Discrete Mathematics 76 (1989) 123–129
North-Holland

LE SUPPORT DE L'ALGEBRE DE LIE LIBRE

G. DUCHAMP and J.Y. THIBON
L.I.T.P., Université Paris VII, 2 Place Jussieu, 75251 Paris Cédex 05, France

Received April 7, 1987

We characterize the words appearing as monomials in Lie polynomials.

1. Introduction

L'algèbre de Lie libre (à coefficients dans $\mathbb{Z}$) sur un alphabet A peut être vue comme l'ensemble des polynômes non commutatifs obtenus à partir des lettres de A au moyen du crochet de Lie $[x, y] = xy - yx$, et par combinaison linéaire de telles expressions. Les mots du monoïde libre A^* n'apparaissent pas tous dans les polynômes ainsi formés: par exemple, pour $a \in A$, il est clair que le mot aa ne figure dans aucun polynôme de Lie. M.P. Schützenberger a posé la question de déterminer les mots qui n'apparaissent jamais. Nous y répondons dans cet article.

2. Notations et rappels

Dans ce qui suit, A désigne un alphabet (fini ou non), A^* le monoïde libre sur A et $A^+ = A^* - \{1\}$ le semigroupe libre.

On notera $|w|$ la longueur d'un mot $w \in A^*$.

On note $\mathbb{Z}\langle A\rangle$ la $\mathbb{Z}$-algèbre associative libre sur A, $\mathbb{Z}\langle\langle A\rangle\rangle$ l'algèbre des séries formelles non commutatives sur A, et $L(A)$ la $\mathbb{Z}$-algèbre de Lie libre sur A, i.e. la sous-algèbre de Lie de $\mathbb{Z}\langle A\rangle$ (pour la structure de Lie canonique $[x, y] = xy - yx$) engendrée par A. Les éléments de $L(A)$ sont appelés polynômes de Lie. Le fait que $L(A)$ soit effectivement libre, i.e. que toute application de A dans une algèbre de Lie $\mathfrak{g}$ s'étende de manière unique à un morphisme de $L(A)$ dans $\mathfrak{g}$ n'est pas trivial: c'est une conséquence du théorème de Poincaré–Birkhoff–Witt, qui montre aussi que $\mathbb{Z}\langle A\rangle$ est l'algèbre enveloppante de $L(A)$. Pour toutes ces questions, voir [2, 3].

On appelle composante homogène de degré n de $L(A)$ le sous-module noté $L^n(A)$, formé des polynômes de Lie homogènes de degré n. On note $\mathbb{Z}_n\langle A\rangle$ l'ensemble de tous les polynômes homogènes de degré n. Si $\mathfrak{g}$ est une algèbre de Lie et $x \in \mathfrak{g}$, on appelle adjointe de x l'endomorphisme (pour la structure de module) de $\mathfrak{g}$ noté $\mathrm{ad}(x)$ et défini par: $\mathrm{ad}(x)(y) = [x, y]$. C'est une dérivation de

$\mathfrak{g}$ (conséquence de l'identité de Jacobi). On définit sur $\mathbb{Z}\langle A\rangle$ un produit scalaire par:

$$\text{si } u, v \in A^* \quad (u, v) = \begin{cases} 1 & \text{si } u = v \\ 0 & \text{si } u \neq v \end{cases}$$

est prolonge par bilinéarité. Pour $f \in \mathbb{Z}\langle\langle A\rangle\rangle$ et $w \in A^*$, on désigne encore par (f, w) le coefficient de w dans f. Pour $P, Q \in \mathbb{Z}\langle A\rangle$ et $a \in A$, on a: $(aP, aQ) = (P, Q) = (Pa, Qa)$.

L'image miroir d'un mot $w = x_1 \ldots x_n \in A^*$ $(x_i \in A)$ est par définition le mot $\tilde{w} = x_n \ldots x_1$. On prolonge cette opération à $\mathbb{Z}\langle\langle A\rangle\rangle$ par linéarité: si $f = \sum_{w \in A^*} (f, w)w$, $\tilde{f} = \sum_{w \in A^*} (f, w)\tilde{w}$. Un palindrôme est un mot tel que $\tilde{w} = w$.

