Lecture Notes in Mathematics

Edited by A Dold and B Eckmann

691

Gérard Viennot

Algèbres de Lie Libres et Monoïdes Libres

Bases des Algebres de Lie Libres
et Factorisations des Monoides Libres

Springer-Verlag
Berlin Heidelberg New York 1978

Author
Gérard Viennot
ENS – Centre de Mathématiques
45, rue d'Ulm
F-75005 Paris

Library of Congress Cataloging in Publication Data

Viennot, Gérard, 1945-
Bases des algèbres de Lie libres et factorisations des monoïdes libres.

(Lecture notes in mathematics ; 691)
Bibliography: p.
Includes indexes.
1. Lie algebras. 2. Monoids. I. Title.
II. Series: Lecture notes in mathematics (Berlin) ; 691.
QA3.L28 no. 691 [QA252.3] 510'.8s [512'.55] 78-23919

AMS Subject Classifications (1970): 05-00, 08A10, 16A68, 17-04, 17B99, 20E15, 20F35, 20F40, 20M05, 68A25, 94A10

ISBN 3-540-09090-8 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-09090-8 Springer-Verlag New York Heidelberg Berlin

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2141/3140-543210

TABLE DES MATIERES

INTRODUCTION

Le but du présent travail est de proposer une théorie unifiée du calcul des commutateurs basiques ou d'une manière équivalente, des bases et familles basiques des algèbres de Lie libres.

L'intérêt porté aux algèbres de Lie libres vient essentiellement des applications importantes dans la théorie que l'on appelle aujourd'hui "théorie combinatoire des groupes" [MKS, 66]. L'origine en est le travail de P. Hall [HaP, 33] sur l'étude de certains p-groupes. Il n'est pas question là d'algèbre de Lie, mais de calculs profonds sur les commutateurs itérés et la suite centrale descendante (F_n) du groupe libre. Les travaux fondamentaux de Magnus [Ma, 35] [Ma, 37] et Witt [Wi, 37] "linéarisent" ces calculs en introduisant une structure plus riche que celle de groupe libre : celle d'algèbre de Lie libre. C'est là que Magnus définit l'algèbre de Lie libre $L(X)$ comme sous-algèbre de l'algèbre $\mathbb{K}\langle X\rangle$ des séries formelles en variables non commutatives X sur l'anneau $\mathbb{K}$, introduite auparavant par Hausdorff. Il montre que la filtration naturelle de $\mathbb{K}\langle X\rangle$ définit une suite décroissante de sous-groupes du groupe libre $F(X)$ qui est précisément la suite centrale descendante. Witt complète ces résultats et donne la dimension des com-

posantes homogènes de degré n de L(X) (ou "formules de Witt"). Ces travaux sont à la base de nombreux autres sur la correspondance entre groupes et algèbres de Lie. Citons seulement celui de M. Lazard [La, 54] et les applications importantes dans l'approche du célèbre problème de Burnside pour les groupes.

Un autre théorème important dans la correspondance entre groupes et algèbresde Lie est la "formule de Hausdorff", affirmant que la série z (en variables non commutatives) définie par $e^z = e^x e^y$ est une somme infinie d'alternants (ou éléments homogènes) de l'algèbre de Lie libre engendrée par x et y. Cette formule est jalonnée des noms de Poincaré, Campbell, Pascal, Baker et c'est Hausdorff qui le premier prouvera de manière précise la "formule" en se plaçant dans l'algèbre des séries en variables non commutatives, qui sera reprise plus tard par Magnus [Hau, 06]. Les coefficients de cette série ont été abondamment étudiés depuis. Un calcul ou une expression de ceux-ci dépend de la base de l'algèbre de Lie libre utilisée et met en évidence l'intérêt de trouver de "bonnes" bases. On verra par exemple les calculs sur ordinateurs de Michel jusqu'au degré 11, et dans certains cas au degré 30 [Mi, 74] [Mi, 76]. Un autre exemple d'applications pratiques est celui de la résolution d'équations différentielles, par exemple la solution exponentielle de l'équation différentielle linéaire dans une algèbre de Banach [Ma, 55] [Mi, 74] ou certaines équations de la théorie quantique des champs.

