Séminaire Lotharingien de Combinatoire **54** (2006), Article B54h

MOTS DE LYNDON GÉNÉRALISÉS

CHRISTOPHE REUTENAUER*

Dédié à mon ami Xavier Viennot

ABSTRACT. By choosing for each position i of infinite words in $A^{\mathbb{N}}$ a total order on A, one defines a lexicographical order on $A^{\mathbb{N}}$. It allows to define generalized Lyndon words. They factorize the free monoid, form Hall sets and give bases of the free Lie algebras. The main example, apart from usual Lyndon words, are the Galois words, obtained through the alternate lexicographical order on $A^{\mathbb{N}}$. They have several number-theoretical applications : Galois numbers, their homographics classes, binary indefinite quadratic forms, Markoff numbers.

1. INTRODUCTION

Un mot w sur l'alphabet totalement ordonné A est un *mot de Lyndon* si pour toute factorisation non triviale $w = uv$, la suite w^∞ est strictement plus petite que la suite $(vu)^\infty$, pour l'ordre lexicographique sur $A^{\mathbb{N}}$.

Nous introduisons la variante suivante : étant donnée une suite $<_i, i = 0, 1, 2, \ldots$ d'ordres totaux sur A, nous considérons l'ordre lexicographique sur $A^{\mathbb{N}}$ obtenu en considérant en chaque position i l'ordre $<_i$. Ainsi $a_0a_1a_2\ldots < b_0b_1b_2\ldots$ si : $a_0 <_0 b_0$, ou $a_0 = b_0$ et $a_1 <_1 b_1$, ou $a_0 = b_0, a_1 = b_1$ et $a_2 <_2 b_2$, etc... Un mot de Lyndon généralisé, pour cet ordre fixé $<$, s'obtient par la même définition que ci-dessus.

Nous montrons que ces mots de Lyndon généralisés forment une factorisation complète du monoïde libre (Th. 2.1). Pour ce faire, nous avons recours aux ensembles de Hall, généralisés par Shirshov et Viennot. Nous montrons que l'ensemble des mots de Lyndon généralisés est un ensemble de Hall (Th. 2.2). Le lemme crucial donne une propriété combinatoire de l'ordre $<$ sur $A^{\mathbb{N}}$ (lemme 2.1). Le théorème de Fine et Wilf se révèle également utile (voir lemme 2.2). Une fois qu'on sait que l'ensemble des mots de Lyndon généralisés forme un ensemble de Hall, il s'ensuit directement que c'est une factorisation du monoïde libre. Comme autre conséquence, on tire que les polynômes de Lie associés forment une base de l'algèbre de Lie libre.

L'exemple motivateur de ces ordres et de ces ensembles vient des fractions continues : on prend sur $A^{\mathbb{N}}$ l'*ordre lexicographique alterné* (cf. [Ca, p. 11]), c'est-à-dire

*Université du Québec à Montréal; Département de mathématiques; Case postale 8888, succursale Centre-Ville, Montréal (Québec) Canada, H3C 3P8 (mailing address); e-mail : `christo@math.uqam.ca`.

$<_i=<_0$ si i pair, $<_i=<_1$ si i impair, et de plus $<_0$ et $<_1$ sont des ordres opposés. Alors $a_0a_1a_2\ldots < b_0b_1b_2\ldots$ si et seulement si

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots}}} < b_0+\cfrac{1}{b_1+\cfrac{1}{b_2+\cfrac{1}{\ddots}}},$$

l'où l'on a supposé que les a_i, b_j sont des entiers strictement positifs, avec $<_0$ l'ordre usuel et $<_1$ l'ordre opposé. Nous appelons *mots de Galois* les mots de Lyndon généralisés correspondant à cet ordre.

