SÉMINAIRE DUBREIL.
ALGÈBRE ET THÉORIE
DES NOMBRES

MARCEL P. SCHÜTZENBERGER

Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, nº 1 (1958-1959), exp. nº 1, p. 1-23
<http://www.numdam.org/item?id=SD_1958-1959__12_1_A1_0>

Faculté des Sciences de Paris
-:-:-:-

Séminaire P. DUBREIL
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1958/59
-:-:-:-

10 novembre 1958

SUR UNE PROPRIÉTÉ COMBINATOIRE DES ALGÈBRES DE LIE LIBRES POUVANT ÊTRE UTILISÉE DANS UN PROBLÈME DE MATHÉMATIQUES APPLIQUÉES

par Marcel P. SCHÜTZENBERGER

INTRODUCTION. - Le but de ces notes est de signaler la possibilité d'utiliser, dans un problème de Mathématiques appliquées ([1]), certaines propriétés combinatoires élémentaires des bases de Marshall HALL des algèbres de Lie libres.

Dans la section I, on rappelle divers résultats fondamentaux de Marshall HALL [9] et de ŠIRŠOV [17].

Dans la section II, on vérifie les propriétés cherchées, qui permettent d'ailleurs de donner une démonstration nouvelle d'un théorème de MEIER WUNDERLI [16].

Dans la section III, on complète les considérations précédentes en montrant que la méthode de Birkhoff donne une démonstration très simple de l'indépendance des bases de Marshall HALL.

Dans la section IV, on vérifie que le calcul des "shuffles" de CHEN, FOX et LYNDON [2], ou plutôt un cas particulier de celui-ci, s'applique encore aux bases considérées ici.

Je remercie M. JAZARD pour de nombreuses et utiles discussions.

([1]) consistant à construire des sous-demi-groupes (sous-monoïdes) G du demi-groupe (monoïde) libre F satisfaisant les deux conditions :

$\mathfrak{U}_z$: pour tout f, $f' \in F$, si ff', $f'f \in G$ alors f, $f' \in G$.

$\mathfrak{N}_\ell$: pour tout $f \in F$, $Ff \cap G \neq \emptyset$.

(G est "net à droite" selon la théorie de P. DUBREIL, cf. [3], [4], [5], [6]).

La signification de ce problème est discutée dans [8] et surtout dans [15], ce dernier ouvrage contenant une bibliographie très complète de la question, apparemment insoupçonnée des auteurs de [8].

I. Résultats préliminaires

I.1. Définitions préliminaires.

Soient A un ensemble, $D = D(A)$ le système algébrique libre à une seule opération (ne satisfaisant aucune identité) sur A (cf. [10]). Par définition, $D = A \cup D^+$, où D^+ est construit par induction comme l'ensemble des symboles $d = [d' , d'']$ avec $d' , d'' \in D$. On dira que d' (resp. d'') est le composant gauche (resp. droit) d'ordre un de d ; d sera le composant d'ordre zéro de soi-même.

Un composant gauche (resp. droit) d'ordre α d'un composant (gauche ou droit) d'ordre α' de d sera un composant gauche (rep. droit) d'ordre $\alpha + \alpha'$ de d.

Pour tout sous-ensemble $X \subset D$, on désignera par $\mathfrak{F}(X)$ le sous-demi-groupe (sous-monoïde) engendré par X du demi-groupe libre $S = \mathfrak{F}(D)$ engendré par D. 1 désignera l'élément neutre de S.

Soit $s = d_1\, d_2 \dots d_i \dots d_n$ un élément de S factorisé de la façon indiquée en un produit d'éléments de D. On pose :

$$\delta_j\, s = s\,, \quad \text{si} \quad j \neq 1, 2, \dots, i, \dots, n \quad \text{ou si} \quad d_j \in A\,;$$

$$\delta_i\, s = d_1\, d_2 \dots d_{i-1}\, d'\, d''\, d_{i+1} \dots d_n \quad \text{si} \quad d_i = [d' , d''] \,.$$

Les δ_j engendrent de façon naturelle un demi-groupe $\Delta = \{\delta\}$ d'opérateurs de S dans lui-même ; si $s' = \delta s$, on dira que s' est une décomposition de s. Les facteurs de s' sont, de façon bien déterminée (pour δ fixé) des composants des facteurs de s, ou, pour abréger, des composants de s.

Réciproquement on pose

$$\delta_j^{-1}\, s = s\,, \quad \text{si} \quad s \in D \quad \text{ou si} \quad j \neq 1, 2, \dots, n$$

$$\delta_1^{-1}\, s = [d_n , d_1]\, d_2 \dots d_i \dots d_n\,, \quad \text{quand} \quad j = 1$$

et dans les autres cas :

$$\delta_i^{-1}\, s = d_1 \dots d_{i-2}\, [d_{i-1} , d_i]\, d_{i+1} \dots d_n$$

$\delta_i^{-1}\, s$ est une recomposition de s.

Tout $s \in S$ possède une décomposition unique notée $\delta^* s$ qui est un élément de $F (= \mathfrak{F}(A))$; δ^* est donc un endomorphisme de demi-groupe $S \to F$. Le degré $|s|$ de s est la longueur de $\delta^* s$.

Pour tout ~~sous-ensemble~~ $X \subset S$ on pose

$$\mathcal{Z}_p(X) = \{ s \in \mathfrak{F}(X) : s = x^p \ (x \in X) ; s \notin \mathcal{Z}_{p' > p}(X) \}$$

et

$$\mathcal{Z}(X) = \bigcup_{1 \leq p < \infty} \mathcal{Z}_p(X) .$$

Si $s' = d_j d_{j+1} \dots d_n d_1 d_2 \dots d_{j-1}$ se déduit de $s = d_1 d_2 \dots d_j \dots d_n$ par une permutation circulaire de ses facteurs, s et s' seront dits π-conjugués ([2]).

Manifestement si $s \in \mathcal{Z}_p(S)$ il en est de même de tous les éléments de sa π-classe (c'est-à-dire : de l'ensemble des éléments π-conjugués de s).

I.2. Monômes standards.

On suppose donnée une fois pour toute une relation d'ordre total $<$ sur D satisfaisant :

(H0) : si d' est un composant (gauche ou droit) d'ordre ≥ 1 de d, alors $d' < d$.

On définit par induction un sous-ensemble $H = H(A)$ de D par les règles suivantes :

$A \subset H$ et si $d = [d', d''] \in D^+$, $d \in H$ si et seulement si

(H1) $\qquad d', d'' \in H$

(H2) $\qquad d' > d''$

([2]) La relation de π-conjugaison introduite ici n'est évidemment rien d'autre que la restriction à S de la relation habituelle de conjugaison du groupe libre engendré par D. On notera que s et s' sont π-conjugués si et seulement s'il existe $s'' \in S$, tel que $ss'' = s''s'$. La théorie générale de ces équivalences est faite par R. CROISOT dans [3].

(H3) ou bien $d' \in A$ ou bien, si $d' = [d''', d^{IV}]$, $d^{IV} \leq d''$.

Ces définitions sont celles de Marshall HALL, sauf (H0) qui remplace la condition un peu plus stricte :

(H0)' si $|d'| < |d|$, alors $d' < d$ (cf. [9]).

Après ŠIRŠOV [17], on considère une partition $H = Q \cup P$ telle que $q < p$ pour tout $q \in Q$, $p \in P$. On appellera "partion de Širšov" toute partition de H satisfaisant cette condition.

