-2 + 2i + 2j + 2k$$
$$\text{<-(5,5)(5.8,4.2):U1}$$

Un quaternion $a + bi + cj + dk$ sera représenté par une liste de ces quatre composantes `[a,b,c,d]`. Il faut, tout d'abord, programmer les différentes opérations élémentaires sur le corps des quaternions. Par exemple la multiplication:

```
Hmult := proc(x, y)
local a, b, c, d, A, B, C, D;
  if x = 0 or y = 0 then RETURN(0)
  else
     a := x[1];b := x[2];c := x[3];d := x[4];
     A := y[1]; B := y[2];C := y[3];D := y[4];
     if x = 1 and y = 1 then RETURN([1, 0, 0, 0])
     elif x = 1 then RETURN([A, B, C, D])
     elif y = 1 then RETURN([a, b, c, d])
     else
       RETURN([a*A - b*B - c*C - d*D, a*B + b*A + c*D - d*C,
         a*C - b*D + c*A + d*B, a*D + b*C - c*B + d*A])
     fi
 fi
end
```

Une fois ceci effectué[3], il faut créer un nouveau semi-anneau et lui affecter ces opérations.

```
> QUATERNIONFIELD := newsemiring();

                          QUATERNIONFIELD := T

> setisone(QUATERNIONFIELD,Hisone);

                                  Hisone

> setiszero(QUATERNIONFIELD,Hiszero);
...
```

[3]Il faut faire attention, tout de même, au cas particulier du 0 et du 1 qui peuvent être représentés comme des réels

Vérifions que tous les champs aient bien été renseignés.

```
> eval(QUATERNIONFIELD);


table(sparse, [
    * = Hmult
    isequal = Hequal
    + = Hadd
    iszero = Hiszero
    inverse = Hinverse
    caract = 0
    isone = Hisone
    - = Hopp
    0 = 0
    1 = 1
    ])
```

Ensuite, il faut créer un automate à multiplicités sur ce corps. Le mieux est d'écrire une procédure permettant d'initialiser ce type d'automate.

```
QuaternionAutomaton := proc()
local A;
    A := Automaton();
    setsemiring(A, QUATERNIONFIELD);
    setmini(A, smini);
    RETURN(A)
end
```

La procédure `smini` étant la procédure qui permet la minimisation d'un automate à multiplicités sur n'importe quel corps. Il suffit alors de créer cet automate en appelant cette procédure et en lui donnant sa représentation sous forme de matrice. Ainsi notre automate sera représenté par:

```
>A;
[[[1, 0, 0, 0], [1, 1, 1, 1], [1, 1, 1, 1], [-2, 2, 2, 2] ],
     [[2, 0, 2, 0] [0, 0, 0, 41] [0, 0, 0, 41]         0     ]
     [                                                       ]
     [[0, 1, 0, 1] [2, 2, 2,  0]        0       [0, 0, 0, 41]]
[a=  [                                                       ] ],
```

```
     [[0, 1, 0, 1]        0        [2, 2, 2, 0]   [0, 0, 0, 41]]
     [                                                          ]
     [      0        [0, 1, 0, 1] [0, 1, 0, 1]    [2, 4, 2, 0]]
  [0]
  [ ]
  [0]
  [ ]]
  [0]
  [ ]
  [1]
```

La minimisation se fait alors de façon classique.

```
> minimization(A);

[

    [[-2, 2, 2, 2] , [-98, 74, -74, 82] , [-3542, 84, -180, 116]],

         [     0               0          [360, 344, 360, -328]]
         [                                                     ]
    [a = [[1, 0, 0, 0]          0          [-188, -8,  -8,   0 ]]],
         [                                                     ]
         [     0          [1, 0, 0, 0]    [  6,   2,   2,   0 ]]

    [1]
    [ ]
    [0]]
    [ ]
    [0]
```

5.6 Validation

Afin de valider l'ensemble des procédures programmées, nous avons effectué plusieurs types de tests.

- Des tests exhaustifs sur des automates de petites dimensions lorsque l'anneau est fini (Par exemple dans /2 il y a 256 automates de dimension 2 sur l'alphabet a).
- Des tests exhaustifs sur des automates de petites dimensions à valeur dans un sous-ensemble fini de K lorsque celui-ci est infini (ou trop grand).
- Des tests sur des automates de plus grandes dimensions générés aléatoirement.