Les mots de Galois sont en bijection naturelle avec les classes homographiques de nombres de Galois ; α est un *nombre de Galois* si α est un réel algébrique de degré 2, si $\alpha > 1$ et si son conjugué est dans $]-1,0[$: son développement en fraction continue est w^∞, où w est le mot de Galois qui lui correspond dans la bijection ci-dessus. Une classe homographique est une orbite sous le groupe des homographies $\frac{az+b}{cz+d}$, où $a,b,c,d \in \mathbb{Z}, ad-bc=\pm 1$.

Dans une telle classe, le plus petit nombre de Galois correspond à un mot de Galois ; on peut donc le calculer en utilisant un algorithme de Schützenberger–Melançon. Les mots de Galois sont aussi en bijection avec les classes de formes quadratiques binaires indéfinies. D'autre part, nous utilisons l'ordre lexicographique pour retrouver une partie des résultats de Markoff [M1], [M2] (voir aussi [D2], [CF]). Notre approche utilise les mots de Christoffel et leurs symétries, et permet de retrouver le calcul des nombres de Markoff, entre autres une formule de Harvey Cohn [C].

Nous concluons l'article en mentionnant le spectre de Cassaigne [Ca] et les factorisations de Viennot.

2. Mots de Lyndon généralisés

Soit A un alphabet et $A^{\mathbb{N}}$ l'ensemble des suites sur A. Considérons une suite $<_0, <_1, <_2, \ldots$ d'ordres totaux sur A. Nous définissons l'ordre $<$ sur $A^{\mathbb{N}}$ par : $s<t$ si $s_0 <_0 t_0$, ou $s_0=t_0$ et $s_1 <_1 t_1$, ou $s_0=t_0, s_1=t_1$ et $s_2 <_2 t_2$, etc...

Si w est un mot non vide dans A^* (le monoïde libre sur A), w^∞ désigne la suite dans $A^{\mathbb{N}}$ obtenue en répétant w une infinité de fois. Nous dirons que w est un *mot de Lyndon généralisé* (relatif aux ordres $<_0, <_1, <_2, \ldots$) si pour toute factorisation non triviale $w=uv$, on a $w^\infty < (vu)^\infty$. Remarquons tout de suite que dans ce cas, w est primitif, i.e. n'est pas une puissance pure : en effet $w=x^n$ avec $n\geq 2$ implique une factorisation $w=uv=x^{n-1}x$ avec $w^\infty=(vu)^\infty$.

Exemples

1. Si nous prenons $<_i=<_0$ pour tout i dans $\mathbb{N}$, nous obtenons l'ordre lexicographique usuel sur $A^{\mathbb{N}}$. Pour des mots u,v d'égale longueur dans A^*, on a $u^\infty < v^\infty$ si et

seulement si u est plus petit que v dans l'ordre lexicographique usuel sur A^*. Donc un mot de Lyndon généralisé est un mot de Lyndon usuel, voir Lothaire [L, p. 64].

2. Nous choisissons ici l'*ordre lexicographique alterné* sur $A^{\mathbb{N}}$, c'est-à-dire : $<_i=<_0$ si i pair, $<_i=<_1$ si i impair, et de plus $<_0$ est l'ordre opposé à $<_1$. Par exemple, pour $A=\mathbb{P}$ (l'ensemble des nombres entiers naturels non nuls), on prend pour $<_0$ l'ordre naturel et pour $<_1$ l'ordre opposé. On a donc $1\ldots<2\ldots$ et $12\ldots<11\ldots$.

Nous appellerons *mot de Galois* un mot de Lyndon généralisé pour ce choix des ordres $<_i$; nous justifierons cette terminologie plus loin. Avec $A=\mathbb{P}$ comme ci-dessus, nous avons entre autres les mots de Galois :

$$1, 2, 3, 12, 4, 13, 121, 5, 14, 23, 122, 1211, \ldots,$$

énumérés par poids croissant (le poids est ici la somme des chiffres).

Nous allons donner une caractérisation des mots de Lyndon généralisés, semblable à celle des mots de Lyndon [L, Prop. 5.1.2] : w est un mot de Lyndon si et seulement si w est plus petit que tous ses suffixes non triviaux pour l'ordre alphabétique.