A l'intérieur de P, on distingue le sous-ensemble

$$K = \{p \in P : p \in A \text{ ou } p = [d', d''] \text{ avec } d'' \in Q\}$$

Dans tout le reste de ces notes, sauf mention expresse du contraire, on supposera fixés une fois pour toutes P et Q. Les cas le plus intéressant sont évidemment ceux où $Q = H$ et $P = K = \emptyset$; ou, à l'opposé, où $Q = \emptyset$ $P = H$ et $K = A$.

PROPRIÉTÉ I.1. - Soit d_i un facteur de $s = d_1 \dots d_i \dots d_n$ où s est une décomposition d'un élément $\bar{s} \in \mathfrak{F}(H)$

1° $s \in \mathfrak{F}(H)$

2° si d_i est un composant gauche d'un facteur de $\bar{s}$, $d_i > d_{i+1}$.

3° si d_i est un composant droit d'un facteur h_j de $\bar{s}$ ou bien $d_{i-1} \leq d_i$ ou bien $d_{i-1} > d_i$ et alors $[d_{i-1}, d_i]$ est un composant de h_j.

DÉMONSTRATION. - Le 1° est une conséquence immédiate de (H1). Supposons le 2° et le 3° déjà établis pour s, et montrons qu'ils sont encore vrais pour $\delta_i s = d_1 d_2 \dots d_{i-1} d' d'' d_{i+1} \dots d_n$. Les seuls cas à considérer sont évidemment :

- d', d'' : d'après (H2), $d' > d''$, d' et d'' sont respectivement des composants gauches et droits d'un certain facteur h_j de $\bar{s}$ dont, par hypothèse, $d_i = [d', d'']$ est un composant (écentuellement d'ordre zéro !) ;

- si d_{i-1} (resp. d_{i+1}) est un composant droit (resp. gauche) ou d'ordre zéro le résultat subsiste ;

- si d_{i-1} est un composant gauche : par induction $d_{i-1} > d_i$ et, a fortiori, $d_{i-1} > d'$ d'après (H0) ;

- si d_{i+1} est un composant droit : on a toujours $d'' \leq d_{i+1}$, car, ou bien $d_i < d_{i+1}$, et a fortiori $d'' < d_{i+1}$ ou bien $d_i > d_{i+1}$; par induction, $[d_i , d_{i+1}]$ est un composant d'un certain $h_j \in H$ et l'on a $d'' \leq d_{i+1}$ d'après (H3).

On observera que l'énoncé subsiste si l'on suppose que les indices sont pris modulo la longueur du mot considéré (c'est-à-dire $d_{i+1} = d_1$ quand $i = n$, et $d_{i-1} = d_n$ quand $i = 1$).

Considérons en particulier $h \in H$ et ce que nous appellerons sa décomposition normale (à gauche) d'ordre p :

$$s = \delta_1^p h = \delta_1(\delta_1^{p-1} h) = h_1^* h_2 \dots h_{p+1}$$

h_{p+1} étant le composant droit (d'ordre 1) de h ; h_p, le composant droit (d'ordre 1) du composant gauche (d'ordre 1) de h, etc.

h_1^* est par définition le composant "d'extrême gauche" d'ordre p de h.

En appliquant la propriété 1, on obtient immédiatement

$$h_1^* > h_2 \leq h_3 \leq \dots \leq h_{p+1} .$$

Tenant compte de (H0) et du fait que tout composant propre c'est-à-dire d'ordre $\neq 0$), non d'extrême gauche de h, est composant de l'un des h_i $(2 \leq i \leq p + 1)$ il en résulte que seuls les composants d'extrême-gauche de h peuvent être en relation $\gg$ avec son composant droit d'ordre un.

PROPRIÉTÉ I.2. (ŠIRŠOV). - Tout $p \in P$ admet une et une seule décomposition dont tous les facteurs appartiennent à K. Inversement, tout $p \in P$ appartient à K, si et seulement si aucun de ses composants propres, non d'extrême gauche, appartient à K.

DÉMONSTRATION.

1° si $h \in A$, la propriété est trivialement vérifiée. Soit donc $p = [h' , h'']$; si $p \in K$, $h'' \in Q$, et comme toute décomposition de p admet comme facteurs ceux d'une décomposition de h'', p ne peut pas être décomposé de la façon indiquée ; si $p \notin K$, $h'' \in P$ et a fortiori (d'après (H2)) $h' \in P$; par induction chacun des facteurs de $\delta_1 p = h'h''$ admet une décomposition du type indiqué.

2° Si $p \in P$ admet un composant propre non d'extrême-gauche k appartenant à K, le composant droit d'ordre un, h'' de p est tel que $h'' \geq k$; donc $h'' \in P$ et $p \notin K$.

3° Supposons déjà établi que pour tous les $p' \in P$ tels que $|p'| < |p|$, $p' \in K$ si aucun des composants non d'extrême-gauche de p', appartient à K, et soit $p = [h' , h'']$ ayant cette propriété; celle-ci est encore vérifiée pour h'' donc (par l'hypothèse d'induction), h'' lui-même appartiendrait à K s'il appartenait à P, comme ceci est exclu par hypothèse, $h'' \in Q$ et donc $p \in K$.

PROPRIÉTÉ I.3. – Si $P \neq \emptyset$ à tout $q \in Q$ il correspond au moins un $k \in K$ dont q est un composant d'extrême-droite.

DÉMONSTRATION. – D'après la propriété 2, $P \neq \emptyset$ entraîne $K \neq \emptyset$. Le résultat est trivialement vrai quand $K \cap A \neq \emptyset$ ou quand K contient un $k = [k_1' \, k_1]$ avec $k_1 \leq q$ car, d'après (H3), $[k , q] \subset H$ (et donc $[K , q] \in K$) puisque $k > q$. Considérons $k \in K$, quelconque et une décomposition "<u>normale à droite</u>" de k :

$$k = h_1' \, h_2' \, \dots \, h_i' \, h_i^* \quad \text{avec} \quad k = [h_1' \, h_1] \; ; \quad h_1^* = [h_2' \, h_2^*] \; ; \quad h_{i-1}^* = [h_i' \, , \, h_i^*]$$

Supposons le résultat déjà établi pour tous les $q' \in Q$ tels que $h_i^* \leq q'$ où h_i^* est le plus petit (selon $\leq$) composant d'extrême-droite de h tel que $h_i^* > q$:

Si $h_i^* \in A$, $q_1 = [h_i , q] \in H$ d'après (H3) ;

Si $h_i^* = [h_{i+1}' , h_{i+1}^*]$, par hypothèse $h_{i+1}^* \leq q$ et donc, encore d'après (H3), $q_1 = [h_i^* , q] \in H$.

Dans les deux cas, $q_1 > h_i^*$ et q_1 admettant q comme composant droit d'ordre un, le résultat est établi par induction.

REMARQUE I.1. – Il résulte de la propriété I.2 qu'à tout $d \in \mathfrak{F}(D(P))$ ($D(P)$: l'ensemble des éléments de D admettant une décomposition dont tous les facteurs sont dans P), correspond une et une seule décomposition que l'on notera $\delta_P \, d$ et dont tous les facteurs sont dans K.

Après ŠIRŠOV, on dira que d et d' ($d , d' \in \mathfrak{F}(D(P))$) ont le même "P-contenu" si $\gamma \delta_P \, d = \gamma \delta_P \, d'$ où γ désigne l'homomorphisme canonique (de demi-groupe) de $\mathcal{F}(K)$ dans le demi-groupe commutatif libre engendré par K.

