

# Empilements de Lyndon et bases d'algèbres de Lie

Pierre Lalonde

Department of mathematics, M.I.T., Cambridge,  
Massachusetts, U.S.A, 02139-4307

*-Résumé-* Les empilements de Lyndon forment un analogue partiellement commutatif des mots de Lyndon. On construit une base de l'algèbre de Lie libre (partiellement commutative) correspondante en utilisant les propriétés combinatoires des empilements de Lyndon.

## Mots de Lyndon

On connaît l'intérêt qu'offrent les mots de Lyndon pour la combinatoire et l'algèbre. En particulier, en partant des mots de Lyndon, on peut construire bijectivement une base de l'algèbre de Lie libre engendrée par les lettres. Une généralisation de ce concept pour les empilements permet de relever cette dernière affirmation dans un contexte partiellement commutatif.

Pour comprendre les distinctions à apporter lors de ce passage, revoyons brièvement la définition des mots de Lyndon. Étant donné deux mots  $u$  et  $v$  sur un même alphabet  $A$ , on dit que le mot  $vu$  est un *transposé* (ou un *conjugué*) du mot  $uv$ . On écrit alors  $uv \sim vu$ . Chercher les transposés d'un mot revient à le considérer comme une séquence circulaire. Pour les mots, la transposition est une relation d'équivalence; en particulier, si  $u \sim v \sim w$  pour des mots  $u, v, w$ , on a alors  $u \sim w$ . Le résultat de deux transpositions consécutives s'obtient par une seule transposition.

Sur l'alphabet  $A$ , on aura au préalable défini un ordre total qui induit alors l'ordre lexicographique sur l'ensemble  $A^*$  des mots. Les *mots de Lyndon* forment, par construction, un système de représentants des classes de conjugaison de mots qui sont primitives (voir Lothaire [Lo; ch. 5]).

## Empilements

Nous supposons connue la théorie des empilements (Viennot [Vi]) qui permet de donner une image géométrique des éléments du monoïde partiellement commutatif (Cartier-Foata [CF]), aussi nous ne ferons que fixer les notations s'y rapportant. Soit  $P$  un ensemble de positions (analogue de l'alphabet) avec relation de concurrence  $\zeta$ . On note  $\mathcal{H}(P)$  le monoïde des empilements sur  $P$ . Le produit d'empilements s'appelle superposition;  $E \circ F$  est la superposition de  $F$  sur  $E$ . Le symbole  $\Phi$  représente l'empilement vide. Si  $E$  est un empilement,  $\pi(E)$  est l'ensemble des positions occupées par les pièces de  $E$  et  $\zeta(E)$  l'ensemble des positions concurrentes avec une position de  $E$ . Le nombre de pièces de  $E$  se note  $|E|$ ; le nombre de pièces en position  $p$  dans  $E$  est  $|E|_p$ . On note  $\min(E)$  l'empilement constitué des pièces de  $E$  qui ne recouvrent aucune autre pièce de  $E$ ;  $\max(E)$  l'empilement constitué des pièces de  $E$

qu'aucune autre ne recouvre. On reconnaîtra, dans ce dernier, l'ensemble des lettres maximales de Cori, Metivier et Zielonka [CMZ] et l'alphabet terminal de Duchamp et Krob [DK].

Pour les empilements, nous devons définir un concept de conjugaison et introduire un ordre qui s'apparentera à l'ordre lexicographique. Ainsi, on dira que l'empilement  $V \circ U$  est un *transposé* de l'empilement  $U \circ V$  (noté  $U \circ V \sim V \circ U$ ). La *conjugaison* sera alors la fermeture transitive de la relation transposition. Remarquez que, contrairement au cas des mots, la transposition d'empilements n'est pas la conjugaison (fig. 1). Duboc [Du] a dégagé ces deux notions et montré l'équivalence de diverses définitions de la conjugaison.

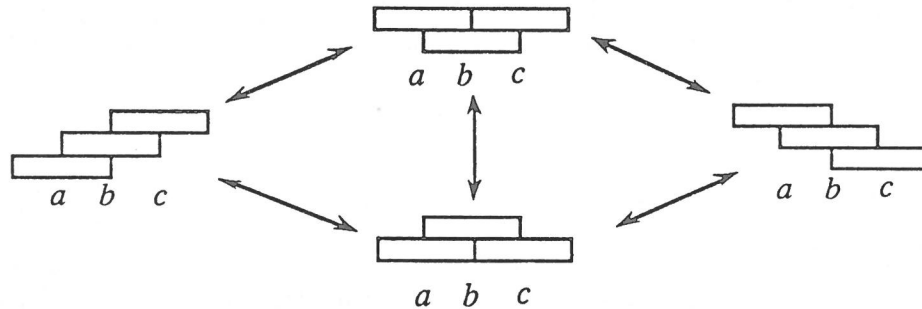


Fig. 1 La conjugaison d'empilements ne se ramène pas à la transposition.

Deux empilements,  $E$  et  $F$ , sont *connectés* (l'un à l'autre) si il existe une pièce de  $E$  concurrente avec une pièce de  $F$ . Un empilement  $E$  est *primitif* si  $E = U \circ V = V \circ U$  implique que  $U = \Phi$  ou  $V = \Phi$ . Remarquer que si  $E$  est primitif, il n'est pas puissance (non-triviale) d'un autre empilement. Duboc définit la primitivité par cette propriété [Du, ch.3, sect.2.2]. Le concept que nous utilisons ici est plus général; il recouvre en effet le cas où  $U$  et  $V$  ne sont pas connectés.