Proposition 2.1. *Un mot w est un mot de Lyndon généralisé si et seulement si pour toute factorisation non triviale $w=uv$ on a $w^\infty<v^\infty$.*

Nous aurons besoin du fait bien connu suivant : pour u,v dans $A^+=A^*\backslash\{\varepsilon\}$, où ε désigne le mot vide, on a $u^\infty=v^\infty$ si et seulement si u et v sont puissances d'un même mot.

Par ailleurs, nous utiliserons la terminologie suivante : si s,t sont deux éléments distincts de $A^{\mathbb{N}}$, avec une factorisation $s=u_1\ldots u_k s'$ ($u_1,\ldots,u_k$ sont des mots finis, et $s'\in A^{\mathbb{N}}$), nous dirons que *la comparaison entre* s et t *se fait dans* u_k si $u_1\ldots u_{k-1}$ est préfixe de t, mais pas $u_1\ldots u_k$. Avec ceci, on peut écrire $t=u_1\ldots u_{k-1}u'_k t'$, où $|u'_k|=|u_k|, u'_k\neq u_k$, et l'ordre entre s et t est le même qu'entre n'importe quelles suites $u_1\ldots u_k\ldots$ et $u_1\ldots u_{k-1}u'_k\ldots$. Nous utiliserons constamment cette remarque dans la suite.

Preuve.
0. Si $w,v\in A^+$ et $w^\infty\neq v^\infty$, nous pouvons écrire $w^\infty=v^n s$, où n est maximum ; donc v n'est pas préfixe de s et $s=v's', |v'|=|v|, v'\neq v$.

1. Soit w un mot de Lyndon généralisé et $w=uv$ une factorisation non triviale. Alors w n'est pas une puissance pure. Donc w et v ne sont pas puissances d'un même mot, car ce mot devrait être plus court que w, puisque v l'est, et w serait une puissance pure. Donc $w^\infty\neq v^\infty$.

D'après 0., on peut donc écrire $w=v^n s$ avec les conditions énoncées dans 0. Par hypothèse $w^\infty<(vu)^\infty=v(uv)^\infty=vw^\infty=v^{n+1}s$, et comme v^{n+1} n'est pas préfixe de w^∞, la comparaison entre w^∞ et $v^{n+1}s$ se fait dans le $(n+1)-$ème facteur v. Donc on a aussi $w^\infty<v^{n+1}v^\infty=v^\infty$.

2. Supposons qu'on ait $w^\infty<v^\infty$ pour toute factorisation non triviale $w=uv$. D'après 0., on a alors $w^\infty=v^n v's'$, où $|v'|=|v|, v'\neq v$. Alors la comparaison entre

w^∞ et v^∞ se fait dans v'. On a donc aussi $w^\infty < v^{n+1}s = vv^ns = vw^\infty = v(uv)^\infty = (vu)^\infty$. Donc w est un mot de Lyndon généralisé. ■

Nous avons en vue de démontrer le théorème de factorisation suivant.

Théorème 2.1. *Les mots de Lyndon généralisés constituent une factorisation du monoïde libre. C'est-à-dire : tout w dans A^* a une unique factorisation $w = w_1 \dots w_n$ où chaque w_i est un mot de Lyndon généralisé, avec $w_1^\infty \geq \dots \geq w_n^\infty, n \geq 0$.*

On notera que la condition $u^\infty \geq v^\infty$, qui n'induit pas un ordre sur A^+, mais un préordre, induit cependant un ordre total sur l'ensemble des mots de Lyndon généralisés : ceci parce qu'un tel mot est primitif.

Pour démontrer le théorème, nous nous ramènerons aux ensembles de Hall. Un *ensemble de Hall* est un sous-ensemble H du magma libre $M(A)$ engendré par A (i.e. la structure algébrique avec une loi non associative engendrée librement par A ; ses éléments s'identifient aux arbres binaires complets à feuilles étiquetées dans A) tel que :

- H est totalement ordonné ;
- H contient A ;
- tout élément de $H \backslash A$ est de la forme $t = (t_1, t_2)$ avec $t_1, t_2 \in H$ et $t < t_2$;
- plus précisément, si $t_1, t_2 \in H$, alors $(t_1, t_2) \in H$ si et seulement si $t_1 < t_2$ et : soit $t_1 \in A$, soit $t_1 = (t_1', t_1'')$ et $t_1'' \geq t_2$.