Dan la suite, nous noterons P l'ensemble des palindrômes de longueur paire, N l'ensemble des mots de la forme a^k, avec $a \in A$ et $n \geqslant 2$. On pose $S = P \cup N \cup \{1\}$. On appelle support d'un polynôme ou d'une série f l'ensemble:

$$\text{supp}(f) = \{w \in A^* \mid (f, w) \neq 0\}.$$

Lorsqu'il n'y a pas de risque de confusion avec la longueur d'un mot, le support de f est aussi noté $|f|$. On appelle support d'une partie de $\mathbb{Z}\langle\langle A\rangle\rangle$ la réunion des supports de ses éléments.

Rappelons aussi une propriété simple:

Lemme. *Soient $\mathfrak{g}$ une algèbre de Lie sur un anneau $\mathcal{A}$ et σ un automorphisme de $\mathfrak{g}$. Pour $\alpha \in \mathcal{A}$ posons*:

$$\mathfrak{g}_\alpha = Ker(\sigma - \alpha Id)$$

Alors, $\bigoplus_{\alpha \in \mathcal{A}} \mathfrak{g}_\alpha$ est une sous-algèbre de Lie de $\mathfrak{g}$, graduée par le monoïde multiplicatif $(\mathcal{A}, .)$.

Preuve. Si $x \in \mathfrak{g}_\alpha$, $y \in \mathfrak{g}_\beta$, $\sigma([x, y]) = [\sigma(x), \sigma(y)] = [\alpha x, \beta y] = \alpha\beta[x, y]$ donc $[x, y] \in \mathfrak{g}_{\alpha\beta}$. □

3. Résultats

Voici la caractérisation annoncée:

Théorème. *Les mots qui n'apparaissent pas dans les polynômes de Lie sont exactement*:

1. *les mots de la forme a^n, $a \in A$, $n \geqslant 2$*
2. *les palindrômes de longueur paire.*

Avec les notations de la Section 2, le support de $L(A)$ est donc le complémentaire de S dans A^*.

La démonstration occupe les Sections 4 à 6. Dans la Section 4 nous définissons des systèmes générateurs de $L(A)$ adaptés au problème. Leur comportement par rapport à l'opération d'image miroir (Lemmes 5 à 8) permet (Section 5) de comprendre pourquoi les mots de S n'apparaissent jamais. La réciproque, i.e. le fait que tout mot de $A^* - S$ apparaît dans au moins un polynôme de Lie, est établie au Section 6, essentiellement au moyen d'une formule du type Leibniz permettant de calculer les puissances de l'adjointe d'une lettre (Lemme 3).

4. Adjointes itérées

On définit une application $\pi: A^+ \to L(A)$ récursivement par: si $a \in A$, $\pi(a) = a$ et pour $w \in A^+$, $\pi(aw) = \mathrm{ad}(a)\pi(w)$. Autrement dit, si $w = a_1 \cdots a_n$ avec $a_i \in A$,

$$\pi(w) = (\mathrm{ad}(a_1) \circ \mathrm{ad}(a_2) \circ \cdots \circ \mathrm{ad}(a_{n-1}))(a_n) = [a_1, [a_2, [\ldots, a_n] \ \ldots]].$$

On définit également $\varphi: A^+ \to L(A)$ par: pour $a \in A$, $\varphi(a) = a$, et $\varphi(wa) = [\varphi(w), a] = -\mathrm{ad}(a)\varphi(w)$. Ces deux applications permettent de construire des systèmes générateurs de $L(A)$ bien adaptés au problème.

Lemme 1. $\pi(w) = \widetilde{\varphi(\tilde{w})}$.