Les algorithmes ont été testés sur les corps , , , H, $/p$ (lorsque p est premier), $/p[i]$ (lorsque p est premier et $p \equiv 3 \quad [4]$, ainsi que sur les anneaux et $[x]$.

Chapter 6

Conclusion générale

Dans le cas non commutatif, le produit de mélange est relié à de nombreuses notions: les sous-mots, les bases de Hall, la transformation de Magnus, le projecteur orthogonal, les polynômes primitifs (algèbre de Lie) etc...

Ce produit admet une généralisation dans les monoïdes de traces. Nous avons montré que le cadre des commutations partielles est maximal (aux identifications de lettres près) lorsque K est un semi-anneau qui n'est pas un anneau ou un anneau de caractéristique non première. Nous avons donc étudié quelques propriétés combinatoires du monoïde des traces.

Dans un premier temps, nous nous sommes intéressés à l'étude des factorisations de (A, θ) et des bases de $L_K(A, \theta)$. Nous avons montré qu'il était possible de généraliser l'élimination de Lazard pour des sous-alphabets quelconques mais que les facteurs droits ne sont pas toujours des monoïdes partiellement commutatifs libres. Nous nous sommes donc intéressé aux bisections transitives car elles respectent la liberté du facteur droit. Ainsi par composition nous avons construit des factorisations complètes et par crochetage des bases de $L_K(A, \theta)$. En utilisant cette méthode, nous avons donné une généralisation des bases de Hall pour une famille d'alphabets à commutations. Il reste cependant de nombreuses questions encore ouvertes:

- Peut-on trouver une généralisation des bases de Hall pour l'ensemble des algèbres de Lie partiellement commutatives libres?
- Est-il décidable si deux factorisations transitives finies admettent un majorant commun?
- Comment factoriser les facteurs droits des bisections non transitives?

- Y a-t-il une algorithmique intéressante avec des automates reconnaissants $\beta_Z(B)$?
- Existe-t-il d'autres factorisations dichotomiques transitives?

Le problème du support, qui est l'objet du chapitre 3, est intimement lié au produit de mélange. En effet, le théorème de Ree (ou plutôt son analogue partiellement commutatif) implique que tout mot (toute trace) qui n'appartient pas au support peut s'écrire comme une combinaison linéaire de mélanges de deux mots non vides. Nous avons apporté une solution à ce problème pour les monoïdes de traces dont l'alphabet à commutations ne contient aucun sous-graphe (strict) de la forme $a - b - c - d$.

Étrangement, ce sous-graphe apparaît dans d'autres problèmes, comme le problème du sous groupe et de la décidabilité du fait que deux parties rationnelles sont disjointes. Nous n'avons, pour l'instant, aucune explication à ce phénomène qui reste mystérieux.

Le produit de mélange s'étend à d'autres monoïdes dans le cas de la caractéristique première. Bien que nous n'ayons pas encore réussi à caractériser complètement l'ensemble de ces monoïdes, nous avons dégagé un outil : l'existence d'un découpage primitif, qui permet de n'utiliser que des polynômes de Lie pour construire des congruences $K-$ compatibles. Nous avons montré que les congruences de profondeur 1 sont toutes engendrées par des p-commutations et des p-identifications et que ce cas absorbe toutes les relations de la forme $a^\alpha \equiv b^\beta$ et $a^\alpha b^\beta \equiv b^\beta a^\alpha$. Nous donnons dans le cas de la caractéristique première une famille de congruences de profondeur 2.

Nous avons prouvé que le mélange de séries reconnaissables saturées par une congruence $\equiv$, $K-$ compatible est lui aussi saturé. Il reste à écrire une algorithmique des congruences $K-$ compatibles: peut-on décider si une congruence est $/p-$ compatible?

Bien qu'il reste de nombreux travaux à effectuer dans ce domaine, on peut espérer trouver une théorie plus complète mettant en évidence les propriétés combinatoires des monoïdes $A^*/_\equiv$ et des algèbres associées (existe-il des bases de Lyndon? quels sont les propriétés des classes de conjugaison? quels sont les dimensions des composantes multihomogènes -lorsque $\equiv$ est homogène- de l'algèbre de Lie des polynômes primitifs? Quelles sont ses bases?...). Ce qui précède montre qu'il y aurait une branche de la combinatoire à développer en caractéristique p (la p-combinatoire selon A.A.Mikhalev [**?**]).