La définition que nous prenons ici des ensembles de Hall est plus générale que la définition de Marshall Hall ; elle provient des travaux de Shirshov [S] et Viennot [V] (voir [R] pour un historique et la présente définition).

Il y a un homomorphisme (de magma) naturel de $M(A)$ vers A^*, qui consiste à oublier le parenthésage. Un *ensemble de mots de Hall* est l'image sous cet homomorphisme d'un ensemble de Hall dans $M(A)$.

De manière plus intrinsèque, un ensemble de mots de Hall peut être défini de la manière suivante. C'est un sous-ensemble H de A^* tel que :

- H est totalement ordonné ;
- H contient A ;
- à tout élément w de $H \backslash A$ est associée une factorisation non triviale $w = uv$ appelée sa *factorisation standard* ;
- pour tout $w \in H \backslash A$, de factorisation standard $w = uv$, on a $u, v \in H$ et $w < v$;
- si $u, v \in H$, alors $w = uv$ est dans H et uv est sa factorisation standard si et seulement si $u < v$ et soit $u \in A$, soit u a la factorisation standard u_1u_2 et $u_2 \geq v$.

L'équivalence des deux définitions des ensembles de mots de Hall découle entre autres de ce que la fonction naturelle $M(A) \to A^*$ est toujours injective sur un ensemble de Hall (voir [R, Cor. 4.5]).

Nous allons donc démontrer le théorème suivant.

Théorème 2.2. *L'ensemble des mots de Lyndon généralisés est un ensemble de mots de Hall.*

D'après [R, Cor. 4.7], le théorème 2.1 se déduit du théorème 2.2. Commençons par quelques lemmes.

Lemme 2.1. *Soient u, v, w_1, w_2 des mots non vides sur A.*

1. *Si $(uw_1)^\infty < v^\infty < (uw_2)^\infty$ et $|u| \leq |v|$ alors $v = uv'$.*
2. *Si $(uv)^\infty < v^\infty < u^\infty$, alors $v = u^n u', u = u'u'', n \geq 0$.*
3. *On a $(uv)^\infty < v^\infty \Leftrightarrow u^\infty < v^\infty$.*
4. *On a $(uv)^\infty = v^\infty \Leftrightarrow u^\infty = v^\infty$.*

Remarque 2.1. Parmi les nombreux résultats intermédiaires qui mènent à la démonstration de son théorème du centralisateur, Bergman [B, Lemma 5.1] donne le résultat suivant, pour l'ordre lexicographique usuel (dans nos notations, on choisit donc $<_i = <_0$ pour tout i) : si $u^\infty < v^\infty$, alors $u^\infty < (uv)^\infty < (vu)^\infty < v^\infty$. Il en donne une preuve simple et élégante. Celle-ci ne se généralise pas à nos ordres lexicographiques, d'autant plus que la conclusion n'est pas vraie. On peut en effet avoir $u^\infty < v^\infty$ sans qu'on ait $u^\infty < (uv)^\infty$ ou $(vu)^\infty < v^\infty$; par exemple, reprenant l'exemple de l'ordre lexicographique alterné ci-dessus, nous avons $1^\infty < 2^\infty$ mais $1^\infty > (12)^\infty$, et $(21)^\infty > 2^\infty$.

Nous avons cependant le résultat suivant, qui découle du lemme précédent et de la dernière partie de la preuve de la proposition 2.1.

Corollaire 2.1. *Si $u^\infty < v^\infty$, alors $u^\infty < (vu)^\infty, (uv)^\infty < (vu)^\infty, (uv)^\infty < v^\infty$.*

Nous aurons besoin dans la preuve du lemme 2.1 d'un résultat qui se déduit facilement d'un thérorème de Fine et Wilf (voir [L, Prop. 1.3.5]).