La preuve est laissée au lecteur. □

Lemme 2. *$(\pi(w))_{w \in A^n}$ engendre $L^n(A)$ en tant que $\mathbb{Z}$-module.*

Preuve. Voir [1], Ch. II, 2, Prop. 7. □

Corollaire. *$(\varphi(w))_{w \in A^n}$ engendre $L^n(A)$.*

Lemme 3. *Pour $x, y \in \mathbb{Z}\langle A \rangle$, on a la formule:*

$$(\mathrm{ad}(x))^n(y) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k x^{n-k} y x^k.$$

Preuve. Par récurrence sur n: pour $n = 0$, la formule donne $y = y$, et:

$$\begin{aligned}
(\mathrm{ad}(x))^{n+1}(y) &= \sum_{k=0}^{n} \binom{n}{k} (-1)^k (x^{n+1-k} y x^k - x^{n-k} y x^{k+1}) \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k x^{n+1-k} y x^k - \sum_{k=1}^{n+1} \binom{n}{k-1} (-1)^{k-1} x^{n+1-k} y x^k \\
&= \sum_{k+1}^{n} \binom{n+1}{k} (-1)^k x^{n+1-k} y x^k + x^{n+1} y + (-1)^{n+1} y x^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^k x^{n+1-k} y x^k. \quad \square
\end{aligned}$$

Donnons maintenant une formule pour le calcul de $\varphi(w)$. Dans ce qui suit, $(\mathbb{N})^*$ désigne le monoïde libre d'alphabet l'ensemble des entiers naturels $\mathbb{N}$. Considérons la série formelle $E \in \mathbb{Z}\langle\langle\mathbb{N}\rangle\rangle$ dont les composantes homogènes $E_n \in \mathbb{Z}_n\langle N\rangle$ sont définies récursivement par les formules:

$$\begin{cases} E_1 = 1 \\ E_{n+1} = E_n(n+1) - (n+1)E_n \end{cases}$$

On note $|E_n|$ le support du polynôme E_n. Une récurrence immédiate montre que tout mot de $|E_n|$ est de la forme $m = i_1 \cdots i_n$, où $(i_1, \ldots, i_n)$ est une permutation de $(1, \ldots, n)$. Ainsi, tout mot $m \in (\mathbb{N})^*$ tel que $(E_n, m) \neq 0$ définit une permutation $\sigma_m \in \mathfrak{S}_n$ par $m = \sigma_m(1) \cdots \sigma_m(n)$. On pose $\mu(m) = (E_n, m)$, avec $n = |m|$. Remarquons qu'on a toujours $\mu(m) = \pm 1$ lorsque $m \in |E_n|$. De plus, si $m' \in |E_{n-1}|$,

$$\mu(m'n) = \mu(m'), \qquad \mu(nm') = -\mu(m').$$

Pour $w \in A^n$ et $m \in |E_n|$, on pose $w_m = x_{\sigma_m(1)} \cdots x_{\sigma_m(n)}$ $(w = x_1 \cdots x_n)$.

Avec ces notations, on *a*:

Lemme 4. $\varphi(w) = \sum_{m \in |E_n|} \mu(m) w_m$.

Preuve. Par récurrence sur $|w|$: pour $|w| = 1$, $\varphi(w) = w$ et la formule est vérifiée. Si maintenant $w = x_1 \cdots x_n \in A^n$, et $x_{n+1} \in A$,

$$\begin{aligned} \varphi(wx_{n+1}) &= [\varphi(w), x_{n+1}] = \varphi(w)x_{n+1} - x_{n+1}\varphi(w) \\ &= \sum_{m \in |E_n|} \mu(m) w_m x_{n+1} - \sum_{m \in |E_n|} \mu(m) x_{n+1} w_m \\ &= \sum_{p \in |E_{n+1}|} \mu(p)(wx_{n+1})_p. \quad \square \end{aligned}$$

Lemme 5. $\tilde{E}_n = (-1)^{n+1} E_n$. *En particulier,* $|\tilde{E}_n| = |E_n|$.

Preuve. Par récurrence:

$$E_1 = 1 = \tilde{E}_1$$

$$E_2 = 12 - 21 = -\tilde{E}_2$$

Alors,

$$\begin{aligned} E_{2n+1} &= E_{2n}(2n+1) - (2n+1)E_{2n} = (-E_{2n})(2n+1) \\ &\quad - (2n+1)(-E_{2n}) = E_{2n+1}. \end{aligned}$$

De même, $E_{2n+2} = -\tilde{E}_{2n+2}$. $\square$

Lemme 6. $w_{\tilde{m}} = \widetilde{(w_m)}$.

Preuve. Laissée au lecteur. $\square$

Lemme 7. *Soit* $n = |w|$. *Alors* $\widetilde{\varphi(w)} = (-1)^{n+1}\varphi(w)$.