La détermination d'une base de l'algèbre de Lie libre ne semble apparaître pour la première fois que dans l'article de M. Hall [HaM, 50], et est connue sous le nom de "base de Hall". Toutefois cette base est implicitement connue dans les travaux de P. Hall et Magnus cités ci-dessus. Notamment P. Hall définit ce qu'il appelle le "collecting process", c'est-à-dire un procédé de calcul permettant d'écrire de manière unique tout mot du groupe libre comme produit de certains commutateurs, modulo le $n^{\text{ième}}$ groupe de la série centrale descendante. Les commutateurs apparaissant dans ce procédé sont totalement ordonnés et sont appelées commutateurs basiques. Si l'on remplace les parenthèses définissant l'itération des commutateurs

par des crochets de Lie, on obtient alors la base de Hall. Diverses généralisations des bases ou commutateurs basiques de Hall ont été proposées par Meier-Wunderli [MW, 52], Schützenberger [Sc, 58], Širšov [Si, 62], Gorchakov [Go, 69], Ward [Wa, 69]. Un autre procédé pour trouver une base est liée à la notion de mots lexicographiques standards : ce sont les commutateurs basiques de Chen, Fox et Lyndon [CFL, 58] dont la base associée est définie sous une autre forme équivalente par Širšov [Si, 58]. Le premier but de notre travail est de donner une exposition commune à toutes ces différentes constructions de bases d'algèbres de Lie libres. Par souci de simplicité, nous ne parlerons qu'en termes d'algèbres de Lie et laisserons de côté la traduction en termes de "commutateurs basiques" et "collecting process" généralisé.

Cette étude se ramène à celle de certaines familles de mots du monoïde libre, jouissant d'une propriété d'unique factorisabilité, et introduites par Schützenberger [Sc, 65] sous le nom de factorisations du monoïde libre. Il est ainsi surprenant qu'une structure aussi pauvre que le monoïde libre apparaisse comme fondamentale pour l'étude des algèbres de Lie libres.

Une factorisation du monoïde libre X^* est une famille $\mathcal{F} = (Y_j,\ j \in J)$ dans laquelle les Y_j sont des parties de X^* et J un ensemble totalement ordonné, et telle que tout mot f s'écrive de manière unique $f = f_1 \dots f_p$ avec $p \geq 1$, $f_i \in Y_{j_i}$ et $j_1 \geq \dots \geq j_p$. Le théorème principal de ce travail est que pour de "bonnes" factorisations on peut, par un "crochetage" des mots de Y_j, construire un ensemble $[Y_j]$ d'alternants de $L(X)$, en bijection avec Y_j et qui est une famille basique pour la sous-algèbre de Lie libre qu'il engendre. De plus l'algèbre de Lie $L(X)$ est, en tant que module, isomorphe à la somme directe $\bigoplus_j L([Y_j])$. Lorsque $\mathcal{F}$ est une factorisation complète, c'est-à-dire lorsque chaque ensemble Y_j est réduit à un seul élément, on obtient ainsi une base de $L(X)$.

Notre démarche comprend trois étapes. La première consiste à prouver le théorème fondamental dans le cas des bissections, c'est-à-dire des factorisations

pour lequelles J n'a que deux éléments. La deuxième est la définition, l'étude et les différentes caractérisations commodes d'une classe de "bonnes" factorisations. Cette classe est suffisamment vaste pour permettre de retrouver, dans le cas des factorisations complètes, toutes les bases connues des algèbres de Lie libres. La troisième étape est la caractérisation et la preuve de l'équivalence des différents "crochetages" possibles des mots d'une factorisation. Les deux dernières étapes ne font appel qu'à des manipulations de mots du monoïde libre et il n'est plus question là d'algèbre de Lie. Par souci pédagogique, nous avons d'abord fait toute la théorie dans le cas des factorisations complètes. C'est l'objet du chapitre I.