Lemme 2.2. *Si $s = u^\infty \neq v^\infty = t$, alors il existe $i \in \{0, 1, 2, \ldots, |u| + |v| - 2\}$ tel que $s_i \neq t_i$. Autrement dit, la comparaison entre s et t se fait dans leur préfixe de longueur $|u| + |v| - 1$.*

Preuve. Dans le cas contraire, le mot w, préfixe de longueur $|u| + |v| - 1$ de s et t, admet les périodes $|u|$ et $|v|$. D'après le théorème de Fine et Wilf, w a la période $d = pgdc(|u|, |v|)$. Comme u et v sont préfixes de w, et que d divise leur longueur, u et v sont puissances d'un même mot. Donc $u^\infty = v^\infty$. ∎

Preuve du lemme 2.1.
1. On peut écrire $v = u'v'$ avec $|u'| = |u|$. On a $(uw_1)^\infty < (u'v')^\infty = u'v'u'v'\dots$. Si la comparaison se fait dans le premier u', on aura aussi $(uw_2)^\infty < (u'v')^\infty$, ce qui contredit l'hypothèse. Donc la comparaison ne se fait pas dans cet u', ce qui signifie que $u = u'$, ce qu'il fallait démontrer.

2. Nous pouvons écrire $v = u^n v'$, où n est maximum, donc u n'est pas préfixe de v'. Nous avons donc $(uv)^\infty = (u^{n+1}v')^\infty < v^\infty < (u^{n+1})^\infty$. Si l'on avait $|v'| \geq |u|$, i.e. $|v| \geq |u^{n+1}|$, la première partie du lemme montrerait que u^{n+1} est préfixe de v, contradiction. Donc $|v'| < |u|$. Écrivons $u = u'u''$ avec $|u'| = |v'|$. Alors les inégalités ci-dessus s'écrivent $(u^n u'u''v')^\infty < v^\infty < (u^n u'u'')^\infty$.

Comme $|v| = |u^n u'|$, la première partie montre qu'on a $v = u^n u'$, ce qu'il fallait démontrer.

4. D'après la remarque faite avant la preuve de la proposition 2.1, on a $(uv)^\infty = v^\infty \Leftrightarrow u^\infty = v^\infty$, ce qui démontre 4.

3. Nous supposons que $(uv)^\infty < v^\infty$. Nous supposons dans un premier temps que $|v| \leq |u|$. Si la comparaison entre $(uv)^\infty$ et v^∞ se fait dans le premier u de $(uv)^\infty$, on aura aussi $u^\infty < v^\infty$. Si elle ne s'y fait pas, on aura $u = v^i v', v = v'v''$ et $i \geq 1$ à cause de l'hypothèse sur les longueurs. Supposons qu'on ait $u^\infty > v^\infty$, c'est-à-dire $v^i v' v \ldots > v^\infty$; d'après le lemme 2.2, la comparaison se fait dans le préfixe $v^i v' v$ de u^∞, puisqu'il est de longueur $|u| + |v|$. Par suite, on a aussi $(v^i v' v)^\infty > v^\infty$, c'est-à-dire $(uv)^\infty > v^\infty$, une contradiction. Donc $u^\infty < v^\infty$.

Il nous faut encore traiter le cas $|v| > |u|$. Raisonnant encore par l'absurde, supposons que $v^\infty < u^\infty$, donc $(uv)^\infty < v^\infty < u^\infty$. D'après la 2ème partie, on a donc $v = u^n u', u = u'u''$ et $n \geq 1$ d'après l'hypothèse sur les longueurs. La dernière égalité se réécrit $u^n u' u \ldots < u^{n+1} u' \ldots$ et d'après le lemme 2.2, la comparaison se fait dans les préfixes $u^n u' u$ et $u^{n+1} u'$ des mots v^∞ et u^∞, car $|u| + |v| = |u^{n+1} u'|$. Comme $u^{n+1} u' = uv$, on a aussi $v^\infty < (uv)^\infty$, une contradiction. En conclusion, on doit avoir $u^\infty < v^\infty$.