Bibliography

[1] J. Aalbersberg, H.J. Hoogeboom, *Characterizations of the Decidability of Some Problems for Regular Trace Languages*, Mathematical System Theory, 22, 1-19,1989.

[2] J. Berstel and D. Perrin, *Theory of codes* (Academic Press, New-York, 1985).

[3] J. Berstel and C. Reutenauer, *Rational Series and Their Languages,* (EATCS Monographs on Theoretical Computer Science, Springler-Verlagm Berlin, 1988).

[4] N.Bourbaki, *Éléments de mathématiques, Groupes et algèbres de Lie, Chap. 1* (Hermann, Paris, 1972).

[5] N.Bourbaki, *Éléments de mathématiques, Groupes et algèbres de Lie, Chap. 2 et 3* (Hermann, Paris, 1972).

[6] N. Bourbaki, *Éléments de mathématiques, Groupes et algèbres de Lie, Chap. 4,5 et 6,* (Hermann, Paris, 1972).

[7] P.Cartier, D.Foata, *Problèmes combinatoires de commutation et réarrangement*, Lect. Not. In Math., n 85, 1969.

[8] K.T.Chen, R.H.Fox, R.C.Lyndon, *Free differential calculus IV- The quotient groups of the lower central series,* Ann. Of Math, 1958.

[9] C.Choffrut, *Free partially commutative monoids,* (Technical Report 86, LITP, Université Paris 7, 1986).

[10] R. Cori, D.Perrin, *Automates et commutations partielles*, R.A.I.R.O., Informatique théorique et applications, 19, 21-32,1985.

[11] W. Dicks, *An exact sequence for rings of polynomials in partly commuting indeterminates,* Journal of Pure and Applied Algebra, **22**, 215-228, 1981.

[12] V. Diekert, *A partial trace semantics for Petri nets,* Theoretical Computer Science, 113,87-105,1994, Special issue of ICWLC 92, Kyoto (Japan).

[13] V. Diekert, *Mathematical aspects of trace theory*, Mitt. Math Ges. Hamburg, 12,1171-1181,1992, Soecial issue of tricentenary.

[14] V. Diekert and G. Rozenberg, *The book of traces* (World Scientific, Singapour, 1995).

[15] C.Droms, *Graph groups, coherence and three-manifolds,* Journal of algebra, **106**, 484-489,1987

[16] C.Droms, *Subgroups of graph groups,* Journal of algebram, **110**, 519-522,1987.

[17] C.Duboc, *Commutations dans les monoïdes libres : un cadre théorique pour l'étude du parallélisme* (Thèse, Université de Rouen, 1986).

[18] P.Dubreuil,*Contribution à la théorie des demi-groupes,* Mem.Acad.Sc.Inst, France, 63 1941.

[19] G.Duchamp, *Portes et factorisations d'idéaux*, Deuxièmes Journées franco-belges 3-5 semptembre 1991, Publications de L'Université de Rouen

Nř176,91-98,1991.

[20] G.Duchamp, *Orthogonal projection onto the free Lie algebra,* Theorical Computer Science, **79**, 227-239, 1991.

[21] G. Duchamp , A. Klyachko, D. Krob., J.Y. Thibon, *Noncommutative symmetric functions III: Deformations of Cauchy and convolution algebras* Discrete Mathematics and Theoretical Computer Science Vol. **2** (1998).

[22] G.Duchamp, D.Krob, *The free partially commutative Lie algebra: bases and ranks,* Advances in Mathematics, vol 95 N 1, septembre 1992, p. 92-126.

[23] G.Duchamp, D.Krob, *Free partially commutative structures J. Algebra* **156**-2 (1993) 318–361.

[24] G.Duchamp, D.Krob, *Partially commutative Magnus transformation* Int. J. of Alg. And comp., 3-1, 1993,15-41.

[25] G.Duchamp, E.Laugerotte, J.G. Luque, *Support d'une famille d'algèbres de Lie partiellement commutatives libres* Colloque WORDS'99, Rouen, 1999.

[26] G.Duchamp, J.G.Luque, *Transitive Factorizations*, Colloque FPSAC'99 Barcelone,1999.

[27] G.Duchamp, A.A. Mikhalev, *Graded shuffle algebras over a field of prime characteristic* Colloque FPSAC'99 Barcelone, 1999.