Nous rappelons au paragraphe 1 les notations usuelles ainsi que les définitions des différentes bases connues. La première étape de notre démarche se réduit ici à un cas trivial de bissections et le théorème fondamental devient alors le théorème d'élimination de Lazard [La, 60] [Bo, 72]. Nous en redonnons la preuve au paragraphe 2 . Nous sommes conduit à introduire directement la notion assez technique de <u>factorisation de Lazard</u>. L'avantage est de pouvoir vérifier facilement le théorème fondamental pour cette classe de factorisations. Le paragraphe 3 introduit une généralisation des "<u>ensembles de Hall</u>" tels qu'ils sont définis par le "collecting process" de Hall. Nous montrons que la condition ainsi introduite est une condition nécessaire et suffisante pour que le procédé donne naissance à des bases. Cette condition était déjà connue de Širšov [Si, 62] et a été retrouvée indépendemment de nous par Michel [Mi, 74] . Nous montrons enfin dans ce même paragraphe l'équivalence des ensembles de Hall introduits avec les factorisations de Lazard. Les procédés de définition des bases associées aux factorisations de Lazard étant assez compliqués, nous proposons au paragraphe 4 des critères simples et commodes pour retrouver ces factorisations de Lazard, ainsi que le "crochetage" associé des mots. En particulier nous retrouvons les bases de Chen, Fox, Lyndon [CFL, 58] et de Širšov [Si, 58] et prouvons leur équivalence. En fait la factorisation associée à cette base peut être considérée aussi comme une factorisation de Lazard dans l'autre sens. L'étude de telles factorisations, que nous appelons <u>régulières</u>, constitue le paragraphe 5. Ces factorisations, ainsi que les bases

associées, ont des propriétés remarquables. En particulier, elles sont très commodes pour les calculs sur ordinateur. Par exemple, on verra les calculs de Michel sur la série de Hausdorff et le problème restreint de Burnside [Mi, 76].

Le reste de ce travail est la généralisation du chapitre I pour les factorisations non nécessairement complètes. Les deuxième et troisième étapes mentionnées ci-dessus se répètent à peu près comme au chapitre I. Là aussi on peut introduire les factorisations de Lazard, les ensembles de Hall et les factorisations régulières. C'est l'objet du chapitre III. Nous omettons les démonstrations qui ont leurs analogues au chapitre I. La généralisation correspond au passage entre les bissections triviales et les bissections générales. Par contre, la première étape, qui est la généralisation du théorème d'élimination de Lazard pour les bissections nécessite tout le chapitre II. Pour ceci nous sommes conduits à introduire de nouveaux objets : les bascules. Les bissections apparaissent comme les objets libres de la catégorie des bascules. A toute bascule est associée une algèbre de Lie, qui devient libre lorsque la bascule s'identifie à une bissection. Lorsque la bascule ne "bascule" pas, on retrouve le produit semi-direct d'algèbres de Lie et les bissections triviales. Le paragraphe 1 donne une construction fondamentale des bissections, particulièrement commode pour définir le "crochetage" des mots. Cette construction simplifie une construction antérieure de Schützenberger [Sc, 65]. Le paragraphe 2 expose les préliminaires nécessaires sur les bascules. Enfin le paragraphe 3 prouve le théorème fondamental pour les bissections. Notons que le théorème a aussi un analogue dans l'algèbre enveloppante, ce qui constitue une extension du théorème de Poincaré-Birkhoff-Witt dans le cas des algèbres de Lie libres.

S'il n'existe pas de bases canoniques de $L(X)$, il existe par contre des décompositions canoniques en somme directe de sous-algèbres de Lie libres. Par exemple pour $X = \{x, y\}$ et pour p/q rationnel irréductible, soit $L_{p,q}$ l'algèbre de Lie formée des sommes d'alternants de bidegré mp en x, mq en y avec

$m \geq 1$. Une application de nos méthodes est d'exhiber (au paragraphe 3 du chapitre III) une famille basique de $L_{p,q}$, qui est en bijection avec les "chemins minimaux" du plan $\mathbb{N} \times \mathbb{N}$ situés strictement (sauf aux extrémités) sous la droite de pente q/p. La décomposition de $L(X)$ selon les $L_{p,q}$ correspond en fait à celle relative à une factorisation dite de Spitzer, introduite en théorie des fluctuations de sommes de variables aléatoires [Sp, 56] [Sc, 65]. Dans le cas de deux lettres, il n'y a d'ailleurs qu'une seule factorisation de Spitzer non triviale (à un isomorphisme près). La décomposition de L selon les $L_{p,q}$ donne naissance à des alternants et Foata avait conjecturé qu'ils forment une base. Les chapitres II et III permettent donc de démontrer cette conjecture. Nous appelons cette base, la base de Spitzer-Foata et nous l'introduisons dès la fin du paragraphe 5, chapitre I.