Manifestement, si d et d' ont le même P-contenu, d et d' ont aussi le même P'-contenu pour toute partition de Širšov : $H = Q' \cup P'$, telle que $P' \supset P$. On dira que d est en relation ρ_P avec d' quand :

1° d et d' ont le même P'-contenu pour tout $P' \supset P$, $P' \neq P$

2° si $\gamma \delta_P d = k_1^{n_1} k_2^{n_2} \ldots k_m^{n_m} \ldots$; $\gamma \delta_P d' = k_1^{n'_1} k_2^{n'_2} \ldots k_m^{n'_m} \ldots$ où $k_1 < k_2 < k_3 < \ldots < k_m < \ldots$ sont les éléments de K et si pour un certain m :

$$n_m > n'_m \quad \text{et} \quad \sum_{i=m+1}^{\infty} n_i = \sum_{i=m+1}^{\infty} n'_i$$

ρ_P est une relation de préordre et la relation $\gg$ définie par

$$d \gg d'$$

si et seulement s'il existe une partition de Širšov $H = Q'' \cup P''$ telle que $d \, \rho_{P''} \, d'$ est une relation d'ordre total sur D.

On notera que $d \, \rho_P \, d'$ entraîne $[d , d''] \, \rho_P \, [d' , d''']$ pour toutes les paires d'', $d''' \in D(P)$ ayant le même P-contenu.

REMARQUE I.2. - Il sera commode d'utiliser la notation suivante : la paire (h , h') sera dite "légale" si :

1° $h , h' \in Q \cup K$

2° ou bien $h \leq h'$, ou bien $[h , h'] \in Q \cup K$, ou bien $h , h' \in K$.

On utilisera le fait que si (h , h') est légale, il en est de même pour (h , h''), quand $h' \leq h''$ et $h'' \in Q \cup K$.

En effet, puisque $h \in Q \cup K$:

- si $h'' \in K$: ou bien $h \leq h''$ ou bien $h \in K$

- si $h'' \in Q$: ou bien $h \leq h''$ ou bien $h > h''$, et alors soit $h \in A$, soit $h = [h''' , h^{iv}]$ avec $h^{iv} \leq h'$, donc $h^{iv} \leq h''$; dans les deux cas,

$$[h , h''] \in H$$

et d'après la propriété 2

$$[h , h''] \in Q \cup K .$$

II. Théorème de Meier-Wunderli.

II.1. Recompositions légales.

Soit $s = h_1 h_2 \dots h_i \dots h_n$; $s \in \mathcal{F}(H)$.

s sera dit "légal" (resp. π-légal, resp. complètement légal) si toutes les paires (h_{i-1}, h_i), avec $i = 2, \dots, n$ (resp. avec $i = 1, 2, \dots, n$, les indices étant pris modulo n ; resp. toutes paires $(h_i, h_{i'})$ avec $i < i'$), sont légales.

Manifestement, s est π-légal si et seulement si $s^2 = ss$ est légal ou, de façon équivalente, si tous les éléments de sa π-classe sont légaux.

On notera les cas particuliers suivants qui définissent en même temps des notations utilisées plus loin :

1° Tous les mots de F, $T = \mathcal{F}(K)$; $\mathcal{X}(Q)$ sont à la fois π-légaux et complètement légaux.

2° Soit $V \in \mathcal{F}(Q)$ l'ensemble des Q-mots non décroissants ($v \in V$; si $v = e$ ou si $v \in Q$ ou si $v = v_1 v_2 \dots v_n$ avec $v \in \mathcal{F}(Q)$ et $v_1 \leq v_2 \leq \dots \leq v_n$) .

3° W : l'ensemble des mots de la forme vt ($v \in V$; $t \in T$) . Tous les mots de W et de V sont complètement légaux (mais en général non π-légaux).

D'autre part on dira que le facteur h_i de s est "critique" si :

(C1) $\qquad h_i \in Q$;

(C2) $\qquad h_{i-1} > h_i \leq h_{i+1}$

(les indices étant pris modulo n :

$$h_{i+1} = h_1 \quad \text{pour} \quad i = n \ ;$$

$$h_{i-1} = h_n \quad \text{pour} \quad i = 1 \ ).$$

Une recomposition δ_i^{-1}, où d_i est un facteur critique, sera dite "légale".

PROPRIÉTÉ II.1. - Si s est π-conjugué d'une décomposition de $\bar{s} \in T \cup \mathfrak{X}(Q)$ une condition nécessaire et suffisante pour qu'il ne possède aucun facteur critique est qu'il soit π-conjugué de $\bar{s}$ lui-même.

Réciproquement quel que soit le facteur critique h_i de s, $\delta_i^{-1} s$ est π-conjugué d'une décomposition de $\bar{s}$ et dans les mêmes conditions quand s est une décomposition de $\bar{s}$, $\delta_i^{-1} s$ est aussi une décomposition de cet élément.

DÉMONSTRATION.

Si $\bar{s} \in T$, il en est de même de sa π-classe et aucun de ses facteurs ne satisfait (C1).

Si $\bar{s} \in \mathfrak{X}(Q)$, ou bien $\bar{s} = q$ $(q \in Q)$ ou bien $\bar{s} = q^p$: dans les deux cas (C2) n'est pas satisfaite.

Soit d'abord $s \in \mathfrak{F}(K \cup Q)$ quelconque. Si $s \notin \mathfrak{X}(Q) \cup \mathfrak{X}(T)$, s possède au moins deux facteurs différents, et donc au moins un facteur satisfaisant (C2) ; supposons que h_i soit précisément le plus petit (selon $\leq$) facteur de s : s'il appartenait à K il en serait de même de tous les autres facteurs de s (puisque $q < k$ pour tout $q \in Q$ et $k \in K$). Or ceci est impossible, dans les conditions de l'énoncé, car si s est π-conjugué d'une décomposition non triviale de $\bar{s}$, s admet au moins deux facteurs h_{j-1}, h_j tels que $[h_{j-1}, h_j] \in K \cup Q$: donc (d'après la propriété I.1) $h_{j-1} > h_j$ (et donc $s \notin \mathfrak{X}(Q) \cup T$) et donc (d'après la propriété I.2) $h_j \in Q$, ce qui achève la preuve que h_i est critique. On a montré du même coup que tout $s \in \mathfrak{F}(K \cup Q)$, $s \notin \mathfrak{X}(Q) \cup T$ admet au moins un facteur critique.

RÉCIPROQUE. - Soit h_i, un facteur critique de s ;

1° h_i n'est pas un composant d'ordre zéro d'un facteur de $\bar{s}$ car : $h_{i-1} > h_i$ d'après (C2), ce qui exclut le cas où $\bar{s} \in \mathfrak{X}(Q)$; $h_i \in Q$ (d'après (C1)), ce qui exclut le cas ou $\bar{s} \in T$.

2° h_i n'est pas un composant gauche d'après la proposition I.1 et l'inégalité $h_i \leq h_{i+1}$; donc, d'après la même propriété, $[h_{i-1}, h_i]$ est un composant de $\bar{s}$ puisque $h_{i-1} > h_i$.

Si $s = \delta \bar{s}$, le facteur h_1 (le premier facteur à gauche) de s ou bien appartient à K ou bien, toujours d'après la proposition I.1, satisfait $h_1 > h_2$;

h_i n'est donc jamais un facteur critique et $\delta^*(\delta_i^{-1} s) = \delta^* \bar{s}$ pour tout facteur critique h_i de $s = \delta \bar{s}$.