[28] G.Duchamp, C. Reutenauer, *Sur un critère de rationalité provenant de la géométrie non-commutative,* Invent. Math, **128**, 613-622,1997.

[29] G.Duchamp, J.-Y. Thibon, *Le support de l'algèbre de Lie libre,* Discrete Mathematics, **76**,46-51, 1980.

[30] S.Eilenberg, *Automata, language and machines*, Vol A. Acad.Press.,1974.

[31] M. Fliess, *Matrices de Hankel,* J. Math. Pures and Appl., **53**, 197-224, 1974.

[32] M. Fliess, *Sur divers produits de séries formelles,* Bull. Sc. Math., **102**, 181-191, 1974.

[33] M.Flouret, *Contribution à l'algorithmique non commutative*, Thèse de doctorat, Univerité de Rouen, 1999.

[34] M.Flouret, E. Laugerotte, *Noncommutative minimization algorithms,* Inform. Process. Lett. **64**, (1997), 123-126.

[35] M.Flouret, J.G.Luque, G.Duchamp, *Théorème de factorisation de Schützenberger pour les monoïdes partiellement commutatifs libres,* Colloque AMI, Marseille, 1996.

[36] P.Gastin, *Un modèle asynchrone pour les systèmes distribués*, Theoretical Computer Science, 74,121-162, 1990.

[37] P. Gastin, *Decidability of the Star problem in* $A^* \times \{b\}^*$, Information Processing Letters, 44,65-71,1992.

[38] P.Gastin, A.Petit, W.Zielonka, *An extension of Kleene's and Ochmański's theorem to infinite traces,* Theoretical Computer Science, 120,101-121,1993.

[39] S. Gaubert, J.Mairesse, *Medeling and analysis of timed Petri nets using heap of pieces*, IEEE,Trans. Autom. Control, Vol 44, n4,683-697,1999.

[40] S. Gaubert, J.Mairesse, *Asymptotic Analysis of heaos of pieces and application to timed Petri Nets*, Proceedings of the 8th int. Workshop on Petri nets and performance Models-(PNPM'99),september 99, Zaragoza-Spain.

[41] J.Hopcroft, D.Ullman, *Introduction to automata theory languages and computation,* (Addison Wesley, 1979).

[42] K.H. Kim, L. Makar-Limanov, J. Neggers, F.W. Roush, *Graph algebras,* Journal of Algebra,64,46-51,1980.

[43] S.C Kleene, *Representation of events in nerve nets and finite automata,* Automata Studies, Princeton univ. Press, 3-42, 1956.

[44] Y. Kobayashi, *Partial commutation, homology and the Möbius inversion formula*, In M.Ito, editors, Words, Languages and Combinatorics (Kyoto, Japan, 1990)m 288-298, World Scientific, Singapore, 1992.

[45] D. Krob and P.Lalonde, *Partially commutative Lyndon words Lect. Notes in Comput. Sci.* **665** (1993) 237–246.

[46] P.Lalonde, *Contribution à l'étude des empilements* (Thèse de doctorat, LACIM, 1991).

[47] M.Lazard, *Groupes, anneaux de Lie et problème de Burnside*, Istituto Matematico dell' Università di Roma,1960.

[48] M.Lothaire, *Combinatorics on words*, Addison Wesley, 1983.

[49] M.Lucas, *Théorie des nombres*, Paris 1891, (reimp Blanchard 1961).

[50] J. Mairesse, L. Vuillon, *Optimal sequences in a heap model of two pieces* LIAFA Research report 98/09,1998.

[51] A.Mazurkiewicz, *Concurrent program schemes and their interpretations*, DAIMI Rep., PB 78, Aarhus University, 1977.

[52] A.Mazurkiewicz, *Traces, histories and graph: instances of a process monoid*, Lect. Notes in Comp. Sci., n 176,115-133,1984.

[53] A. Muscholl, *On the complementation of Büchi asynchronous cellular automata*, In S. Abiteboul and E. Shamir, editors, Proceeding of the 21st Internationnal Colloquium on Automata, Langages and programming (ICALP'94), Jerusalem (Israel) 1994, 820, Lecture Notes in Computer Science, 142-153, Springer, 1994.

[54] P. Ochsenschläger, Binomialkoeffitzenten und Shuffle-Zahlen, Technischer Bericht, Fachbereich Informatik, T. H. Darmstadt,1981.