Ainsi nous voudrions que ce travail soit une illustration de certaines idées de Schützenberger menant à penser que certains phénomènes ou identités remarquables apparaissant dans des structures algébriques ou combinatoires sont le reflet de propriétés naturelles des mots du monoïde libre, et qu'il n'est donc pas sans intérêt de développer toute une étude algébrique et combinatoire de ces mots.

D'ailleurs les factorisations introduites dans ce travail sont des objets liés à d'autres théories complètement étrangères aux algèbres de Lie. Par exemple, il est touchant d'observer que les factorisations de Lazard liées aux bases classiques de Hall se retrouvent définies à des fins statistiques dans un article de Good [Go, 71] ou encore en théorie des codes dans [Sh, 68]. Là Scholtz donne une construction de codes "comma-free" maximaux dont le cardinal est exactement la dimension de la composante homogène de degré n de l'algèbre de Lie, et redémontre ainsi après Eastman une conjecture de Golomb, Gordon et Welch. La construction de Scholtz, comme celle de Good, est celle de la factorisation de Lazard associée aux bases classiques de Hall. En théorie des fluctuations des sommes de variables aléatoires déjà citée ci-dessus, le principe d'équivalence de Sparre Andersen est une certaine propriété de réarrangement relative à une classe particulière de bissections, comme l'ont montré Foata et Schützenberger [FS, 71]. Un autre théorème de

réarrangement est celui de l'égalité des distributions des "montées" et des "excédances" parmi les suites avec répétitions. Les premières bijections de réarrangement ont été mises en évidence par Foata [Fo, 65]. Chacune d'elle est définie à partir d'une factorisation complète vérifiant une condition appelée "spéciale". Notons que les factorisations régulières du paragraphe 5, chapitre I, sont des factorisations spéciales. Dans ces bijections les mots de la factorisation jouent le même rôle que les cycles pour les suites sans répétitions, ou permutations. Cette étude sera reprise sous une forme plus élégante par Cartier et Foata [CF, 69]. Il est enfin assez curieux que les bascules et bissections du chapitre II sont des objets de la théorie des automates et langages développée en Informatique théorique. Les bascules apparaissent en effet comme une généralisation de la notion d'automate, et jouent vis-à-vis des langages linéaires le rôle que jouent les automates finis vis-à-vis des langages rationnels. Ils sont équivalents à la notion "d'automate ordonné". On peut développer une théorie de ces objets, similaire à celle des monoïdes syntactiques des codes préfixes rationnels (voir [Vi, 74]).

Les résultats de ce travail avait déjà été annoncés précédemment par trois notes aux Comptes rendus [Vi, 73] ainsi que par des exposés [Vi, 72] [Vi, 74'] [Vi, 74"]. On trouvera les preuves complètes du chapitre III dans la thèse de l'auteur [Vi, 74]. Indépendamment de nous, Michel [Mi, 74] a retrouvé plus tard l'équivalence entre les ensembles de Hall tels qu'ils sont définis au paragraphe 3, chapitre I et la condition (v') de la proposition 1.8 caractérisant les factorisations de Lazard. Il prouve alors directement par un argument de développement que ces ensembles génèrent des bases de l'algèbre de Lie.

Je remercie sincèrement Pierre Cartier de m'avoir fait l'honneur de s'être intéressé dans les détails à mon travail. C'est avec joie que je remercie ici Marcel Paul Schützenberger. Il est à l'origine de ma thèse et de ce présent travail qui s'appuie sur certains de ses travaux personnels. Il fut et est toujours pour moi plus qu'un "bon maître". Enfin la forme définitive de ce mémoire n'aurait pas vu le jour sans les encouragements, l'aide et le dévouement de Dominique Foata.

La frappe a été réalisée par Sylvie Lutzing du Centre de Calcul de l'Esplanade de Strasbourg, que je remercie également.

CHAPITRE I

BASES DES ALGÈBRES DE LIE LIBRES.