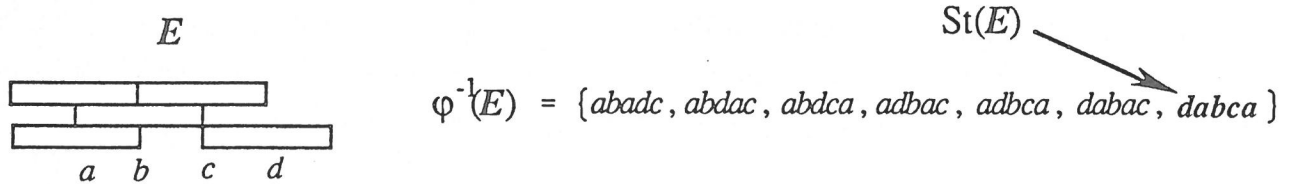


Fig. 2 Un empilement  $E$ , l'ensemble  $\varphi^{-1}(E)$  des mots qui lui sont associés et le mot standard associé.

Soit  $\varphi: P^* \rightarrow \mathcal{H}(P)$  la fonction qui associe à un mot  $p_1 \dots p_k$ , l'empilement  $p_1 \circ \dots \circ p_k$ . On suppose que l'ensemble des positions  $P$  est totalement ordonné. À tout empilement, on associe le mot  $\text{St}(E) = \max(\varphi^{-1}(E))$  dit le *mot standard associé* à  $E$  (voir fig. 2). Ceci permet de reporter l'ordre lexicographique des mots aux empilements en posant  $E \leq F$  ssi  $\text{St}(E) \leq \text{St}(F)$ . Cet ordre est linéaire. On notera  $\text{inf}(E)$  (respectivement:  $\text{sup}(E)$ ) la position minimale (respectivement: maximale) dans  $\pi(E)$  (si  $E \neq \Phi$ ). Ceci permet de distinguer cette position de l'empilement  $\text{min}(E)$ . On vérifie facilement les propriétés énoncées dans le prochain lemme.

**Lemme 1** Soit  $E$  et  $F$  des empilements. On a:

$$1) \text{St}(E \circ F) \geq \text{St}(E)\text{St}(F) \geq \text{St}(E);$$

- 2) tout facteur d'un mot standard est un mot standard;
- 3) si  $E \neq \Phi$  alors la première lettre de  $\text{St}(E)$  est  $\text{sup}(\min(E))$ ;
- 4) si  $E$  et  $F$  sont non-vides et si  $\text{sup}(\min(F)) \leq \text{inf}(E)$ , alors  $\text{St}(E \circ F) = \text{St}(E)\text{St}(F)$ .

**Démonstration** Le premier énoncé est clair, puisque  $\text{St}(E)\text{St}(F)$  est un mot associé à l'empilement  $E \circ F$ . Pour démontrer le deuxième, soit  $uvw$  un mot standard. Soit  $V = \varphi(v)$ . On a  $\text{St}(V) \geq v$ , d'où  $uvw \leq u\text{St}(V)w$  (puisque  $|\text{St}(V)| = |v|$ ). Mais comme  $u\text{St}(V)w$  est un mot associé à  $\varphi(uvw)$ , on a aussi  $u\text{St}(V)w \leq uvw$ . En simplifiant, on trouve  $v = \text{St}(V)$ . Le troisième énoncé est évident; passons au quatrième. Soit  $E'$  un facteur droit non-vide de  $E$ . On montre que les positions  $p = \text{sup}(\min(E' \circ F))$  et  $q = \text{sup}(\min(E'))$  sont égales. Comme  $\pi(\min(E')) \subseteq \pi(\min(E' \circ F))$  alors  $q \leq p$ . Si  $p \in E'$  alors  $p \leq q$ . Si  $p \in \pi(\min(F))$  alors  $p \leq \text{sup}(\min(F)) \leq \text{inf}(E) \leq \text{inf}(E') \leq q$ . Dans tous les cas, on a  $p = q$ . Donc,  $\text{St}(E' \circ F) = p\text{St}(E'' \circ F)$  où  $E' = p \circ E''$ . Terminer par une induction. ■

Remarquez que  $\text{St}(E \circ F) \neq \text{St}(E)\text{St}(F)$  en général (sinon la théorie des empilements serait identique à la théorie des mots).

### Empilements de Lyndon

**Définition 2** Un empilement non-vide  $L$  est un empilement de Lyndon si  $L = U \circ V$  avec  $U, V \neq \Phi$  implique que  $L = U \circ V < V \circ U$ . On note  $\mathcal{L}(P)$  l'ensemble des empilements de Lyndon sur  $P$ . ■

On aurait pu aussi les définir comme suit.

**Définition 3** Un empilement non-vide  $L$  est un empilement de Lyndon si il est primitif et minimal dans sa classe de conjugaison. ■

Comme la conjugaison est plus générale que la transposition, il est étonnant, à priori, que ces deux définitions coïncident. Le lecteur intéressé par la démonstration consultera [La1] ou [La2].

Une *pyramide*  $D$  est un empilement vérifiant  $|\min(D)| = 1$ . On note  $\mathcal{D}(P)$  l'ensemble des pyramides sur  $P$ . Elle est *admissible* si  $\text{inf}(D) = \pi(\min(D))$ ; c'est à dire si la pièce minimale occupe la plus petite position. Si  $D$  est une pyramide admissible dont la pièce minimale est la seule occupant la position  $\text{inf}(D)$ , on dit que  $D$  est une *super-lettre*. Toute super-lettre est nécessairement un empilement de Lyndon (voir fig. 3).

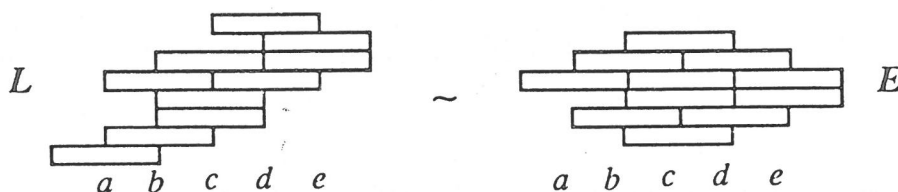


Fig. 3 Une super-lettre  $L$  et un de ses conjugués  $E$ . On a  $\text{St}(L) = abcdeebcd$  et  $\text{St}(E) = cdeebccdbcd$ .