[55] D.Perrin, *Partial commutations,* In Proceeding of the 16th Internationnal Colloquium on Automata, Languages and Programming (ICALP'89), Stresa (Italy) 1989, 372, Lecture Note in Computer Science, 637-651, Berlin-Heidelberg-New York, 1989, Springer.

[56] R.Ree, *Lie elements and an algebra associated with shuffles,* Annals of Mathematics,68,221-220,1958.

[57] C. Reutenauer, *Free Lie algebras* (Oxford University Press, New-York, 1993).

[58] J.Sakarovitch, *On reguar trace languages*, Theoretical Computer Science, 82, 59-75,1987.

[59] J.Sakarovitch, *The "last" decision problem for rational trace languages,* IN I.Simon, editor, Proceeding of the 1st Latin American Symposium on Theoretical Informatics (LATIN'92), 583, Lecture

Note in Computer Science, 460-473, Berlin-Heidelberg-New York, 1992, Springer.

[60] W.Schmitt, *Hopf algebras and identities in free partially commutative monoids*, T.C.S. North Holland, 1990.

[61] M.P. Schützenberger, *On a factorization of free monoids*, *Proc. Amer. Math. Soc.* **16** (1965) 21-24.

[62] M.P. Schützenberger, *Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de Mathématiques appliquées*, seminaire Dubreuil-Pisot Année 1958-1959, Paris, 1958.

[63] M.P. Schützenberger, *On the definition of a family of automata,* Inform. and Contr., **4**, 245-270, 1961.

[64] M.P. Schützenberger, *On a theroem of R. Jungen,* Proc. Amer. Soc., **13**, 885-890, 1962.

[65] A.I. Shirshov, *Bases of free Lie algebra*, Algebra i Logika ,**1**(1962), 14-9.

[66] G. Viennot, *Algèbres de Lie libres et Monoïdes Libres* Thèse d'État, Paris 7,1974.

[67] G. Viennot, *Algèbres de Lie libres et Monoïdes Libres Lecture Notes in Mathematics*, **691** (1978).

[68] X.G.Viennot, *Heaps of pieces I: Basic definitions and combinatorial lemmas* In G. Labelle et al., editors, Proceeding Combinatoire énumeratice, Montréal Quebec 1985, nymber 1234 in Lectures notes in Mathematics, 321-350, Berlin-Heidelberg-New York, 1986, Springer.

[69] W. Zielonka, *Notes on finite asynchronous automata,* R.A.I.R.O., Informatique Théorique et Applications,21:99-135,1987.

[70] W. Zielonka, *Safe executions of recognizable trace langages by asynchronous automata,* In A.R. Mayer et al., editors, Proceeding of the Symposium on Logical Foundation of Computer Science, Logic at Botik'89, Pereslavl-Zalessky (USSR) 1989, 363 in Lecture notes in Computer Science, 278-289, Berlin- Heidelberg-New York, 1989, Springer.

Appendix A

Structures partiellement commutatives

D'autres structures partiellement commutatives sont bien connues et sont utilisées dans le document. En fait, le problème de l'existence d'une structure partiellement commutative libre peut se poser dans toute catégorie pour laquelle il existe une notion de commutation symétrique.
Mentionons tout d'abord l'algèbre associative partiellement commutative libre sur un semi-anneau K définie comme $K < A, \theta >= K[(A, \theta)]$. Lorsque K est un anneau , l'algèbre de Lie partiellement commutative libre $L_K(A, \theta)$ peut être réalisée comme étant l'algèbre de Lie engendrée par les lettres. Le groupe partiellement commutatif libre (A, θ) est le groupe construit à partir du monoïde (A, θ). Ces structures ont été étudiées par Duchamp et Krob dans [?], [?] et [?]. Les structures $K < A, \theta >$, $L_K(A, \theta)$, (A, θ) et (A, θ) sont libres chacune dans leur catégorie.

De la même façon que dans le cas non commutatif, on définit l'algèbre associative $K << A, \theta >>$ des séries formelles de traces. On définit les composantes multihomogènes d'une série $S = \sum(S, w)w$ par $S_\alpha = \sum_{w \in M_\alpha}(S, w)w$.

Le résultat suivant, très général, sera utilisé dans la discussion sur les congruences $K-$ compatibles. Il s'applique aux commutations partielles.