1. Notations et bases usuelles.

Le lecteur pourra se reporter à [Ja, 62] pour les notions générales d'algèbre de Lie et d'algèbre enveloppante, ainsi qu'à [Bo, 72] pour les algèbres de Lie libres et les bases de Hall.

Notations générales. Dans tout ce travail $\mathbb{K}$ désigne, sauf mention expresse du contraire, un anneau commutatif non réduit à 0 et dont l'élément unité est noté 1. Si E est un ensemble, $|E|$ désigne son cardinal.

Soit P_n, $n \geq 1$ une suite de parties de E. Nous notons $\overline{P}_n$ la suite définie par :

$$\overline{P}_n = \bigcup_{1 \leq i \leq n} P_i \ .$$

Pour $P \subset E$, on note $E \setminus P = \{u \in E \ , \ u \notin P\}$.

Monoïde et magma libre. Soit X un ensemble non vide. Nous désignons par $M(X)$, X^+, X^* respectivement le magma libre, demi-groupe libre, monoïde libre engendré par X, c'est-à-dire la structure libre engendrée par X relativement, respectivement à une loi de composition, une loi de composition associative, une loi de composition associative avec élément neutre.

Les éléments de X^* sont appelés aussi mots sur l'alphabet X. La loi de composition de X^* est la "concaténation" des mots et e désigne l'élément neutre de X^*, c'est-à-dire le mot vide n'ayant aucune lettre. En fait X^+ est $X^* \setminus \{e\}$, le monoïde libre privé du mot e.

Les éléments de $M(X)$ sont les "mots parenthésés" munis de la loi de composition :

$$u \in M(X) , \quad v \in M(X) \to h = (u, v) \in M(X) .$$

Nous notons $\lambda h = u$ et $\rho h = v$.

Nous désignons par δ l'application canonique $M(X) \to X^*$ de "déparenthésage" des mots, c'est-à-dire l'unique morphisme de magma dont la restriction à X est l'identité.

EXEMPLE.

$$\delta((x, x) , (y, (x, y))) = x^2 y x y \in \{x, y\}^* .$$

Pour $f \in X^*$ (resp $f \in M(X)$), nous notons $|f|$ la longueur (ou degré) de f. C'est l'unique morphisme $f \to |f|$ de monoïde $X^* \to \mathbb{N}$ (resp. de magma $M(X) \to \mathbb{N}$) tel que $|f| = 1$ pour tout $f \in X$.

Nous notons $M_n(X)$ (resp X^n) l'ensemble des éléments de $M(X)$ (resp X^*) de longueur n.

Sous-monoïde libre et conjugaison. Si A et B sont deux parties de X^*, le produit AB est :

$$AB = \{f \in X^*, \ f = ab, \ a \in A, \ b \in B\}$$

Le sous-monoïde engendré par A est noté encore A^*, soit :

$$A^* = \bigcup_{i \geq 0} A^i .$$

Lorsqu'une confusion est à craindre, nous noterons $Mo(A)$ le monoïde libre engendré par A.

Tout sous-monoïde M de X^* admet un et un seul système minimal de générateurs. Le sous-monoïde M sera un sous-monoïde libre ssi il est librement engendré par son système minimal de générateurs A, c'est-à-dire si A vérifie :

$$\forall a_1, \ldots, a_p \in A, \quad \forall b_1, \ldots, b_q \in A,$$
$$a_1 a_2 \cdots a_p = b_1 b_2 \cdots b_q \Rightarrow p = q \text{ et } a_1 = b_1, \ldots, b_p = b_q$$

On dit que A est la base de M ou encore que A est un code sur X.

Soit $f = uvw$ un mot de X^*. Le mot v (resp u, resp w) est dit facteur de f (resp facteur gauche, resp facteur droit). Si ces mots sont distincts de f, ils sont dits facteurs propres.