Nous venons de prouver que $(uv)^\infty < v^\infty$ implique $u^\infty < v^\infty$. Comme ceci est valable pour l'ordre lexicographique associé à toute suite $(<_i)_{i \geq 0}$, c'est aussi valable pour l'ordre opposé, qui est associé à la suite des ordres opposés. Donc on a aussi $(uv)^\infty > v^\infty \Rightarrow u^\infty > v^\infty$. Comme ces ordres sont totaux, nous obtenons 3, puisque 4. est déjà acquis. ■

Preuve du théorème 2.2. Soit H l'ensemble des mots de Lyndon généralisés relatifs à l'ordre lexicographique $<$ associé à la suite des ordres totaux $(<_i)_{i \in \mathbb{N}}$ sur A. Comme nous l'avons vu après le théorème 2.1, la condition $u^\infty < v^\infty$ induit sur les u, v dans H un ordre total, car les mots dans H sont primitifs. Nous écrirons $u < v$ pour $u^\infty < v^\infty$ et u, v dans H.

Clairement, H contient A. Si $w \in H \backslash A$, nous appelons *factorisation standard* de H la factorisation non triviale $w = uv$, où v satisfait à la condition suivante : pour tout facteur droit propre non trivial v' de w, soit $v^\infty < v'^\infty$, soit $v^\infty = v'^\infty$ (i.e. v, v' sont puissances d'un même mot) et v' est puissance de v.

On a alors $u^\infty < v^\infty$: en effet, comme w est un mot de Lyndon généralisé, on a $w^\infty < v^\infty$ (Proposition 2.1), i.e. $(uv)^\infty < v^\infty$, ce qui implique par le lemme 2.1 que $u^\infty < v^\infty$.

Si v' est un facteur droit propre non trivial de v, on a $v^\infty < v'^\infty$ par construction de v ; donc v est un mot de Lyndon généralisé d'après la Proposition 2.1. De plus, u est aussi un mot de Lyndon généralisé : en effet, si $u = u_1u_2$ est une factorisation non triviale, on a $v^\infty \leq (u_2v)^\infty$ par construction de v. Donc, par le lemme 2.1, $v^\infty \leq u_2^\infty$, et par ce qui précède, $u^\infty < u_2^\infty$. Donc u est un mot de Lyndon généralisé d'après la proposition 2.1. Nous en concluons que pour tout mot de Lyndon généralisé w, qui n'est pas dans A, sa factorisation standard $w = uv$ satisfait à : $u, v \in H$ et $w < v$ (cette dernière égalité d'après la proposition 2.1).

Supposons de plus que u ne soit pas une lettre et ait la factorisation standard $u = u_1u_2$. Il découle alors de l'argument ci-dessus que $u_2^\infty \geq v^\infty$, donc que $u_2 \geq v$ (u_2, v sont dans H).

Pour finir, il faut montrer que si u, v sont dans H, si $u < v$ et si, soit $u \in A$, soit u a la factorisation standard $u = xy$ avec $y \geq v$, alors $w = uv$ est dans H et a uv comme factorisation standard.

Supposons d'abord que $u \in A$. On a $u^\infty < v^\infty$ par l'hypothèse, donc $w^\infty = (uv)^\infty < v^\infty$ d'après le lemme 2.1. Si $v = v_1v_2$ est une factorisation non triviale, on aura $v^\infty < v_2^\infty$ d'après la proposition 2.1. Donc $w^\infty < v'^\infty$ pour tout facteur droit propre non trivial v' de w (car $u \in A$), et $w \in H$ d'après la proposition 2.1. De plus $w = uv$ est sa factorisation standard.