Soit $\bar{s}' = \delta_s^{-1*}$ un élément sans facteur critique obtenu par une suite de recomposition légales, effectuées dans un ordre quelconque à partir de $s = \delta \bar{s}$ (resp. d'un élément π-conjugué de $s = \delta \bar{s}$) , et en particulier à partir de $s = \delta^* \bar{s} \in F$ (resp. d'un mot s de la π-classe de $\delta^* \bar{s}$) . On vient de voir que tous les facteurs de $\bar{s}'$ sont des composants de $\bar{s}$; $\bar{s}'$ est une décomposition de $\bar{s}$ mais, d'une part $\bar{s}' \in T \cup \mathfrak{X}(Q)$ (puisque $\bar{s}'$ n'a pas de facteur critique), d'autre part on sait qu'aucune décomposition propre de $\bar{s} \in T \cup \mathfrak{X}(Q)$ n'appartient à cet ensemble. $\bar{s}'$ est donc identique à $\bar{s}$ (resp. est π-conjugué de $\bar{s}$).

PROPRIÉTÉ II.2 (MEIER-WUNDERLI [16]). - δ^* établit, pour tout $p \geqslant 1$, une application bijective de l'ensemble des π-classes de $\mathfrak{X}_p(T) \cup \mathfrak{X}_p(Q)$ sur celui des π-classes de $\mathfrak{X}_p(F)$.

DÉMONSTRATION. - Montrons d'abord que si s est π-légal il en est de même de $\delta_i^{-1} s$, si et seulement si h_i est un facteur critique : en effet, d'après la propriété I.2 et (H2) , la condition (C1) et l'inégalité $h_{i-1} > h_i$ sont nécessaire et suffisantes (puisque s est π-légal par hypothèse) pour que $h = [h_{i-1} , h_i]$ appartienne à $K \cup Q$. Considérons la paire (h , h_{i+1}) : puisque, par construction, $h \notin A$, (h , h_{i+1}) est légale (d'après (H3)) si et seulement si $h_i \leqslant h_{i+1}$. Considérons la paire (h_{i-2} , h) ; ou bien $h_{i-2} \leqslant h$ ou bien, dans le cas contraire, $[h_{i-2} , h] \in K \cup Q$, car $h_{i-2} > h$ implique, a fortiori, $h_{i-2} > h_i$, donc $[h_{i-2} , h_i] \in K \cup Q$ puisque, par hypothèse, s est π-légal, donc, a fortiori, soit $[h_{i-2} , h] \in K \cup Q$, soit $h_{i-2} , h \in K$.

Soit maintenant $f = f'^p \in \mathfrak{X}_p(F)$; d'après la propriété II.1, il correspond à f' un élément $\bar{s}' \in \mathfrak{X}_1(T) \cup \mathfrak{X}_1(Q)$ dont la π-classe est bien déterminée et qui est tel que $\delta^* \bar{s}'$ soit π-conjugué de f' . Considérons $\bar{s}'^p$; $\delta^* \bar{s}'^p$ est π-conjugué de f et donc $\delta^{-1*} f$ est un élément de la π-classe de $\bar{s}'^p$.

Ainsi que l'a montré MEIER WUNDERLI, cette propriété permet de retrouver la formule de WITT [18] (une fois établi que H correspond biunivoquement à une base (indépendante) de l'algèbre de Lie libre sur A) en utilisant un résultat combinatoire dû au Colonel MOREAU [13] .

PROPRIÉTÉ II.3. - δ^* établit une application bijective de W (cf. définition supra) sur F.

DÉMONSTRATION. - Nous considérons, F, D, H, P, etc. comme des sous-ensembles des systèmes correspondants construits à partir de $A^* = A \cup a^*$ où a^* est un nouvel élément. Il est compatible avec (HO) de supposer que, dans $D(A \cup a^*)$, on a $h < a^*$ pour tout $h \in D = D(A)$; par hypothèse on a donc $a^* \in K(A \cup a^*)$.

Soit maintenant $f \in F(A)$, et considérons $\delta^{-1*}(a^* f) = \vec{s}^*$; manifestement

$$\vec{s}^* \in \mathfrak{X}_1(T(A \cup a^*)) \cup \mathfrak{X}_1(Q(A \cup a^*))$$

et, d'après la propriété II.1, $\delta^* \vec{s}^* = a^* f$. On a donc :

- soit $\vec{s}^* = a^* \bar{s}$ avec $\bar{s} \in T \vee \mathfrak{X}(Q)$ et donc $\bar{s} \in W(A)$.
- soit $\vec{s}^* = k^* \bar{s}'$ avec $k^* \in K(A \cup a^*)$ et $\bar{s}' \in T(A)$. Considérons dans ce cas la décomposition normale à gauche $a^* h_1 h_2 \dots h_n$ de k^* ; d'après les remarques faites à la fin de la propriété I.1, $h_1 \leq h_2 \leq \dots \leq h_n$, c'est-à-dire $h_1 h_2 \dots h_n \in V$ et par conséquent $\bar{s} = \delta^{-1**} f = h_1 h_2 \dots h_n \bar{s}' \in W$. et $\delta^* \bar{s} = f$. Réciproquement, si $w \in W$ est de la forme vt avec $t \in T$ et $v = h_1' h_2' \dots h_n'$ de longueur non nulle $[a^* h_1'] h_2'] \dots] h_n'] \in K(A \cup a^*)$ et δ^* et δ^{-1**} sont donc bien inverses l'un de l'autre.

REMARQUE II.1. - La propriété II.3 peut aussi être établie en considérant des facteurs "c-critique" d_i définis par

(C'1) $\qquad d_i \in Q$;

(C'2) $\qquad d_i$ est critique et $i = 2, \dots, n-1$ ou $d_i = d_n$ et $d_{n-1} > d_n$

(C'3) $\qquad d_i \leq d_{i'}$ pour tout $i' \geq i$.

W est alors l'ensemble des $s \in \mathfrak{F}(Q \cup K)$ n'admettant aucun facteur c-critique et on montre comme plus haut que si s est complètement légal, il en est de même de $\delta_i^{-1} s$ si et seulement si d_i est c-critique.

PROPRIETE II.4. - L'application $\delta^* : T \to F$ est un monomorphisme et $G = \{\delta^* t : t \in T\}$ satisfait les conditions $\mathfrak{U}_z$ et $\mathfrak{N}_\ell$.

DEMONSTRATION.

1° Que δ^* est un monomorphisme est une conséquence immédiate de la propriété II.1, car la restriction de δ^* à T admet comme on l'a vu, un inverse δ^{-1**} G est donc un sous-demi-groupe libre de F .

2° Soit $ff' = \delta^* t$ et $f'f = \delta^* t'$ $(f\ ,\ f' \in F\ ;\ t\ ,\ t' \in T)$. Puisque ff' et $f'f$ sont π-conjugués, il en est de même de t et de t' ; considérons la recomposition légale de ff' , $h_1 h_2 \dots h_n$ qui est de longueur minimale parmi celles possèdant la propriété que $\delta^*(h_1 h_2 \dots h_i) = f$ et $\delta^*(h_{i+1} h_{i+2} \dots h_n) = f'$. Comme t' est π-conjugué de t , les facteurs $h_1 , h_2 , \dots , h_n$ sont des composants de t' ; en particulier, h_{i+1} est un composant gauche (ou d'ordre zéro) et n'est donc pas un facteur critique ; la même remarque vaut pour h_1 et, puisque par hypothèse la recomposition $h_1 \dots h_i h_{i+1} \dots h_n$ est de longueur minimale avec les propriétés indiquées, elle n'admet pas de facteur critique. Tous les facteurs h_i appartiennent donc à K et par conséquent $\delta^{-1*} f$, $\delta^{-1*} f' \in T$ ce qui achève de montrer que G satisfait $\mathcal{U}_z$.