Théorème 123 *Soit g une algèbre de Lie sur un anneau de caractéristique première p, de base $(b_i)_{i \in I}$ et telle que son algèbre enveloppante A soit munie du coproduit usuel c .*
Alors la famille $(b_i^{p^e})_{\substack{i \in I \\ e \in}}$ est une base de l'algèbre de Lie des éléments primitifs (c.a.d. tels que $c(x) = x \otimes 1 + 1 \otimes x$) de A.

Preuve La famille $(b_i^{p^e})_{\substack{i\in I\\ e\in}}$ est une famille libre de A (c'est une sous famille de la base de Poincaré-Birkhoff-Witt). Il suffit donc de prouver qu'elle engendre tous les éléments primitifs (c'est à dire que si un élément de la base de Poincaré-Birkhoff-Witt est primitif alors il s'écrit sous la forme d'une combinaison linéaire de $b_i^{p^e}$) .
Soient

$$P_a = a_{i_1}^{\alpha_1} \cdots a_{i_n}^{\alpha_n},$$

et

$$P_b = b_{j_1}^{\beta_1} \cdots b_{j_m}^{\beta_m}.$$

Alors

$$c(P_a) = \sum_{r_1,\ldots,r_n} \binom{\alpha_1}{r_1} \cdots \binom{\alpha_n}{r_n} a_{i_1}^{r_1} \cdots a_{i_n}^{r_n} \otimes a_{i_1}^{\alpha_1 - r_1} \cdots a_{i_n}^{\alpha_n - r_n} \tag{A.1}$$

et

$$c(P_b) = \sum_{s_1,\ldots,s_m} \binom{\beta_1}{s_1} \cdots \binom{\beta_m}{s_m} b_{j_1}^{s_1} \cdots b_{j_m}^{s_m} \otimes b_{j_1}^{\beta_1 - s_1} \cdots b_{j_m}^{\beta_m - r_m}$$

Si $P_a \neq P_b$ alors les produits tensoriels intervenant dans $c(P_a)$ sont différents de ceux intervenant dans $c(P_b)$. Donc si

$$P = \sum_{\substack{i_1>\ldots>i_n\\ \alpha_1,\ldots,\alpha_n\neq 0}} \lambda_{i_1,\ldots,i_n,\alpha_1,\ldots,\alpha_n} b_{i_1}^{\alpha_1} \cdots b_{i_n}^{\alpha_n},$$

$c(P)$ est primitif si et seulement si tous les monômes de son support le sont. Soit P_a un tel monôme. Le développement (**??**) montre que si P_a est primitif, $n = 1$ et que pour tout $j \in [1, \alpha_1 - 1]$, $\binom{\alpha_1}{j} \equiv 0 \quad [p]$. D'après le lemme **??** que α_1 est une puissance de p. Ceci prouve le résultat.

Définition 124 *Une série S est dite* **de Lie** *si et seulement si ses composantes multihomogènes sont des polynômes de Lie.*

Le lien avec les éléments primitifs est le suivant.

Théorème 125 *1. Si S est de Lie alors $c(S) = S \otimes 1 + 1 \otimes S$.*

2. Si K est de caractéristique 0, $c(S) = S \otimes 1 + 1 \otimes S$ implique S est de Lie[1].

[1] c désigne le coproduit du produit de mélange

On dira d'une famille de séries $(S_i)_{i\in I}$ qu'elle est sommable (ou localement finie) si pour tout $w \in (A,\theta)$ la famille $((S_i,w))_{i\in I}$ est à support fini. On définit alors

$$\sum_{i\in I} S_i := \sum_{w\in M}\left(\sum_{i\in I}(S_i,w)\right)w.$$

On pourra aussi multiplier une famille ordonnée de séries $(S_i)_{i\in(I,<)}$ telles que $(S_i,1)=1$ si pour tout mot w il existe $F_w \subset I$ fini tel que pour tout L fini, $F_w \subset L \subset I$ on ait

$$\left(\prod_{i\in F_w}^{\rightarrow} S_i, w\right) = \left(\prod_{i\in L}^{\rightarrow} S_i, w\right).$$

On peut alors poser

$$\left(\prod_{i\in I}^{\rightarrow} S_i, w\right) = \left(\prod_{i\in F_w}^{\rightarrow} S_i, w\right).$$

On vérifie facilement que ce coefficient ne dépend pas du choix de F_w stationnaire. Les produits décroissant $\prod_{i\in I}^{\leftarrow} S_i$ se définissent de façon identique.