Deux mots f et g de X^* sont dits conjugués ssi on peut écrire :

$$f = uv, \quad g = vu \text{ avec } u \in X^*, \quad v \in X^* .$$

Si u et v sont distincts de e, g est dit conjugué propre de f. La relation de conjugaison est une relation d'équivalence. Si un mot f d'une classe d'équivalence

est primitif, c'est-à-dire s'il ne peut s'écrire $f = u^p$ avec $p > 1$, alors tous les autres le sont. On peut ainsi parler de classes primitives de conjugaison. Si X est un alphabet à q lettres, le nombre $\ell_q(n)$ de ces classes de longueur n est donné par la formule classique :

$$\ell_q(n) = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}$$

où d parcourt les diviseurs de n, et où μ est la fonction de Moebius habituelle :

$\mu(1) = 1$

$\mu(n) = 0$ si n est divisible par un carré

$\mu(n) = (-1)^r$ si r est le nombre de facteurs premiers tous distincts dans la décomposition de n.

Algèbre associative et algèbre de Lie libre. Nous désignons par $\mathbb{K}\langle X\rangle$ l'algèbre associative libre sur l'anneau $\mathbb{K}$ engendrée par X, c'est-à-dire l'algèbre des polynômes en variables non commutatives X. Cette algèbre est un module libre de base X^*, totalement graduée par les degrés.

Rappelons qu'une algèbre de Lie $\mathfrak{L}$ est une algèbre dont la loi multiplicative notée $[u, v]$ vérifie :

(i) $\quad \forall\, u \in \mathfrak{L},\ [u, u] = 0$

(ii) $\quad \forall\, u, v, w \in \mathfrak{L}\ [[u, v], w] + [[v, w], u] + [[w,u], v] = 0$.

Soit $\mathfrak{A}$ une algèbre associative et $\mathfrak{A}_L$ l'algèbre dont le module sous-jacent est celui de $\mathfrak{A}$ et dont la loi multiplicative est le crochet de Lie $[u, v] = uv - vu$. Alors $\mathfrak{A}_L$ est une algèbre de Lie.

Réciproquement, pour une algèbre de Lie $\mathfrak{L}$ sur $\mathbb{K}$, nous notons $\mathfrak{A}\mathfrak{L}$ l'algèbre (associative) enveloppante de $\mathfrak{L}$, c'est-à-dire en fait un couple $(\mathfrak{A}, i)$

avec $\mathfrak{A}$ une algèbre associative et i un morphisme de $\mathfrak{L}$ dans $\mathfrak{A}_L$ tel que : pour toute algèbre $\mathfrak{U}$ et morphisme $\theta : \mathfrak{L} \to \mathfrak{U}_L$, il existe un unique morphisme $\theta' : \mathfrak{A} \to \mathfrak{U}$ tel que $\theta = \theta' \circ i$. Le foncteur $\mathfrak{L} \to \mathfrak{A}\mathfrak{L}$ est un adjoint du foncteur $\mathfrak{A} \to \mathfrak{A}_L$.

Nous notons $L(X)$ l'algèbre de Lie libre sur $\mathbb{K}$ engendrée par X. Les objets $\mathbb{K}\langle X\rangle$ et $L(X)$ peuvent aussi être définis par le fait que les foncteurs $X \to \mathbb{K}\langle X\rangle$ et $X \to L(X)$ sont des adjoints des foncteurs "d'oubli" des catégories correspondantes, associant à un objet son ensemble sous-jacent. Ainsi d'après la propriété de composition des foncteurs adjoints, l'algèbre $\mathbb{K}\langle X\rangle$ est l'algèbre enveloppante de $L(X)$.

La méthode d'élimination de M. Lazard que nous rappellerons à la proposition 1.1 permet d'affirmer que $L(X)$ est un $\mathbb{Z}$-module libre, et d'identifier $L(X)$ avec la sous-algèbre de Lie engendrée par X dans l'algèbre de Lie $\mathbb{K}\langle X\rangle_L$. Les polynômes de $\mathbb{K}\langle X\rangle$ qui appartiennent à $L(X)$ sont appelés aussi éléments de Lie.