3° Le résultat est trivial si $\delta^{-1**} f \in T$; si $\delta^{-1**} f = qt$ $(q \in Q\ ,\ t \in T)$, on sait trouver (d'après la propriété I.3) $k\ ,\ k' \in K$ tels que $\delta^* k' = (\delta^* k)(\delta^* q)$; on a donc $\delta^{-1**}((\delta^* k)f) \in T$ et, par conséquent, $F f \cap t \neq \emptyset$.

Si $\delta^{-1**} f = vt$, $v = q_1 q_2 \dots q_n \in V$ et s'il existe un $h' \in H$ tel que $k = [h'\ ,\ q_1] \in K$ on a encore $\delta^{-1**}((\delta^* h')f) = [[h' q_1] q_2] \dots] q_n] t \in T$ (et donc $F f \cap G \neq \emptyset$) puisque en raison des inégalités $q_1 \leq q_2 \leq \dots \leq q_n < k$, l'élément $[h'\ ,\ q_1] q_2] \dots] q_n]$ appartient à K .

On peut donc par double induction supposer que le résultat est déjà établi pour tous les f' tels que $\delta^{-1**} f' = q_1' q_2 \dots q_n t$ avec $q_1' > q_1$ et comme en utilisant la propriété I.3 on sait trouver un h' tel que $[h'\ ,\ q_1] \in Q \cup K$ le résultat est établi dans tous les cas.

REMARQUE II.2. - Il existe au moins un autre type de sous-demi-groupes G de F satisfaisant $\mathcal{U}_z$ et $\mathcal{H}_\ell$, ce sont les idéaux à droite J (JF = F) qui satisfont la condition :

$\mathcal{U}_\ell$: pour tout $f \in F$: si $f J \cap J \neq \emptyset$ alors $f \in J$. (qui sont "unitaires à gauche" dans la théorie de P. DUBREIL [4] , [5] , [6]).

Ceci est notamment le cas des idéaux J de la forme $\overline{F}F$, où $\overline{F}$ est un mot fixe de F, ne pouvant pas être écrit sous la forme $f'f''f'$, avec f', $f'' \in F$ et f' de longueur non nulle (cf. [15], pour une théorie de ces problèmes et de leurs liens avec la notion probabiliste "d'événement récurrent") ; j'ignore s'il existe encore d'autres types de sous-demi-groupes satisfaisant $\mathcal{U}_z$, et ne pouvant pas être obtenus comme l'intersection de sous-demi-groupes de l'un des deux types décrits ou de leurs opposés.

REMARQUE II.3. - Il ressort de la démonstration que pour un ensemble K donné il existe un entier naturel n tel que quel que soit $f \in F$, il y ait au moins un $f' \in F$ de longueur inférieure à n et tel que $f'f \in \delta^* T$. Il en découle, par une application élémentaire de la théorie des demi-groupes unitaires et nets d'un seul côté ([4], [5], et [6]), que, si A contient $n < \infty$ éléments la fonction entière de la variable λ

$$1 - \sum_{k \in K} \lambda^{|k|} \qquad (|k| : \text{le degré de } k)$$

admet la racine $1/n$.

REMARQUE II.4. - $\mathcal{U}_z$ est évidemment triviale dans le cas des groupes. La condition suivante $\mathcal{U}'_z$ est équivalente à $\mathcal{U}_z$ dans le cas des demi-groupes libres mais non dans le cas des groupes.

Soient F et F' deux demi-groupes (resp. groupes) libres δ^* un homomorphisme $\delta^* : F' \to F$:

$\mathcal{U}'_z$ si f'_1, $f'_2 \in F'$ sont tels qu'il existe un $f \in F$ de longueur non nulle vérifiant $f(\delta^* f'_1) = (\delta^* f'_2) f$, alors il existe un $f' \in F'$ de longueur non nulle vérifiant $f'f'_1 = f'_2 f'$.

III. Indépendance des bases de Marshall Hall.

III.1. Notations. - On garde les notations précédentes, et on convient que pour tout $X \subset S$, $\overline{X}$ désigne le $\mathbb{Z}$-module libre dont X est une base. On convient aussi que les opérations $(x, y) \to xy$ et $(x, y) \to [x, y]$ sont bilinéaires. Donc, en particulier, $\overline{F}$ (resp. $\overline{D}$) peut être considéré comme la $\mathbb{Z}$-algèbre associative (resp. sans identité) libre sur A_0. L'élément neutre 1 de S est considéré comme l'élément unité de $\overline{S}$ et il sera commode de poser :

$[n , d] = [d , n] = [0 , d] = [d , 0] = 0$ pour tout $n \in \underset{\sim}{Z}$ et $d \in D$.

On définit en outre un homomorphisme (de $\underset{\sim}{Z}$-algèbre associative) $\lambda : \overline{S} \to \overline{F}$ par :

$$(s + s')^\lambda = s^\lambda + s'^\lambda \ ; \quad (ss')^\lambda = s^\lambda s'^\lambda \ ; \quad [s , s']^\lambda = s^\lambda s'^\lambda - s'^\lambda s^\lambda \ .$$

Chaque élément d^λ $(d \in D)$ est donc égal à un élément, que l'on désignera par le même symbole, de l'algèbre de Lie libre $\overline{L}(A)$ engendrée par A .

PROPRIÉTÉ III.1 (Marshall HALL, ŠIRŠOV). – $(\overline{D}(P))^\lambda \subset \overline{P}^\lambda$.

DÉMONSTRATION. – Soient, plus généralement, h et h' deux éléments quelconques de H ; puisque $[h , h']^\lambda + [h' , h]^\lambda = 0$, on peut supposer que $h > h'$, si $[h , h'] \in H$, on a a fortiori $[h , h'] \in P$ quand $h' \in P$; si $[h , h'] \notin H$, nous considérons la partition de Širšov $Q' \cup P'$ de H définis par $\overline{h} \in P'$ si et seulement si $\overline{h} \ngtr h'$. Soit $K' = K'(h')$, $(K' \ni h')$ l'ensemble correspondant défini comme dans I.2 ; naturellement si h appartient à P , P' est un sous-ensemble de P .

Soit $\delta_{P'}\ h = k'_1 \dots k'_n$ la décomposition de h dont tous les facteurs appartiennent à K' (cf. Remarque I.1). Supposons déjà établi, pour toutes les paires (h , h') telles que le H-contenu de $[h , h']$ (par rapport au cas particulier où $Q = \emptyset$; $P = H$ et $K = A$) soit inférieur à celui de $\overline{h}\,\overline{h'}$, que $[h\ h']^\lambda$ est égal à une somme de termes $\pm h_i^\lambda$ où tous les h_i figurant dans la somme :

1° ont le même P'-contenu que $[h , h']$

2° ont leurs deux composants d'ordre un en relation $>$ avec h' .

3° admettent h' comme composant droit.

Si $\overline{h} = [\overline{h}_1\ \overline{h}_2]$ et, par hypothèse $\overline{h}_1 > \overline{h}_2 > \overline{h'}$, on a d'après l'identité de Lie :

$$[\overline{h} , \overline{h'}]^\lambda = [[\overline{h}_1 , \overline{h'}] , \overline{h}_2]^\lambda - [[\overline{h}_2 , \overline{h'}] , \overline{h}_1]^\lambda$$

Suivant l'hypothèse d'induction, $[\overline{h}_1\ \overline{h'}]^\lambda$ et $[\overline{h}_2\ \overline{h'}]^\lambda$ sont égaux à des sommes dont tous les termes ont les propriétés voulues et donc, en particulier sont en relation $>$ avec $\overline{h'}$; le résultat en découle immédiatement puisqu'il n'y a qu'un nombre fini d'éléments de H ayant un P'-contenu donné.