La définition suivante est motivée par le fait que, pour $K=$, les exponentielles de séries de Lie sont des éléments de type groupe.

Définition 126 *Une série S est dite de type groupe si et seulement si $c(S) = S\otimes S$ et $(S,1)=1$.*

Théorème 127 *Dans $<< A,\theta >>$, S est de type groupe si et seulement si $log(S)$ est de type Lie (primitif).*

Le résultat suivant, très général, s'applique dans le cas des commutations partielles.

Proposition 128 *Soit $(1+S_i^+)_{i\in i\in I}$ une famille de séries telle que $(S_i^+,1) = 0$ de $<< A,\theta >>$. Supposons que le produit $\prod_{i\in I}^{\leftarrow}(1+S_i^+)$ soit convergent. Alors*

$$log\left(\prod_{i\in I}^{\leftarrow}(1+S_i^+)\right) - \sum_{i\in I} log(1+S_i^+)$$

est une série de Lie sans terme de degré 1.

Preuve Soit $T = \{t_i\}_{i\in I}$ un alphabet. On considère le morphisme
$\phi :<< T >> \rightarrow << A, \theta >>$ tel que $\phi(t_i) = log(1 + S_i^+)$.
Dans $<< T >>$, e^{t_i} est un élément de type groupe. Donc, il en est de même de $\overleftarrow{\prod_{i\in I}} e^{t_i}$.
Par suite,

$$log\left(\overleftarrow{\prod_{i\in I}} e^{t_i}\right) - \sum_{i\in I} e^{t_i}$$

est une série de Lie sans composante de degé 1 et donc une combinaison linéaire (infinie) de $[u, v]$.
La transformation par ϕ implique que

$$log\left(\overleftarrow{\prod_{i\in I}}(1 + S_i^+)\right) - \sum_{i\in I} log(1 + S_i^+)$$

est une combinaison linéaire de crochets de séries $SR - RS$, ce qui entraîne le résultat.

Appendix B

Quelques graphes connexes minimaux pour le pliage.

n=1 unit=0.5

(1,1) (0.5,0.5)4a

n=2

Pas de graphes minimaux

n=3

Pas de graphes minimaux

n=4

(-2,0)(1,1) (-2,0)4a (-1,0)4b (0,0)4c (1,0)4d ab bc cd

n=5

(-2,0)(1.5,1.5) (-2,0)4a (-1,0)4b (0,0)4c (1,0)4d ab bc cd (-2,0)(2.5,2.5)

(-2,0)4a (-1,0)4b (0,0)4c (1,0)4d (2,0)4e ab bc cd de (-2,0)(1.5,1.5)

(-2,0)4a (-1,0)4b (0,0)4c (1,0)4d (-1,1)4e ab bc dc be (-2,0)(1.5,1.5) (-2,0)4a

(-1,0)4b (0,0)4c (1,0)4d (-.5,1)4e ab bc dc be ec (-1,0)(1.5,2.5) (-1,0)4a

(1,0)4b (-1,1)4c (1,1)4d (0,2)4e ab bd ac de ec (-1,0)(1.5,2.5) (-1,0)4a

(1,0)4b (-1,1)4c (1,1)4d (0,2)4e ab bd ac de ec dc

Appendix C

Quelques graphes qui ne sont pas du type H

n=1

Tous les graphes sont de type H.

n=2

Tous les graphes sont de type H.

n=3

Tous les graphes sont de type H.

n=4

(-2,0)(1,1) (-2,0)4a (-1,0)4b (0,0)4c (1,0)4d ab cd

n=5

(-1,0)(1.5,2.5) (-1,0)4a (1,0)4b (-1,1)4c (1,1)4d (0,2)4e bd ac (-1,0)(1.5,2.5) (-1,0)4a (1,0)4b (-1,1)4c (1,1)4d (0,2)4e ab bd ec (-1,0)(1.5,2.5) (-1,0)4a (1,0)4b (-1,1)4c (1,1)4d (0,2)4e ab bd ad ec (-1,0)(1.5,2.5) (-1,0)4a (1,0)4b (-1,1)4c (1,1)4d (0,2)4e ab bd ac de (-1,0)(1.5,2.5) (-1,0)4a (1,0)4b (-1,1)4c (1,1)4d (0,2)4e ab bd ad de ec dc