Supposons maintenant que $u \notin A$, avec factorisation standard $u = xy$ et $y \geq v$. Comme ci-dessus, on a $w^\infty < v^\infty$. Comme ci-dessus aussi, $w^\infty < v^\infty < v_2^\infty$ pour toute factorisation non triviale $v = v_1v_2$. Soit maintenant $u = u_1u_2$ une factorisation non triviale de u. On a $y^\infty \geq v^\infty$ par hypothèse. De plus $u_2^\infty \geq y^\infty$ par définition de la factorisation standard $u = xy$. Donc $u_2^\infty \geq v^\infty$, ce qui implique $(u_2v)^\infty \geq v^\infty$ par le lemme 2.1. Enfin, $w^\infty < (u_2v)^\infty$. Tout ceci montre que w est dans H, par la proposition 2.1. De plus, $w = uv$ est sa factorisation standard, car v^∞ est minimum parmi les v'^∞, pour v' suffixe propre non trivial de w, et de plus $|v|$ est de longueur minimum. ∎

Remarque 2.2. Nous avons défini la factorisation standard d'un mot de Lyndon généralisé w par $w = uv$, où v^∞ est choisi minimum parmi les facteurs droits (propres non triviaux) de w, et v de longueur minimum. Comme pour les mots de Lyndon usuels, v est aussi le plus long suffixe propre de w qui est un mot de Lyndon généralisé. En effet, s'il existait un suffixe v_1 de w, plus long que v, qui est un mot de Lyndon généralisé, on aurait par la proposition 2.1 $v_1^\infty < v^\infty$, une contradiction.

Ceci montre d'ailleurs que la factorisation standard des mots de Lyndon, telle que définie ici, lorsqu'on prend $<_i=<_0$ pour tout i, est la même que celle définie dans [L, p. 66].

Corollaire 2.2. *Soit $w = l_1 \dots l_n$, $l_1 \geq \cdots \geq l_n$, où les l_i sont des mots de Lyndon généralisés. Alors l_n est le plus court parmi les suffixes non triviaux v de w réalisant le minimum de v^∞.*

Preuve. Notons z le suffixe non trivial de w, le plus court parmi ceux qui réalisent le minimum de z^∞. Si $w = z, w$ est un mot de Lyndon généralisé d'après la proposition 2.1. Sinon $w = uz$, et nous définissons la factorisation $u = l_1 \dots l_{n-1}$ en mots de Lyndon généralisés avec $l_1 \geq \cdots \geq l_{n-1}, n \geq 2$. Il suffit de montrer que $l_{n-1} \geq z$, car z est un mot de Lyndon généralisé, par construction et d'après la proposition 2.1. Mais on a $(l_{n-1}z)^\infty \geq z^\infty$ par construction de z. Le lemme 2.1 montre qu'alors $l_{n-1}^\infty \geq z^\infty$, et donc $l_{n-1} \geq z$. ■

Le corollaire 2.2, joint au théorème de factorisation de Schützenberger [L, Th. 5.4.1], démontre encore une fois le théorème 2.1, sans passer par les ensembles de Hall. Ceux-ci ont cependant l'avantage de permettre la construction de bases de l'algèbre de Lie libre. En effet, par itération de la factorisation standard, chaque mot de Lyndon généralisé vient avec un parenthésage complet. Celui-ci définit un polynôme de Lie dans l'algèbre associative libre $\mathbb{Z}\langle A \rangle$.

Corollaire 2.3. *Les polynômes de Lie ainsi définis forment une base de l'algèbre de Lie libre.*

Cela découle de la théorie des bases de Hall, voir [R, Th.4.9].

3. Mots de Galois et applications

3.1. **Ordre lexicographique alterné.** Cet ordre a été introduit au début de la section précédente. La motivation en est la suivante : cet ordre reflète l'ordre des nombres réels, développés en fraction continues.