REMARQUE III.1. - Soient $<$ satisfaisant (HO)', $H_{m,n}$ l'ensemble des $h \in H$ de degré m dont les <u>deux</u> composants d'ordre un sont de degré $\geqslant n$, $\alpha : \overline{H} \to \overline{H}$ la transformation linéaire induite par une transformation linéaire α_1 de A dans lui-même. La propriété III.1 permet facilement de vérifier que $\alpha \overline{H}_{m,n} \subset \overline{H}_{m,n}$ pour tout m, n. Cette propriété d'invariance des bases de Marshall HALL n'est pas partagée par les bases de CHEN, FOX et LYNDON ([2], [14]

REMARQUE III.2. - Soient h, h' et $\overline{h}$ trois éléments de H, $\overline{h}$ admettant au moins un composant égal à h ; l'élément $\overline{h'}$ de D, obtenu en subsituant h' à h (une fois) dans l'écriture de $\overline{h}$, n'appartient pas nécessairement à H ; d'après la propriété III.1, on peut trouver une somme $\sum \pm h_i$ telle que $\overline{h'}^{\lambda} = \sum \pm h_i^{\lambda}$; on va montrer que si $h \gg h'$ (où ρ est la relation d'ordre total définie dans la remarque I.1), $\overline{h} \gg h_i$ pour tous les h_i figurant avec un coefficient non nul dans la somme $\overline{h'}^{\lambda}$.

Par hypothèse, il existe une partition de Širšov $H = Q \cup P$ telle que $h, h' \in P$ et que $h \,\rho_P\, h'$; P contient certainement les composants droits h_1 et h_1' d'ordre un de h et de h' car sinon, désignant par h_1^* le plus petit de ces deux éléments et par $Q^* \cup P^*$ la partition de Širšov définie par $h'' \in P^*$, si et seulement si $h_1^* \leqslant h''$, on aurait $\gamma \delta_{P^*} h = \gamma \delta_{P^*} h'$ et donc, comme on le vérifie aisément $h = h'$. Le résultat en découle immédiatement par induction car, si $[h , h''] \in H$ ou $[h'' , h] \in H$, h'' est $\gg$ le composant droit d'ordre un de h. Donc, $h'' \in P$ et, comme le P-contenu de tous les termes h_i apparaissant dans la somme $[h' , h'']$ ou $[h'' , h']$ est le même que celui de $[h' , h'']$, on a $[h , h''] \,\rho_P\, h_i$ d'après les propriétés de régularité de la relation $\gg$.

Nous considérons maintenant de nouveau une partition de Širšov $Fl = Q \cup P$ fixe et les ensembles T, W, etc. définis au début de la section II. On rappelle que $\overline{F}$ est la Z-algèbre libre engendrée par A.

PROPRIÉTÉ III.2 (G. BIRKHOFF, E. WITT). - $\overline{W}^{\lambda}$ est une base (indépendante) de $\overline{F}$ ([1], [18]).

DÉMONSTRATION. - On suit la méthode de "straightning" de G. BIRKOFF [1].

Soit U l'ensemble des mots complètement légaux de S. Par définition $F \subset U \subset \mathfrak{F}(K \cup Q)$. On définit une application linéaire σ de $\overline{U}$ dans $\overline{W}$ par :

$(u + u')^{\sigma} = u^{\sigma} + u'^{\sigma}$; $u^{\sigma} = u$, si $u \in W$; $(u' u)^{\sigma} = (u' u^{\sigma})^{\sigma}$

et pour tout u appartenant à l'ensemble U' des mots de la forme $u' = hw$ avec $h \in H$, $w \in W$, $w = h_1 w'$; $w' \in W$ et (h , h_1) légal, on pose :

$$(h w)^{\sigma} = h w \quad , \text{ si } h \leq h_1 \quad (\text{puisqu'alors } hw \in W)$$

$$= ([h\ h_1]\ w')^{\sigma} + h_1 (h\ w')^{\sigma} , \text{ si } h > h_1 .$$

la définition permet effectivement une construction par induction car, si $h > h_1$,

1° les deux termes $[h , h_1] w'$ et hw' sont de longueur strictement inférieure à celle de $h w$.

2° Puisque (h , h_1) est légale, et que $w' = h_2 w''$ avec $h_1 \leq h_2$, $(h_1\ h_2)$ est légale a fortiori et donc $[h , h_1] w' \in U'$

3° Pour les mêmes raisons, $hw' \in U'$. Par une induction facile on vérifie que le premier facteur à gauche de tous les w_i figurant dans la somme $\sum w_i = (h\ w')^{\sigma}$ est toujours en relation $>$ avec h ou h_2 (selon que $h \leq h_2$ ou $h > h_2$) et donc, a fortiori, en relation $>$ avec h_1 .

On note d'autre part :

4° Que hw , $[h , h_1] w'$ et $h_1\ h\ w'$ ont le même H-contenu

5° que $(h\ h_1)^{\lambda} = [h , h_1]^{\lambda} + (h_1\ h)^{\lambda}$.

Il s'ensuit par induction que pour tout $u \in U$, $(u^{\sigma})^{\lambda} = u^{\lambda}$ ce qui achève la démonstration. On remarquera, qu'il résulte de la construction que pour tout $f \in F$, f^{σ} est une somme dont les coefficients sont non négatifs.

Etant donné (Propriété II.3) qu'il existe une correspondance bijective, conservant le contenu, entre F et W , III.2 montre que W^{λ} est une base indépendante de $\overline{F}$. Donc,

1° Les h^{λ} $(h \in H)$ sont linéairement indépendants et forment une base de l'algèbre de Lie libre engendrée par A (Marshall HALL).

2° Les t^{λ} $(t \in T)$ engendrent une sous-algèbre associative libre de $\overline{F}$ (ŠIRŠOV) puisque les $\delta^{*} t$ $(t \in T)$ engendrent un sous-demi-groupe libre de F (propriété II.4).

Soient R un corps, $\overline{X}$ désignant maintenant le R-module libre engendré par X et $\varphi : \overline{L}(A) \to \overline{L}'$, un épimorphisme de $\overline{L}(A)$ la R-algèbre de Lie libre.

REMARQUE III.3. - Quel que soit la base de Marshall HALL, H, il existe un sous-ensemble $Q \subset H$ tel que φQ soit une base (indépendante) de L' et qu'en outre Q contienne tous les composants de ses éléments.

DÉMONSTRATION. - Il est évident que φH est une base (non indépendante) de L' ; définissons une suite $h_1^*, h_2^*, \dots, h_n^*, \dots$ d'éléments de H par les règles suivantes

1° $h_{i+1}^* \in Q(h_i^*)$ où $Q(h_i^*)$ est le sous-ensemble de H formé des éléments dont aucun des composants n'est un $h_{i'}^*$ $(i' \leq i)$.

2° h_{i+1}^* est le plus petit élément de $Q(h_i^*)$ (h_1^* est le plus petit élément de H) selon l'ordre $\gg$ tel que φh_{i+1}^* appartienne au sous-module de L' engendré par tous les φh avec $h \ll h_{i+1}^*$.

Soit maintenant $Q = \bigcap_i Q(h_i^*)$ et $H = Q \cup P$ la partition correspondante de H, Par construction, Q contient tous les composants de ses éléments et les φq , $q \in Q$, sont indépendants ; comme d'après la remarque III.2, $\varphi h \in \varphi Q$ pour tout $h \in P$, le résultat est établi.