**Lemme 4** Si  $L$  est un empilement de Lyndon alors  $L$  est une pyramide admissible.

**Démonstration** Soit  $p$  la pièce minimale de  $L$  en position  $\text{inf}(L)$ . Écrire  $L = U \circ V$  (où  $V$  est la pyramide de  $L$  telle que  $\text{min}(V) = p$ ) et  $V \circ U = U_1 \circ V \circ U_2$  (où  $V \circ U_2$  est la pyramide de  $V \circ U$  telle que  $\text{min}(V \circ U_2) = p$ : voir fig. 4). Ainsi  $L = U_1 \circ U_2 \circ V$ . Si  $U \neq \Phi$ , on peut écrire:  $\text{St}(U_1)\text{St}(U_2 \circ V) \leq \text{St}(L) < \text{St}(V \circ U) = \text{St}(U_1)\text{St}(V \circ U_2)$  (par les énoncés 1 et 4 du lemme 1). Donc  $\text{St}(U_2 \circ V) < \text{St}(V \circ U_2)$  (d'où  $U_2 \neq \Phi$ ). En comparant la première lettre de chacun de ces mots, on obtient une contradiction. Donc  $U = \Phi$  et  $L = V$  qui est une pyramide admissible. ■

Si  $L$  est un empilement de Lyndon, on a donc:  $\text{inf}(L) = \pi(\text{min}(L)) = \text{sup}(\text{min}(L))$ . On dira que  $\text{inf}(L)$  est la *base* de  $L$ .

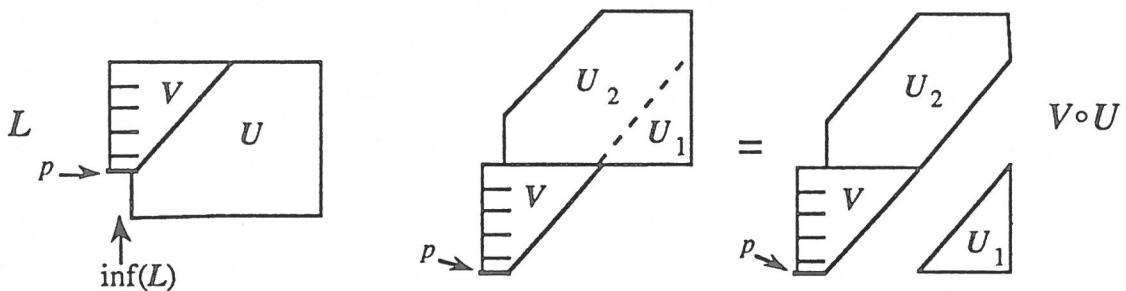


Fig. 4 Schéma des relations entre  $L, U_1, U_2$  et  $V$ .

**Théorème 5** Un empilement  $L$  est de Lyndon ssi  $\text{St}(L)$  est un mot de Lyndon.

**Démonstration** Soit  $L$  un empilement de Lyndon. Soit  $uv = \text{St}(L)$  avec  $u, v \neq 1$ . Poser  $U = \varphi(u)$  et  $V = \varphi(v)$ . Comme  $L$  est une pyramide admissible, on peut en dire autant de  $U$ ; de plus,  $\text{inf}(U) = \text{inf}(L)$ . Donc  $\text{sup}(\text{min}(U)) = \text{inf}(L) \leq \text{inf}(V)$ . Ainsi,  $uv = \text{St}(U \circ V) < \text{St}(V \circ U) = \text{St}(V)\text{St}(U) = vu$ . Donc  $uv$  est un mot de Lyndon.

Inversement, soit  $L$  un empilement non-vidé tel que  $\text{St}(L)$  soit un mot de Lyndon. On montre pour commencer que  $L$  est une pyramide admissible. L'argumentation s'apparente à celle du lemme précédent. Soit  $p$  la pièce minimale de  $L$  en position  $\text{inf}(L)$ . Écrire  $L = U \circ V$  (où  $V$  est la pyramide de  $L$  telle que  $\text{min}(V) = p$ ). On a  $\text{sup}(\text{min}(V)) < \text{inf}(U)$  (si  $U$  est non-vidé). Donc  $\text{St}(L) = \text{St}(U)\text{St}(V) \leq \text{St}(V)\text{St}(U)$ . Si  $U$  est non-vidé, comparer les premières lettres, pour obtenir  $\text{St}(U)\text{St}(V) > \text{St}(V)\text{St}(U)$ , contredisant l'hypothèse voulant que  $\text{St}(L)$  soit un mot de Lyndon. Donc  $U$  est vidé et  $L$  est une pyramide admissible. Reste à montrer que  $L$  est un empilement de Lyndon. Écrire  $L = U \circ V$  ( $U$  et  $V$  non-vidés). On a  $\text{sup}(\text{min}(V)) \geq \text{sup}(\text{min}(U))$ . Si on a l'égalité, alors  $\text{St}(L) = \text{St}(U)\text{St}(V) < \text{St}(V)\text{St}(U) \leq \text{St}(V \circ U)$ . Si on a l'inégalité, alors  $L = U \circ V < V < V \circ U$ . ■

Ce théorème permet de transférer de nombreuses propriétés des mots de Lyndon aux empilements de Lyndon.