Preuve.

$$\widetilde{\varphi(w)} = \sum_{m\in|E_n|} \mu(m)\tilde{w}_m = \sum_{m\in|E_n|} \mu(m)w_{\tilde{m}} = \sum_{p\in|E_n|} \mu(\tilde{p})w_p$$
$$= (-1)^{n+1} \sum_{p\in|E_n|} \mu(p)w_p = (-1)^{n+1}\varphi(w). \quad \square$$

Soit σ l'automorphisme d'algèbre de Lie de $\mathbb{Z}\langle A\rangle$ défini par $\sigma(P) = -\tilde{P}$. Posons comme à la Section 2 $[\mathbb{Z}\langle A\rangle]_\alpha = \{P \in \mathbb{Z}\langle A\rangle \mid \sigma(P) = \alpha P\}$.

Lemme 8. $L^{2n}(A) \subset [\mathbb{Z}\langle A\rangle]_1$ *et* $L^{2n+1}(A) \subset [\mathbb{Z}\langle A\rangle]_{-1}$.

Preuve. En effet, $(\varphi(w))_{w\in A^k}$ engendre $L^k(A)$. $\square$

5. Non-apparition des mots de S dans $L(A)$

Il est maintenant facile d'établir que les mots de S n'apparaissent pas dans $L(A)$.

En effet, comme les $\varphi(w)$ engendrent $L(A)$, tout mot qui apparaît dans $L(A)$ apparaît dans au moins un $\varphi(w)$. Or $\varphi(a^n) = 0$ pour tout $a \in A$ dès que $n \geqslant 2$. Soit maintenant $w = x\tilde{x}$ un palindrôme de longueur paire. Il est clair qu'on a pour tout polynôme $P \in \mathbb{Z}\langle A\rangle$ et tout mot $v \in A^*$:

$$(\tilde{P}, \tilde{v}) = (P, v).$$

Si w apparaît dans $L(A)$, il apparaît dans un $\varphi(u)$ avec $|u| = |w| = 2n$. Mais alors,

$$(\varphi(u), w) = (-\widetilde{\varphi(u)}, w) = (-\widetilde{\varphi(u)}, \tilde{w}) = -(\widetilde{\varphi(u)}, \tilde{w}) = -(\varphi(u), w),$$

d'où $(\varphi(u), w) = 0$. $\square$

6. Un polynôme pour tout mot $w \in A^* - S$

Montrons maintenant la réciproque, i.e. que pour tout mot $w \in S$, il existe un polynôme de Lie $P \in L(A)$ tel que $(P, w) \neq 0$.

La preuve se fait par récurrence sur la longueur n de w. Pour $n = 1$ ou 2, c'est immédiat: $A \cap L(A)$, et si $a, b \in A$, $([a, b], ab) = 1$. Si $n \geqslant 3$, w peut s'écrire sous la forme:

$$w = xvy \quad \text{avec} \quad x, y \in A \quad \text{et} \quad v \in A^+.$$

On distingue alors deux cas:

6.1. *Premier cas*: $x \neq y$

Alors, xv ou $vy \notin S$ (en effet, tous les éléments de S commencent et finissent par la même lettre). Supposons par exemple $xv \notin S$. Alors, par l'hypothèse de récurrence, il existe $Q \in L(A)$ tel que $(Q, xv) \neq 0$, et on a:

$$([Q, y], w) = ([Q, y], xvy) = (Qy, xvy) - (yQ, xvy) = (Q, xv) \neq 0.$$

6.2. *Deuxième cas*: $x = y$

w est alors de la forme $x^c z x^f$, où $z \in A^+$ ne commence ni ne finit par x.

6.2.1.

Si $z \notin S$, il existe $Q \in L(A)$ tel que $(Q, z) \neq 0$. Soit $P = (\mathrm{ad}(x))^{c+f}(Q)$. Par le Lemme 3,

$$P = \sum_{k=0}^{c+f} \binom{c+f}{k} (-1)^k x^{c+f-k} Q x^k,$$

Si $q \in \mathrm{Supp}(Q)$ est tel que $x^{c+f-k} q x^k = x^c z x^f$, on a $c+f-k \leqslant c$ et $k \leqslant f$, d'où $k = f$ et $q = z$; donc:

$$(P, w) = (P, x^c z x^f) = \binom{c+f}{f} (-1)^f (Q, z) \neq 0.$$

6.2.2.