On observera que si, ayant défini une nouvelle relation d'ordre $<'$ sur D , satisfaisant (HO) et $h <' h'$, si $h , h' \in Q$ et $h < h'$ ou si $h \in Q$ et $h' \notin Q$, on construit la base de Marshall HALL correspondante H' , on a :

$$Q \subset H \cap H'$$

et il existe une partition de Širšov $Q \cup P'$ de H' telle que $\overline{P'}^{\lambda} = \overline{P}^{\lambda}$.

IV. Algèbre de "Shuffle"

Soit $\langle s , s' \rangle$ la forme bilinéaire symétrique sur $\overline{S} \times \overline{S}$ définie à partir de $\langle s , s' \rangle = 1$ ou $= 0$, selon que $s = s'$ ou $s \neq s'$ $(s , s' \in S)$. Le théorème de Poincaré-Birkhoff-Witt peut s'écrire sous la forme :

$$s = \sum_{w \in W} \langle w , s^{\sigma} \rangle w^{\lambda}$$

et et nous allons donner une formule un peu différente pour calculer $\langle w , s^{\sigma} \rangle$ Afin de simplifier les énoncés on suppose désormais que $P = \emptyset$, c'est-à-dire que $H = Q$ et $W = V$.

On va munir le $\underset{\sim}{Z}$-module $\overline{F}$ d'une structure $\overline{F}_{\top}$ d'algèbre de "shuffle" qui est un cas très particulier des structures de même nom introduites par R. C. LYNDON [14] et dont la théorie est exposée dans [2].

Soit $\top$ une opération linéaire $\overline{F} \times \overline{F} \to \overline{F}$ définie par prolongement à partir des règles suivantes :

(S1) $\qquad 1 \top f = 0 \top f = f \top 0 = 0 \; ; \; f \top 1 = f$ pour tout $f \in F$

et, par induction :

(S2) $\qquad$ si $f = af'$ $(a \in A \, , \; f' \in F)$,

$$f \top f'' = a(f' \top f'' + f'' \top f') \text{ pour tout } f'' \in \overline{F}$$

Posons pour abréger $x \overline{\top} y = x \top y + y \top x$, pour tout x, y et considérons la double identité :

(S0) $$(x \top y) \top z = (x \top z) \top y = x \top (y \overline{\top} z) \; .$$

Il résulte immédiatement de (S0) que $\overline{\top}$ est non seulement commutative mais encore associative car, à cause de la distributivité :

$$(x \overline{\top} y) \overline{\top} z = (x \top y) \top z + (y \top x) \top z + z \top (x \top y) + z \top (y \top x)$$

avec, d'après (S0) :

$$(x \top y) \top z = x \top (y \overline{\top} z) \; ; \quad (y \top x) \top z = (y \top z) \top x \; ;$$

$$z \top (x \top y) + z \top (y \top x) = z \top (y \overline{\top} x) = (z \top y) \top x$$

et par conséquent :

$$\begin{aligned}(x \overline{\top} y) \overline{\top} z &= x \top (y \overline{\top} z) + (y \top z) \top x + (z \top y) \top x \\ &= x \top (y \overline{\top} z) + (y \overline{\top} z) \top x \\ &= x \overline{\top} (y \overline{\top} z) \; .\end{aligned}$$

D'autre part, (S0) est identiquement vérifiée par l'opération $\top$ définie par (S1) et (S2) car (S0) est trivialement vraie si $x = 1$ et, par induction, si (S0) est vraie pour x, y, z $(x, y, z \in F)$ et si $a \in A$, on a, pour ax , y et z :

$$(ax \top y) \top z = (a(x \bar{\top} y)) \top z = a((x \bar{\top} y) \bar{\top} z)$$

$$= a(x \bar{\top} (y \bar{\top} z)) = (ax) \top (y \bar{\top} z)$$

$$= a((x \bar{\top} z) \bar{\top} y) = (ax \top z) \top y$$

Pour tout f , $f' \in F$, $f \bar{\top} f' = \sum f_i$ $(f_i \in F)$ où le contenu de chacun des f_i apparaissant dans cette somme est le même que celui de ff' .

Les f_i sont les "shuffles" de R. C. LYNDON correspondant au cas particulier où la longueur du "shuffle" est la somme de celle des éléments "shuffled" f et f' .

On observera que $\bar{F}_\top$ est la $\underset{\sim}{Z}$-algèbre libre $\bar{Y}$ sur A satisfaisant (S0) ; en effet, on vérifie facilement que si $\bar{Y}$ satisfait cette identité, tout $y \in \bar{Y}$ est une somme finie de termes "normés" c'est-à-dire de la forme $a_1 \top (a_2 \top (a_3 \top (\ldots))$ avec a_1 , a_2 , ... , a_i $\in A$; or, si $\bar{Y} = \bar{F}_\top$, d'après (S2), $a_1 \top (a_2 \top (a_3 \top (\ldots))) = a_1 a_2 a_3 \ldots \in F$ et le résultat découle immédiatement de ce que F est une base indépendante de $\bar{F}$.

Soit maintenant $\tau : \bar{W} \to \bar{F}$ l'application définie par les règles suivantes :

1° $a^\tau = a$ pour tout $a \in A$

2° $h^\tau = (\delta_1^* h)^\tau$ pour tout $h \in H$ (où, on le rappelle, $\delta_1^* h$ est la décomposition normale gauche de h) .

3° $w^\tau = (\prod n_i!)^{-1} w^{\bar{\tau}} = (\prod n_i!)^{-1} h_1^\tau \bar{\top} h_1^\tau \ldots \bar{\top} h_2^\tau \ldots \bar{\top} h_x^\tau$ pour tout $w = h_1^{n_1} h_2^{n_2} \ldots h_i^{n_i} \ldots h_x^{n_x}$ avec $w^{\bar{\tau}}$ défini récursivement par $(w\, h_j)^{\bar{\tau}} = w^{\bar{\tau}} \bar{\top} h_j^\tau$.

4° $(w + w')^\tau = w^\tau + w'^\tau$.

PROPRIÉTÉ IV.1. - Pour tout $w \in \bar{W}$ et $f \in \bar{F}$,

$$\langle w^\tau , f \rangle = \langle w , f^\sigma \rangle$$

DÉMONSTRATION. - Il suffit évidemment de démontrer le résultat pour $w \in W$ et $f \in F$. Supposons-le déjà établi pour $f' \in F$, et soit $f = af'$, $a \in A$.