**Théorème 6** Un empilement  $L$  est de Lyndon ssi  $L$  est strictement inférieur à tous ses facteurs droits propres.

**Démonstration** Soit  $L$  un empilement de Lyndon. Comme au théorème 5, écrire  $L = U \circ V$  ( $U$  et  $V$  non-vides). On a  $\sup(\min(V)) \geq \sup(\min(U))$ . Si on a l'égalité, alors  $\text{St}(L) = \text{St}(U)\text{St}(V) < \text{St}(V)$  (puisque  $\text{St}(L)$  est un mot de Lyndon). Si on a l'inégalité, alors  $L = U \circ V < V$  (comparer les premières lettres des mots correspondants). Inversement, si  $L$  est un empilement inférieur à tous ses facteurs droits propres, on écrit:  $L = U \circ V < V < V \circ U$ . ■

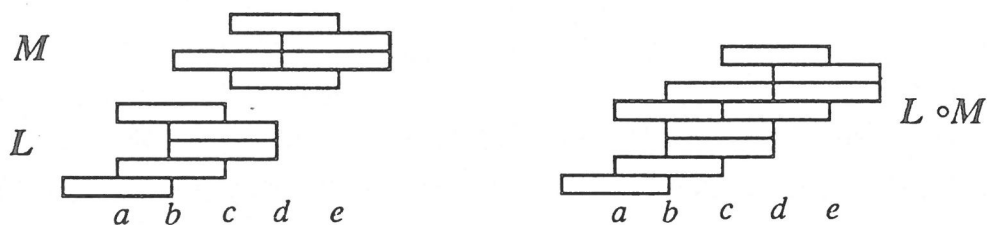
**Théorème 7** Tout empilement  $E$  se factorise de façon unique sous la forme  $E = L_1 \circ \dots \circ L_k$ , où  $k \geq 0$  et où les  $L_i$  sont des empilements de Lyndon tels que  $L_1 \geq \dots \geq L_k$ .

**Démonstration** Écrire  $\text{St}(E) = \ell_1 \ell_2 \dots \ell_k$  (où les  $\ell_i$  sont des mots de Lyndon tels que  $\ell_1 \geq \ell_2 \geq \dots \geq \ell_k$ ). Poser  $L_i = \varphi(\ell_i)$ . Ceux-ci sont donc des empilements de Lyndon vérifiant  $E = L_1 \circ \dots \circ L_k$  et  $L_1 \geq \dots \geq L_k$ . S'il existait une deuxième factorisation de  $E$  en ces termes, alors, en passant aux mots standards, on trouverait une deuxième factorisation de Lyndon de  $\text{St}(E)$ . ■

On sait que si  $\ell$  et  $m$  sont des mots de Lyndon vérifiant  $\ell < m$ , alors  $\ell m$  est un mot de Lyndon et  $\ell < \ell m < m$ . Dans le cas des empilements, le théorème correspondant est faux. (En fait,  $L \circ M$  peut ne pas être une pyramide.) La difficulté provient du fait que la concaténation de deux mots standards ne donne pas nécessairement un mot standard. Cependant, en imposant certaines restrictions, on arrive à un résultat plus faible mais quand même utile.

**Théorème 8** Soit  $L$  et  $M$  deux empilements de Lyndon vérifiant  $L < M$ . Si  $\inf(L) = \inf(M)$ , ou si  $L$  est une super-lettre telle que  $\inf(M) \in \zeta(L)$ , alors  $L \circ M$  est un empilement de Lyndon et  $L < L \circ M < M$ .

**Démonstration** Si  $\inf(L) = \inf(M)$ , alors  $\text{St}(L \circ M) = \text{St}(L)\text{St}(M)$  est un mot de Lyndon standard (théorie des mots de Lyndon). Ainsi,  $L \circ M$  est un empilement de Lyndon. D'autre part, si  $L$  est une super-lettre telle que  $\inf(M) \in \zeta(L)$  et  $\inf(L) < \inf(M)$ , alors  $L \circ M$  est une super-lettre (voir fig. 5); donc un empilement de Lyndon.



*Fig. 5 Si  $L$  est une super-lettre et  $M$  un empilement vérifiant  $\min(M) \subseteq \zeta(L)$  et  $\inf(M) > \inf(L)$ , alors  $L \circ M$  est une super-lettre.*

En fait, les conditions du théorème sont trop fortes. Plus généralement, on pourrait démontrer le résultat suivant (mais cette fois la démonstration n'est pas aussi simple).

**Théorème 9** Soit  $L$  et  $M$  deux empilements de Lyndon vérifiant  $L < M$  et  $\text{inf}(M) \in \zeta(L)$ , alors  $L \circ M$  est un mot de Lyndon et  $L < L \circ M < M$ . ■

Nous n'utiliserons pas ce théorème. Aussi nous le laissons sans démonstration (on la trouvera dans [La1, La2]).

### Formule de Witt

Posons  $v(E) = t^{|E|}$  pour tout empilement  $E$ . Ceci définit un poids sur  $\mathcal{H}(P)$ . Le théorème 7 permet d'écrire:

$$\sum_{E \in \mathcal{H}(P)} t^{|E|} = \sum_{E \in \mathcal{H}(P)} v(E) = \prod_{L \in \mathcal{L}(P)} (1 - v(L))^{-1} = \prod_{L \in \mathcal{L}(P)} (1 - t^{|L|})^{-1} .$$

En prenant le logarithme de ces séries, on obtient:

$$\sum_{D \in \mathcal{D}(P)} \frac{t^{|D|}}{|D|} = \log \sum_{E \in \mathcal{H}(P)} t^{|E|} = - \sum_{L \in \mathcal{L}(P)} \log(1 - t^{|L|}) = \sum_{m \geq 1} \frac{t^{m|L|}}{m} ,$$

la première égalité provenant d'un théorème de Viennot [Vi; proposition 5.10]. Soit  $L(n)$  le nombre d'empilements de Lyndon contenant  $n$  pièces et  $D(n)$  le nombre de pyramides comportant  $n$  pièces. En prenant le coefficient des termes en  $t^n$  dans la dernière équation, on trouve:

$$\frac{D(n)}{n} = \sum_{\substack{D \in \mathcal{D}(P) \\ |D|=n}} \frac{1}{n} = \frac{1}{n} \sum_{d|n} d L(d) .$$

Après simplification, une inversion de Mobius donne le prochain théorème.