Notons $\psi : M(X) \to L(X)$ l'application canonique, unique morphisme de magma (pour le crochet de Lie) coïncidant avec l'identité sur X. L'image d'un élément de longueur n de $M(X)$ est appelé alternant de degré n de $L(X)$. Ceux-ci engendrent le $\mathbb{K}$-module libre $L_n(X)$ et $\{L_n(X),\ n \geq 1\}$ est une graduation totale de $L(X)$. Si X est fini de cardinal q, les classiques formules de Witt donnent la dimension de $L_n(X)$, soit :

$$\ell_q(n) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{n/d}.$$

Si $\mathfrak{L}$ est une sous-algèbre de Lie libre de $L(X)$, une partie Y de $\mathfrak{L}$ est appelée famille basique de $\mathfrak{L}$ lorsque Y engendre librement $\mathfrak{L}$ (en tant qu'algèbre de Lie). Rappelons que lorsque $\mathbb{K}$ est un corps, toute sous-algèbre de Lie de $L(X)$ est libre, d'après un théorème de Širšov-Witt.

Par contre ceci n'est pas vrai pour les algèbres associatives (voir

[Co, 71, § 6.7]) . Ici aussi nous parlerons de famille basique d'une sous-algèbre associative libre de $\mathbb{K}\langle X\rangle$.

Enfin, rappelons que pour une algèbre de Lie $\mathfrak{L}$, l'application $y \to [x, y] \in \mathfrak{L}$ est une dérivation de $\mathfrak{L}$ notée ad. x .

Bases de Hall de L(X). Les bases de Hall constitutent les bases les plus connues de L(X) et ont été en fait définies par P. Hall [HaP, 33] en termes de commutateurs basiques du groupe libre apparaissant dans le "collecting process". Ces bases sont définies de la façon suivante (voir [Ma, 37], [HaM, 50], [HaM, 59], [La, 60], [MKS, 66], [Bo, 72]) :

Soit H une partie du magma libre M(X) , totalement ordonnée par la relation $\leq$, et vérifiant les trois conditions :

- (Ha_1) $X \subset H$
- (Ha_2) $\forall h = (u, v) \in M(X) \setminus X$, $h \in H$ ssi on a les 3 conditions suivantes :
  - $u \in H$, $v \in H$
  - $u < v$
  - $v \in X$ ou bien $v = (v', v'')$ avec $v' \leq u$
- (Ha'_3) $\forall u \in H$, $\forall v \in H$, $|u| < |v| \Rightarrow u < v$
- Alors la famille $\{\psi h , h \in H\}$ est une base de L(X) , appelée base de Hall.

EXEMPLE 1.1 . On peut construire les ensembles H vérifiant les conditions (Ha_1) (Ha_2) et (Ha'_3) (appelés aussi ensembles de Hall dans [Bo, 72]), par récurrence sur les degrés. Une construction possible pour les degrés ≤ 4 avec un alphabet $X = \{x, y, z\}$ de 3 lettres est la suivante (les éléments de chaque ensemble $H_i = H \cap M_i(X)$ sont ordonnés dans l'ordre de leur écriture de gauche à droite):

H_1	x	y	z
H_2	(x, y)	(x, z)	(y, z)

H_3 (x, (x, y)) (x, (x, z)) (y, (x, y)) (y, (x, z)) (y, (y, z))
(z, (x, y)) (z, (x, z)) (z, (y, z))

H_4 (x, (x, (x, y))) (x, (x, (x, z))) (y, (x, (x, y))) (y, (x, (x, z)))
(y, (y, (x, y))) (y, (y, (x, z))) (y, (y, (y, z))) (z, (x, (x, y)))
(z, (x, (x, z))) (z, (y, (x, y))) (z, (y, (x, z))) (z, (y, (y, z)))
(z, (z, (x, y))) (z, (z, (x, z))) (z, (z, (y, z))) ((x, y) , (x, z))
((x, y), (y, z)) ((x, z) , (y, z))

REMARQUE 1.1 . Meier-Wunderli [MW, 52] a donné une généralisation des bases de Hall en montrant que ΨH est toujours une base de $L(X)$ lorsque l'on remplace la condition (Ha'_3) par :

- (Ha''_3) $\forall u \in H$, $\forall v \in H$, $(u, v) \in H \Rightarrow u < (u, v)$ et $v < (u, v)$.

La preuve est écrite en fait en termes de commutateurs basiques . On verra aussi pour d'autres interprétations des bases de Hall [Sc, 58], [Si, 62], [Sc, 71] .