Si $z = u\tilde{u}$ alors $c \neq f$ sinon $w \in S$. Il existe alors $Q \in L(A)$ tel que $(Q, xz) \neq 0$. En effet, z ne commence ni ne finit par x donc $xz \notin S$. Comme Q est de degré impair, $Q = \tilde{Q}$; de plus $\widetilde{zx} = zx$, donc $(Q, zx) = (\tilde{Q}, \widetilde{zx}) = (Q, xz)$. Considérons alors le polynôme de Lie p défini par:

$$P = (\mathrm{ad}(x))^{c+f-1}(Q) = \sum_{k=0}^{C+f-1} \binom{c+f-1}{k} (-1)^k x^{c+f-1-k} Q x^k.$$

Soit $q \in \mathrm{Supp}(Q)$ tel que $x^{c+f-1-k} q x^k = x^c z x^f = w$. Alors, $c+f-1-k \leqslant c$ et $k \leqslant f$, d'où $f-1 \leqslant k \leqslant f$. Si $k = f-1$ alors $x^c q x^{f-1} = x^c z x^f$ d'où $q = zx$, et si $k = f$, $x^{c-1} q x^f = x^c z x^f$ entraîne $q = xz$. Par conséquent,

$$(P, w) = (P, x^c z x^f) = \left[\binom{c+f-1}{f-1}(-1)^{f-1} + \binom{c+f-1}{f}(-)^f\right](Q, xz)$$

$$= (Q, xz)(-1)^{f-1}\left[\binom{c+f-1}{f-1} - \binom{c+f-1}{f}\right] \neq 0$$

car par hypothèse, $c \neq f$ et donc $f+f-1 \neq c+f-1$.

6.2.3.

$z = a^k$, $a \in A$, $k \geqslant 1$.

6.2.3.1. Si $c \neq f$, la preuve est analogue à celle de 6.2.2, à ceci près que $(Q, zx) = (-1)^k (Q, xz)$.

6.2.3.2. Si $c = f$, k est impair, sinon $w \in S$. Calculons alors

$$\begin{aligned} P &= \varphi(xa^k x^{2c-1}) = (-\mathrm{ad}(x))^{2c-1}(\varphi(xa^k)) \\ &= (-1)^{2c-1} \sum_{j=0}^{2c-1} \binom{2c-1}{j} (-1)^j x^{2c-1-j} \varphi(xa^k) x^j \\ &= (-1)^{2c-1} \sum_{j=0}^{2c-1} \binom{2j-1}{j} (-1)^j x^{2c-1-j} \left[(-1)^k \sum_{i=0}^{k} \binom{k}{i} (-1)^i a^{k-i} \cdot x a^i \right] x^j \\ &= (-1)^{2c+k-1} \sum_{j=0}^{2c-1} \sum_{i=0}^{k} \binom{2c-1}{j} \binom{k}{i} (-1)^{i+j} x^{2c-1-j} a^{k-i} x a^i x^j. \end{aligned}$$

On voit que $w = x^c a^k x^c$ n'apparaît dans cette expression que pour $(i, j) = (0, c-1)$ et (k, c). Donc,

$$\begin{aligned} (P, w) &= (-1)^{2c+k-1} \left[\binom{2c-1}{c-1} \binom{k}{0} (-1)^{c-1} + \binom{2c-1}{c} \binom{k}{k} (-1)^{c+k} \right] \\ &= (-1)^{3c+k-2} \left[\binom{2c-1}{c-1} + \binom{2c-1}{c} \right] \quad (k \text{ est impair}), \end{aligned}$$

et donc $(P, w) \neq 0$. □

Références

[1] N. Bourbaki, Groupes et algèbres de Lie, Ch. 2 et 3 (Hermann, Paris, 1972).
[2] N. Jacobson, Lie algebras (Wiley, New York, 1962).
[3] M. Lothaire, Combinatorics on words (Addison-Wesley, Reading, Mass. 1983).