**Théorème 10** Soit  $L(n)$  le nombre d'empilements de Lyndon contenant  $n$  pièces et  $D(n)$  le nombre de pyramides comportant  $n$  pièces. Alors:

$$L(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) D(d) . \blacksquare$$

Comme cas particulier, on remarquera qu'en non-commutatif, les pyramides sont les mots non-vides (il y en a  $k^d$  de longueur  $d$  si l'alphabet comporte  $k$  lettres). Le lecteur pourra aussi examiner le cas totalement commutatif. Par des méthodes similaires, on trouve des formules pour le nombre d'empilements de Lyndon suivant divers paramètres.

### Factorisation standard

**Définition 11** Soit  $E$  un empilement contenant au moins deux pièces. La factorisation standard de  $E$ , notée  $\Sigma(E)$ , est l'unique couple  $(F, N)$  d'empilements non-vides vérifiant:

- 1)  $E = F \circ N$ ,                      2)  $N$  est de Lyndon,                      3)  $N$  est minimal.

(La minimalité en jeu ici est relative à l'ordre lexicographique.) ■

**Théorème 12** Soit  $L$  un empilement de Lyndon contenant au moins deux pièces. Soit  $\Sigma(L) = (M, N)$  sa factorisation standard. Alors  $M$  est un empilement de Lyndon.

**Démonstration** Soit  $p = \inf(L)$ . Si  $L$  ne contient qu'une copie de  $p$ , alors  $M$  est une super-lettre. Dans le cas contraire,  $p = \inf(M) = \inf(N) = \sup(\min(N))$ . Passer aux mots standards associés et appliquer la théorie des mots de Lyndon. ■

**Théorème 13** Soit  $E$  un empilement contenant au moins deux pièces. Soit  $\Sigma(E) = (F, N)$  sa factorisation standard. Soit  $M$  un empilement de Lyndon. On a  $\Sigma(E \circ M) = (E, M)$  ssi  $M \leq N$ . ■

**Démonstration** Supposons que  $M \leq N$ . Soit  $\Sigma(E \circ M) = (U, V)$ .

On peut écrire  $V = V_1 \circ V_2$  où  $V_1$  est la partie de  $V$  qui se trouve dans  $M$  (voir fig. 6). Si  $V_1 = \Phi$ , alors  $V = V_2 \geq M$ . Par définition de la factorisation standard, on a  $V \leq M$ ; donc  $V = M$ . On peut donc supposer que  $V_1 \neq \Phi$ . Soit  $V_1 = L_1 \circ \dots \circ L_k$  la factorisation de Lyndon de  $V_1$  (pour un  $k \geq 1$ ). On a  $L_k \leq L_1 \leq V_1 \leq V \leq M \leq N$ . De plus,  $L_k$  est un facteur droit propre de  $E$  (sinon  $L_k = E = V_1$  et on aurait  $V = E \circ M$ ). Donc  $N \leq L_k$ ; d'où  $V = M$ .

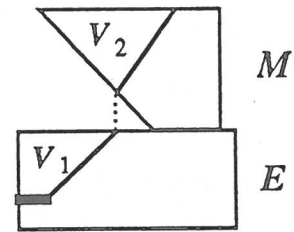


Fig. 6 Les empilements  $V_1$  et  $V_2$ .

Inversement, supposons que  $\Sigma(E \circ M) = (E, M)$  et que  $N < M$ . On a alors  $\inf(N) \leq \inf(M)$ . Soit  $D$  le facteur droit (propre) pyramidal de  $E \circ M$  tel que  $\min(D) = \min(N)$ . Soit  $D = L_1 \circ \dots \circ L_k$  la factorisation de Lyndon de  $D$ . L'empilement  $L_k$  est donc un facteur droit propre de  $E \circ M$  avec  $\inf(L_k) \leq \inf(L_1) = \pi(\min(N)) = \inf(N) < \inf(M)$ . Ceci contredit la factorisation standard de  $E \circ M$ . Donc  $\inf(N) = \inf(M)$ . Par le théorème 8,  $N \circ M$  est de Lyndon, et est un facteur droit propre de  $E \circ M$  vérifiant  $N \circ M < M$ . Ceci contredit encore la factorisation standard de  $E \circ M$ . On doit donc conclure que  $N \geq M$ . ■

**Théorème 14** Soit  $E$  un empilement contenant au moins deux pièces. Soit  $\Sigma(E) = (F, N)$  sa factorisation standard. On a alors  $\text{St}(E) = \text{St}(F)\text{St}(N)$ .

**Démonstration** On a  $\inf(N) \geq \inf(E) = \inf(F)$ . Si l'égalité se vérifie, le résultat est clair. Supposons donc que  $\inf(N) > \inf(E) = \inf(F)$ . Si  $F$  contient deux pièces en position  $\inf(F)$ , alors, comme au théorème 13, on peut extraire un empilement de Lyndon facteur droit propre de  $E$ , de base  $\inf(F)$ ; contradiction. Donc  $F$  et  $E$  sont les super-lettres  $p \circ F'$  et  $p \circ F' \circ N$  (respectivement). Un argument similaire montre que  $\inf(N) \leq \inf(F')$ . On a alors:

$$\text{St}(E) = \text{St}(p \circ F' \circ N) = p \text{St}(F' \circ N) = p \text{St}(F') \text{St}(N) = \text{St}(F) \text{St}(N). \quad \blacksquare$$

## Empilements de Lyndon et algèbres de Lie

Soit  $\mathfrak{L}(P)$  la sous-algèbre de Lie de  $\mathfrak{K}[\mathcal{H}(P)]$  (polynômes formels en  $\mathcal{H}(P)$  sur un anneau  $\mathfrak{K}$  donné). Deux positions non-concurrentes  $p$  et  $q$  vérifient donc:  $[p, q] = p \circ q - q \circ p = 0$ . Soit  $v = (v_p)_{p \in P}$  une suite d'entiers presque tous nuls indexés par  $P$ . On note  $\mathfrak{L}_v(P)$  le sous-module de  $\mathfrak{L}(P)$  composé des éléments de Lie homogènes de degré  $v_p$  en chaque position  $p \in P$ . De même,  $\mathfrak{L}_n(P)$  est la composante homogène de degré  $n$  de  $\mathfrak{L}(P)$ . Nous allons montrer que les empilements de Lyndon comportant  $v_p$  pièces en position  $p$  (pour tout  $p \in P$ ) donnent bijectivement une base de  $\mathfrak{L}_v(P)$ . Nous généraliserons une démonstration qu'on retrouve dans Lothaire [Lo] pour le cas totalement non-commutatif.