Base de Chen-Fox-Lyndon. Cette base a été introduite par Chen, Fox et Lyndon [CFL, 58] ; on verra aussi [Ly, 54], [Si, 62], [Fo, 65] .

Supposons X totalement ordonné et soit $\leq$ l'ordre lexicographique correspondant sur X^+ . Soit F l'ensemble (contenant l'alphabet X) des mots de X^+ strictement inférieurs à tous leurs conjugués propres :

$$F = \{f \in X^+ , \forall u \in X^+ , \forall v \in X^+ , f = uv \Rightarrow f < vu\} .$$

Les mots de F sont appelés aussi mots lexicographiques standards.

Pour $f \in F$, l'ensemble (non vide) des mots $u \in F$ tels que $f = uv$ pour un certain $v \in X^+$, admet un élément de longueur maximum f' , soit $f = f'f''$.

Alors un lemme (voir [CFL, 58] ou la suite de ce chapitre) prouve que $f'' \in F$. On peut donc définir une application $\Pi : F \to M(X)$ par récurrence sur les degrés :

$\forall x \in X$, $\Pi x = x$ et pour tout $f = f'f'' \in F$ comme ci-dessus,

$$\Pi f = (\Pi f', \Pi f'').$$

Alors la famille $\{\psi \circ \Pi (f), f \in F\}$ est une base de $L(X)$ appelée <u>base de Chen-Fox-Lyndon</u> (relativement à l'ordre de X).

EXEMPLE 1.2. Soit $X = \{x, y\}$ de cardinal 2, ordonné par $x < y$. Les mots de F de longueur ≤ 5 sont les suivants :

$F \cap X$	x	y				
$F \cap X^2$	xy					
$F \cap X^3$	x^2y	xy^2				
$F \cap X^4$	x^3y	x^2y^2	xy^3			
$F \cap X^5$	x^4y	x^3y^2	x^2yxy	x^2y^3	$xyxy^2$	xy^4

Les éléments de degré ≤ 5 de la base de Chen-Fox-Lyndon correspondante sont alors :

x	y	
$[x, y]$		
$[x, [x, y]]$	$[[x, y], y]$	
$[x, [x, [x, y]]]$	$[[x, [x, y]], y]$	$[[[x, y], y], y]$
$[x, [x, [x, [x, y]]]]$	$[[x, [x, [x, y]]], y]$	$[[x, [x, y]], [x, y]]$
$[[[x, [x, y]], y], y]$	$[[x, y], [[x, y], y]]$	$[[[[x, y], y], y], y]$

Base de Širšov. Cette base a été introduite par Širšov en [Si, 58] et est en fait identique, à des symétries près sur les ordres, à celle de Chen-Fox-Lyndon, comme nous le verrons dans la suite de ce chapitre. Nous redonnons ici la formulation originale de Širšov.

Soit X totalement ordonné et $\leq$ la relation d'ordre total sur X^+ définie par les deux conditions :

(1.1) $\forall u, v, w \in X^*$ et $\forall x, y \in X$ tels que $x < y$, on a
$uxv < uyw$ et $u > uv$.

On note F' l'ensemble des mots de X^+ strictement plus grands que chacun de leurs conjugués propres (c'est-à-dire en fait l'ensemble des mots lexicographiques standards pour l'ordre opposé sur X) .

Un lemme de Širšov permet de dire : tout mot $f \in X^+$ se factorise de manière unique $f = f_1 \dots f_p$ avec $f_i \in F'$ et $f_1 \leq f_2 \leq \dots \leq f_p$.
Nous définissons une application $\Pi' : F' \to M(X)$ par récurrence sur les degrés :

- $\forall x \in X$, $\Pi' x = x$
- $\forall f \in F' \setminus X$, f s'écrit de manière unique
  $f = g_1 \dots g_q x$ avec $x \in X$, $g_i \in F'$, $g_1 \leq \dots \leq g_q$
  alors $\Pi' f = (\Pi' g_1, (\Pi' g_2, \dots, (\Pi' g_q, x)) \dots)$

La famille $\{\psi \circ \Pi'(f),\ f \in F'\}$ est une base de $L(X)$.

Nous verrons que cette base est identique à celle de Chen-Fox-Lyndon (associée à l'ordre opposé de X) en prouvant que $\Pi' = \Pi$.