On a :

$$<w\ ,\ (af')^{\sigma}> = \sum_{w'\in W} <w\ ,\ (aw')^{\sigma}> < w'\ ,\ f'^{\sigma}>$$

Soit $w' = h_1^{n_1} h_2^{n_2} \dots h_i^{n_i}$; d'après les résultats de III, on vérifie facilement que

$$< w\ ,\ (aw')^{\sigma}> = 0\ ,$$

sauf si w a l'une des formes

$$w = aw' \quad (\text{et alors } a < h_1)$$

$$w = h_1^{n'_1+1} h_2^{n'_2} \dots h_i^{n_i} \quad (\text{et alors } h_1 = a)$$

$$w = h_1^{n_1} h_2^{n_2} \dots h_i^{n_i}$$

où les n_i sont reliés aux n'_i par la condition suivante ; pour un certain i^*

1° $n_i = n'_i - \nu_i \quad (\nu_i \geqslant 0)$ quand $i < i^*$

2° $n_{i^*} = n'_{i^*} + 1$ et $\delta_1^* h_{i^*} = a\, h_1^{\nu_1} h_2^{\nu_2} \dots h_{i^*}^{\nu_{i^*-1}}$

3° $n_i = n'_i$ quand $i > i^*$

Dans ce cas,

$$<w\ ,\ (aw')^{\sigma}> = \prod_{i\leq i^*} \left[{n'_i \atop \nu_i}\right] \quad ([\ ] : \text{le coefficient binomial}).$$

Considérons maintenant w^{τ} ; on a, en raison du fait que $\overline{\top}$ est associative et commutative et des identités (S1) (S2)

$$w^{\tau} = (\prod n_i!)^{-1} \sum_{i^*} n_{i^*} (\prod \nu_j!)^{-1}\, a'_{i^*} \top (w'_{i^*})^{\overline{\tau}}$$

où la somme est étendue à tous les h_{i^*} distincts figurant dans w et où on a posé

1° $\delta_1^* h_{i^*} = a'_{i^*} h_1^{\nu_1} h_2^{\nu_2} \dots h_{i-1}^{\nu_{i-1}}$

2° w' = l'élément de W, $w' = h_1^{n'_1} h_2^{n'_2} \dots h_i^{n'_i}$

avec

$$n'_i = n_i + \nu_i \,, \quad \text{pour} \quad i < i^*$$

$$n'_{i^*} = n_{i^*} - 1 \,, \quad \text{pour} \quad i = i^*$$

$$n'_i = n_i \,, \quad \text{pour} \quad i > i^*$$

Donc,

$$\langle w^\tau , af' \rangle = (\Pi\, n_i!)^{-1} \sum_{i^*} n^*_i (\Pi\, \nu_i!)^{-1} \langle a_{i^*} \top w^{\tilde\tau}_{i^*} , af' \rangle$$

$$= (\Pi\, n_i!)^{-1} \sum_{i^*} n^*_i (\Pi\, \nu_i!)^{-1}\, \Pi (n_i + \nu_i)! \langle w^\tau_{i^*} , f' \rangle$$

où la sommation est étendue à tous les i^* tels que $a_{i^*} = a$.

Comme par hypothèse $\langle w'^{\tilde\tau}_{i^*} , f' \rangle = \langle w_{i^*} , f'^\sigma \rangle$ le résultat découle immédiatement de la comparaison de cette formule avec $\langle w_1 (a\, w')^\sigma \rangle$.

REMARQUE. - Soit $W_{(n)}$ le sous-ensemble de W formé par les w de la forme $f'h$ où $f' \in F$ et $h \in H$ et où h est de degré n .

Soit d'autre part $\mu : \overline{F} \to \overline{F}$ l'homomorphisme de $\overline{F}$ induit par la substitution de $1 + a_i$ à a_i pour tout $a_i \leq A$. On vérifie facilement que pour tout $f \in F$ la composante homogène de degré m de μf est déterminée par la seule donnée des $\langle w^\tau , f \rangle$ avec $w \in W_{(n)}$ $n \leq m$. Il en résulte la possibilité de retrouver les relations de "shuffle" et en particulier le fait que si $f \in F$ est de degré n_1 en a_1 , n_2 en a_2 , ... , n_i en a_i $(n_1 \geq n_2 \geq \dots \geq n_i)$, les inégalités existant entre les coefficients font que f est déterminé par la donnée des $\langle w^\tau , f \rangle$ avec $w \in W_{(n)}$, $n \leq n_2 + 1$.

Les formules utilisant les bases de Marshall HALL semblent cependant moins bien adaptées à ce calcul que celles qui reposent sur les bases de CHEN, FOX et LYNDON.

Mentionnons pour terminer la formule suivante qui se déduit facilement des calculs qui viennent d'être développés :

Si $w = h_1^{\nu_1} h_2^{\nu_2} \dots h_i^{\nu_i}$, le coefficient $N(w) = \langle w^\tau , (\sum a_i)^n \rangle$ est égal à :

$$(\sum \nu_i |h_i|)! \prod_i (\nu_i!)^{-1} (N(h_i)/|h_i|)^{\nu_i}$$

où $|h_i|$ est le degré de h_i $(n = \sum \nu_i |h_i|)$ est où $N(h_i)$ est défini inductivement par $N(h_i) = N(w')$ quand $\delta_1^* h_i = a w'$ $(a \in A)$.

En particulier, si h est multilinéaire de degré n

$$\langle h^\vee, (\sum a_i)^n \rangle = (n-1)! \, (\prod |h_i|)^{-1}$$

où le produit est étendu à tous les composants propres de h qui ne sont pas des composants gauches.

BIBLIOGRAPHIE

[1] BIRKHOFF (Garrett). - Representability of Lie algebras and Lie groups by matrices, Annals of Math., Series 2, t. 38, 1937, p. 526-532.

[2] CHEN (K. T.), FOX (R. H.) and LYNDON (R. C.). - Free differential calculus, IV : The quotient groups of the lower central series, Annals of Math., Series 2, t. 68, 1958, p. 81-95.

[3] CROISOT (Robert). - Automorphismes intérieurs d'un semi-groupe, Bull. Soc. math. France, t. 82, 1954, p. 161-194.

[4] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, I., Mém. Acad. Sc. Inst. France, t. 63, 1941, 52 p.

[5] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, II., Univ. Roma Ist. naz. alta Mat. Rend. Mat. e Appl., t. 10, Série 5, 1951, p. 183-200

[6] DUBREIL (Paul). - Contribution à la théorie des demi-groupes, III., Bull. Soc. math. France, t. 81, 1953, p. 289-306.

[7] FOX (Ralph H.). - Free differential calculus, I : Derivation in the free group ring, Annals of Math., Series 2, t. 57, 1953, p. 547-560.

[8] GOLOMB (S. W.), GORDON (B.) and WELCH (L. R.). - Comma free codes, Canadian J. of Math., t. 10, 1958, p. 202-210.

[9] HALL (Marshall). - A basis for free Lie rings and higher commutators in free groups, Proc. Amer. math. Soc., t. 1, 1950, p. 575-581.

[10] KUROŠ (A. G.). - Neassociativnye svobodnye algebry i svobodnye proizvedenija algebr (Non-associative free algebras and free products of algebras), Recueil math. Soc. math. Moscou (Mat. Sbornik), N. S., t. 20 (62), 1947, p. 239-262.

[11] LAZARD (Michel). - Sur les algèbre enveloppantes universelles de certaines algèbres de Lie, Publ. scient. Univ. Alger, Série A, t. 1, 1954, p. 281-294.

[12] LAZARD (Michel). - Lois de groupes et analyseurs, Ann. scient. Ec. Norm. Sup., Série 3, t. 72, 1955, p. 299-400.

[13] LUCAS (Edouard). - Théorie des nombres. - Paris, Gauthier-Villars, 1891.

[14] LYNDON (R. C.) - On Burnside's problem, I., Trans. Amer. math. Soc., t. 77, 1954, p. 202-215.

[15] MANDELBROT (Benoit). - Logique et langage. - Paris, Presses universitaires de France, 1957.

[16] MEIER-WUNDERLI (H.). - Note on a basis of P. Hall for the higher commutators in free groups, Comment. Math. Helvet., t. 26, 1952, p. 1-5.

[17] ŠIRŠOV (A. I.). - Podalgebry svobodnykh lievykh algebr, Recueil math. Soc. math. Moscou (Mat. Sbornik), N. S., t. 33 (75), 1953, p. 441-452.

[18] WITT (Ernest). - Treue Darstellung Liescher Ringe, J. für reine und ang. Math., t. 177, 1937, p. 152-160.