**Définition 15** Soit  $L$  un empilement de Lyndon. On pose:  $\Lambda(L) = L$  si  $L$  est réduit à une seule pièce. Dans le cas contraire, on pose  $\Lambda(L) = [\Lambda(M), \Lambda(N)]$ , où  $\Sigma(L) = (M, N)$ . ■

Il est clair que si  $|L|_p = v_p$  (pour tout  $p \in P$ ), alors  $\Lambda(L) \in \mathfrak{L}_v(P)$ .

**Théorème 16** Soit  $L$  un empilement de Lyndon. Posons  $\sum_E \alpha_E E = \Lambda(L)$ . On a  $\alpha_L = 1$ . De plus, si  $\alpha_E \neq 0$ , alors  $E \geq L$ .

**Démonstration** Si  $|L| = 1$ , le résultat est clair. Supposons que  $|L| \geq 2$ . Soit  $\Sigma(L) = (M, N)$ . On a  $\Lambda(L) = [\Lambda(M), \Lambda(N)]$ . Par induction, on peut écrire:

$$\Lambda(M) = \sum_{E \geq M} \alpha_E E, \quad \Lambda(N) = \sum_{F \geq N} \beta_F F.$$

avec  $\alpha_M = \beta_N = 1$ . Par linéarité, on a:

$$\Lambda(L) = \sum_{E \geq M} \sum_{F \geq N} \alpha_E \beta_F [E, F] = \sum_{E \geq M} \sum_{F \geq N} \alpha_E \beta_F (E \circ F - F \circ E).$$

On examine alors chaque terme.

Pour les termes de forme  $E \circ F$ ,

si  $E = M$  et  $F = N$ , on a  $\alpha_M \beta_N = 1$ ;

si  $E = M$  et  $F > N$ , ou si  $E > M$ , on a:  $\text{St}(E \circ F) \geq \text{St}(E)\text{St}(F) > \text{St}(M)\text{St}(N) = \text{St}(L)$   
(puisque  $|E| = |M|$ ); d'où  $E \circ F > L$ .

Pour ceux de la forme  $F \circ E$ , on a  $F \circ E > F \geq N > L$ . ■

Ce théorème montre donc que l'ensemble  $\{\Lambda(L): L \text{ est un empilement de Lyndon}\}$  est linéairement indépendant. Il est plus difficile de démontrer que ce même ensemble engendre  $\mathfrak{L}(P)$ . Pour réaliser cet objectif, nous introduisons un ordre sur les couples  $(L, M)$  d'empilements de Lyndon, puis nous formons une induction sur ceux-ci. Nous nous inspirons, en fait, de la preuve de Lothaire [Lo; ch. 5] pour les couples de mots de Lyndon. Cependant, dû à certaines particularités des empilements, l'ordre doit être modifié; sans compter que de nouveaux cas s'ajoutent à ceux énumérés par Lothaire. Remarquons, en passant, que si  $L$  et  $M$  sont des empilements de Lyndon non-connectés alors  $[\Lambda(L), \Lambda(M)] = 0$  (on



utilise la factorisation standard de  $L$  ou de  $M$ , les relations de Jacobi et on termine par une induction sur le nombre de pièces).

**Définition 17** Soit  $(L, M)$  et  $(L', M')$  des couples d'empilements de Lyndon vérifiant  $L < M$  et  $L' < M'$ . On écrit  $(L, M) \leq (L', M')$  si:

- 1)  $|L \circ M|_p < |L' \circ M'|_p$  pour toute position  $p \in P$       ou
- 2)  $|L \circ M|_p = |L' \circ M'|_p$  pour toute position  $p \in P$       et
  - 2.1)  $\inf(M) \in \zeta(L)$  et  $\inf(M') \notin \zeta(L')$       ou
  - 2.2)  $\inf(M) \in \zeta(L)$ ,  $\inf(M') \in \zeta(L')$  et  $M \leq M'$       ou
  - 2.3)  $\inf(M) \notin \zeta(L)$ ,  $\inf(M') \notin \zeta(L')$  et  $M \leq M'$ . ■

**Théorème 18** Soit  $L, M$  deux empilements de Lyndon tels que  $L < M$ . On peut écrire  $[\Lambda(L), \Lambda(M)] = \sum \alpha_N \Lambda(N)$  (avec  $\alpha_N$  entier), la somme portant sur tous les empilements de Lyndon  $N$  vérifiant  $N < M$ .

**Démonstration** Soit  $L, M$  des empilements de Lyndon vérifiant  $L < M$ . Nous développons plusieurs cas. Même si le nombre de ces cas peut sembler extravagant, les raisonnements s'appliquant à chacun d'eux sont tous plus ou moins apparentés. Nous avons à dessein repris la même disposition pour les présenter.

1) Supposons que  $\inf(M) \in \zeta(L)$ .

1.1) Supposons que  $|L| = 1$ .

Par le théorème 8,  $L \circ M$  est un empilement de Lyndon et  $L \circ M < M$ . De plus, on a clairement:  $\Sigma(L \circ M) = (L, M)$ . On peut donc écrire  $[\Lambda(L), \Lambda(M)] = \Lambda(L \circ M)$ .

1.2) Supposons que  $|L| > 1$ . Soit alors  $\Sigma(L) = (U, V)$ .

1.2.1) Supposons que  $V \geq M$ .

Dans ce cas, on a  $\inf(V) \geq \inf(M) \geq \inf(L)$ . Si  $\inf(M) = \inf(L)$ , alors  $L \circ M$  est un empilement de Lyndon (th. 8). Dans le cas contraire,  $\inf(V) > \inf(L)$ , ce qui signifie que  $L$  est une superlettre (sinon, on pourrait extraire de  $L$  un facteur droit propre de Lyndon de même base que  $L$  et qui serait inférieur à  $V$ ). Encore ici,  $L \circ M$  est un empilement de Lyndon. Par le théorème 13,  $\Sigma(L \circ M) = (L, M)$ . On aboutit à la même conclusion qu'au cas 1.1.

1.2.2) Supposons que  $V < M$ .

On peut écrire, en utilisant les relations de Jacobi:

$$\begin{aligned} [\Lambda(L), \Lambda(M)] &= [[\Lambda(U), \Lambda(V)], \Lambda(M)] \\ &= \pm [\Lambda(U), [\Lambda(V), \Lambda(M)]] \pm [\Lambda(V), [\Lambda(U), \Lambda(M)]] \end{aligned}$$

Nous examinons séparément chacun des deux derniers termes.

1.2.2.1)  $[\Lambda(U), [\Lambda(V), \Lambda(M)]]$ .

On sait que  $V < M$ . Comme  $(V, M) < (L, M)$  (définition 17, cas 1), on peut écrire (hypothèse d'induction):  $[\Lambda(V), \Lambda(M)] = \sum_{K < M} \alpha_K \Lambda(K)$  où  $K$  représente un empilement de

Lyndon et où les  $\alpha_k$  sont des entiers. Aussi,  $[\Lambda(U), [\Lambda(V), \Lambda(M)]]$  est une combinaison linéaire de termes de la forme  $[\Lambda(U), \Lambda(K)]$ . Nous examinons deux cas, suivant que  $U < K$  ou  $U > K$  (si  $K = U$ , on a évidemment  $[\Lambda(U), \Lambda(K)] = 0$ ).

1.2.2.1.1)  $[\Lambda(U), \Lambda(K)]$  avec  $U < K$ .

- Comme 1)  $|U \circ K|_p = |L \circ M|_p$  pour tout  $p \in P$ ,  
 2)  $\inf(K) = \inf(V \circ M) = \inf(V) \in \zeta(U)$ ,  
 3)  $K < M$ ,

alors  $(U, K) < (L, M)$  (déf.17, cas 2.2). On peut donc appliquer l'induction pour affirmer que  $[\Lambda(U), \Lambda(K)]$  est une combinaison linéaire (à coefficients entiers) de termes de la forme  $\Lambda(N)$  où  $N$  est un empilement de Lyndon vérifiant  $N < K$  (d'où  $N < M$ ).

1.2.2.1.2)  $[\Lambda(U), \Lambda(K)]$  avec  $U > K$ .

On examine alors  $[\Lambda(K), \Lambda(U)] = -[\Lambda(U), \Lambda(K)]$ .

- Comme 1)  $|K \circ U|_p = |L \circ M|_p$  pour tout  $p \in P$ ,  
 2)  $\inf(U) \geq \inf(K) = \inf(V) \geq \inf(U)$ , d'où  $\inf(U) \in \zeta(K)$ ,  
 3)  $U < V < M$ ,

alors  $(K, U) < (L, M)$  (déf.17, cas 2.2). L'hypothèse d'induction permet d'affirmer que  $[\Lambda(K), \Lambda(U)]$  est une combinaison linéaire de termes de la forme  $\Lambda(N)$  où  $N$  est un empilement de Lyndon vérifiant  $N < U$  (d'où  $N < M$ ).

1.2.2.2)  $[\Lambda(V), [\Lambda(U), \Lambda(M)]]$ .

Remarquons que  $U < V < M$ . Comme  $(U, M) < (L, M)$  (définition 17, cas 1), on a donc :  $[\Lambda(U), \Lambda(M)] = \sum_{K < M} \alpha_K \Lambda(K)$ . Aussi,  $[\Lambda(V), [\Lambda(U), \Lambda(M)]]$  est une combinaison linéaire entière de termes de la forme  $[\Lambda(V), \Lambda(K)]$ . Nous examinons deux cas, suivant que  $V < K$  ou  $V > K$ .

1.2.2.2.1)  $[\Lambda(V), \Lambda(K)]$  avec  $V < K$ .

- Comme 1)  $|V \circ K|_p = |L \circ M|_p$  pour tout  $p \in P$ ,  
 2)  $\inf(V) \leq \inf(K) = \inf(U \circ M) = \inf(U) \leq \inf(V)$ , d'où  $\inf(K) \in \zeta(V)$ ,  
 3)  $K < M$ ,

alors  $(V, K) < (L, M)$  (déf.17, cas 2.2). Ici encore, on applique l'induction pour affirmer que  $[\Lambda(V), \Lambda(K)]$  est une combinaison linéaire de termes de la forme  $\Lambda(N)$  où  $N$  est un empilement de Lyndon vérifiant  $N < K$  (d'où  $N < M$ ).

1.2.2.2.2)  $[\Lambda(V), \Lambda(K)]$  avec  $V > K$ .

On examine alors  $[\Lambda(K), \Lambda(V)] = -[\Lambda(V), \Lambda(K)]$ .

- Comme 1)  $|K \circ V|_p = |L \circ M|_p$  pour tout  $p \in P$ ,  
 2)  $\inf(V) \in \zeta(U) \subseteq \zeta(U \circ M) = \zeta(K)$ ,  
 3)  $V < M$ ,

alors  $(K, V) < (L, M)$  (déf.17, cas 2.2). On peut donc affirmer que  $[\Lambda(K), \Lambda(V)]$  est une combinaison linéaire de termes de la forme  $\Lambda(N)$  où  $N$  est un empilement de Lyndon vérifiant  $N < V$  (d'où  $N < M$ ).

2) Supposons que  $\inf(M) \notin \zeta(L)$ .

2.1) Supposons que  $|M| = 1$ .

Dans ce cas,  $L$  et  $M$  ne sont pas connectés et  $[\Lambda(L), \Lambda(M)] = 0$ .

2.2) Supposons que  $|M| > 1$ .

Soit alors  $\Sigma(M) = (R, S)$ . On peut écrire, en utilisant les relations de Jacobi:

$$\begin{aligned} [\Lambda(L), \Lambda(M)] &= [\Lambda(L), [\Lambda(R), \Lambda(S)]] \\ &= \pm [[\Lambda(L), \Lambda(S)], \Lambda(R)] \pm [[\Lambda(L), \Lambda(R)], \Lambda(S)]. \end{aligned}$$

Nous examinons séparément chacun des deux derniers termes.

2.2.1)  $[[\Lambda(L), \Lambda(S)], \Lambda(R)]$ .

Remarquons que  $L < M < S$ . Comme  $(L, S) < (L, M)$ , on peut écrire:  $[\Lambda(L), \Lambda(S)] = \sum_{K < S} \alpha_K \Lambda(K)$ . Aussi,  $[[\Lambda(L), \Lambda(S)], \Lambda(R)]$  est une combinaison linéaire de termes de la forme  $[\Lambda(K), \Lambda(R)]$ . Remarquons que  $\inf(K) = \inf(L \circ S) = \inf(L) < \inf(M) = \inf(R)$  (la dernière inégalité est stricte puisque  $\inf(M) \notin \zeta(L)$ ). On a donc  $K < R$ . De plus, comme

$$1) |K \circ R|_p = |L \circ M|_p \text{ pour tout } p \in P,$$

$$2) R < M,$$

alors  $(K, R) < (L, M)$  (déf.17, cas 2.1 ou 2.3). Aussi  $[\Lambda(K), \Lambda(R)]$  est une combinaison linéaire de termes de la forme  $\Lambda(N)$  où  $N$  est un empilement de Lyndon vérifiant  $N < R$  (d'où  $N < M$ ).

2.2.2)  $[[\Lambda(L), \Lambda(R)], \Lambda(S)]$ .

Remarquons que  $\inf(L) < \inf(M) = \inf(R)$ , d'où  $L < R$ . Comme  $(L, R) < (L, M)$ , on a:  $[\Lambda(L), \Lambda(R)] = \sum_{K < R} \alpha_K \Lambda(K)$ . Aussi,  $[[\Lambda(L), \Lambda(R)], \Lambda(S)]$  est une combinaison linéaire de termes de la forme  $[\Lambda(K), \Lambda(S)]$ . Remarquons que  $K < R < S$ . De plus, comme

$$1) |K \circ S|_p = |L \circ M|_p \text{ pour tout } p \in P,$$

$$2) \inf(S) \in \zeta(R) \subseteq \zeta(L \circ R) = \zeta(K),$$

alors  $(K, S) < (L, M)$  (déf.17, cas 2.1). Ainsi  $[\Lambda(K), \Lambda(S)]$  est une combinaison linéaire de termes de la forme  $\Lambda(N)$  où  $N$  est un empilement de Lyndon. Mais  $\inf(N) = \inf(L \circ M) = \inf(L) < \inf(M)$ ; aussi, on a:  $N < M$ . ■

**Remarques** On peut éliminer le cas 1.2.2.1.2 ( $U > K$ ) en demandant dans l'hypothèse d'induction que  $\text{St}(N) \geq \text{St}(L)\text{St}(M)$ . Ceci a l'avantage de rapprocher la présente démonstration de celle de Lothaire. Bien sûr, on paie par l'augmentation des vérifications dans chacun des autres cas.

Le théorème 18 montre que le module engendré par  $\{\Lambda(L): L \text{ est un empilement de Lyndon}\}$  est une sous-algèbre de Lie de  $\mathfrak{L}(P)$  contenant  $P$ . La minimalité de cette dernière assure que ce module et  $\mathfrak{L}(P)$  sont égaux. Grâce au théorème 10, on connaît la dimension de chacune de ses composantes homogènes.

Notons que  $\mathfrak{K}[\mathcal{H}(P)]$  est l'algèbre enveloppante de  $\mathfrak{L}(P)$ , un résultat dû à Thibon [Th]. D'autres bases de  $\mathfrak{L}(P)$  apparaissent dans les travaux de Duchamp et Krob [DK]. Ils obtiennent alors des formules de Witt analogues à celle présentée ici.

L'auteur remercie le comité de lecture du Colloque pour les suggestions qui ont permis l'amélioration de cet article.

## Bibliographie

- [CF] P. CARTIER et D. FOATA. *Problèmes combinatoires de commutations et réarrangements*. Lecture Notes in Math., 85, Springer-Verlag, (1969).
- [CMZ] R. CORI, Y. METIVIER, W. ZIELONKA. *Asynchronous mapping and asynchronous cellular automata*. LABRI, Rapport # 89-97, Bordeaux, (1990).
- [DK] G. DUCHAMP, D. KROB. *The free partially commutative Lie algebra: Bases and Ranks*. Rapport LITP # 90.87, Paris, (1990).
- [Du] C. DUBOC. *Commutations dans les monoïdes libres: un cadre théorique pour l'étude du parallélisme*. Thèse de l'université de Rouen, (1986).
- [La1] P. LALONDE. *Contribution à l'étude des empilements*. thèse de doctorat, UQAM, Montréal, (1990).
- [La2] P. LALONDE. *Lyndon Heaps: an Analogue of Lyndon Words in Partially Commutative Monoids*. (soumis à Discrete Mathematics).
- [Lo] LOTHAIRE. *Combinatorics on words*. Encyclopedia of Math., 17, Addison Wesley, Reading, (1983).
- [Th] J. Y. THIBON. *Intégrité des algèbres de séries formelles sur un alphabet partiellement commutatif*. T.C.S., 41, (1985), 109-112.
- [Vi] G.X. VIENNOT. *Heaps of pieces, I: Basic definitions and combinatorial lemmas*, dans: G. Labelle, P. Leroux, eds., *Combinatoire Énumérative*, Lecture Notes in Math., 1234, Springer-Verlag, (1986), 321-350.