Plus précisément, étant donné une suite d'entiers $a_0, a_1, a_2, \dots$ naturels strictement positifs, notons $\alpha = [a_0, a_1, a_2, \dots]$ le nombre réel ayant le développement en fraction continue

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}.$$

Si $b_0, b_1, b_2, \dots$ est une autre suite, il est bien connu et facile de vérifier que $[a_0, a_1, a_2, \dots] < [b_0, b_1, b_2, \dots]$ si et seulement si : soit $a_0 < b_0$, soit $a_0 = b_0$ et $a_1 > b_1$, soit $a_0 = b_0, a_1 = b_1$ et $a_2 < b_2$, etc. ; autrement dit, si l'on a $a_0a_1a_2 \dots < b_0b_1b_2 \dots$ pour l'ordre lexicographique alterné.

La version finitaire de cet ordre permet de comparer avec une grande efficacité les nombres rationnels (de manière équivalente, calculer le signe du déterminant d'une matrice 2×2 à coefficients entiers), voir [Va].

3.2. **Mots de Galois.** Ceux-ci ont été définis au paragraphe 2, Exemples. Avant de poursuivre les applications, donnons-en une propriété combinatoire. Celle-ci est inspirée du fait que les mots de Lyndon usuels sont sans bord (voir [L, p. 65]). Une preuve très élégante en est donnée par Duval [Du] ; nous l'adaptons à notre cas ci-dessous. Rappelons qu'un *bord* d'un mot w est un mot v tel qu'on ait une égalité non triviale $w = uv = vu'$, pour des mots u, u' (par exemple, *ababa* a pour bords a et *aba*). Les exemples de mots de Galois donnés dans la section 2 montrent que ceux-ci peuvent avoir des bords.

Proposition 3.1. *Si un mot de Galois w a un bord v, alors v est de longueur impaire.*

Preuve. On a $w = uv = vu'$. Comme w est un mot de Galois, on doit avoir $w^\infty = (uv)^\infty < (u'v)^\infty$ et $w^\infty = (vu')^\infty < (vu)^\infty$. Comme u, u' sont de même longueur, la comparaison pour la première inégalité se fait dans u, u' : $uvuv \cdots < u'vu'v \ldots$ Si v était de longueur paire, à cause de la définition de l'ordre lexicographique alterné, on obtiendrait $vuvuv \ldots < vu'vu'v \ldots$, i.e. $(vu)^\infty < (vu')^\infty$, ce qui contredirait la deuxième inégalité. ∎

3.3. **Nombres quadratiques.** D'après un théorème de Lagrange, un nombre réel $\alpha > 0$ a un développement en fraction continue périodique si et seulement si c'est un nombre quadratique, c'est-à-dire s'il n'est pas rationnel et annule un polynôme de degré 2 à coefficients entiers (autrement dit, si $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, $d \in \mathbb{N}$, non carré). Galois précise les choses : le développement est purement périodique si et seulement si de plus $\alpha > 1$ et si son conjugué est dans l'intervalle $]-1, 0[$ (le conjugué de $a + b\sqrt{d}$ est $a - b\sqrt{d}$). Appelons *nombre de Galois* un tel nombre.

Il y a donc clairement une bijection entre les mots primitifs dans $\mathbb{P}^+$ et les nombres de Galois : à tout $w \in \mathbb{P}^+$, primitif, est associé le nombre de Galois dont le développement en fraction continue est w^∞.

Rappelons que deux nombres réels α, β ont même développement en fraction continue à partir d'un certain rang (i.e.. $\exists k \in \mathbb{Z}$ tel que $a_n = b_{n+k}$ pour n assez grand) si et seulement s'ils sont reliés par une homographie entière : $\beta = \frac{a\alpha+b}{c\alpha+d}, a, b, c, d \in \mathbb{Z}, ad - bc = \pm 1$. Nous obtenons donc le résultat suivant.

Proposition 3.2. *Il y a une bijection naturelle entre mots de Galois et classes homographiques de nombres de Galois, qui associe à un mot de Galois w le plus petit nombre de la classe.*

Ceci justifie bien sûr notre terminologie. Un exemple : 121 est un mot de Galois et ses deux conjugués satisfont $(121)^\infty < (112)^\infty < (211)^\infty$. Les nombres quadratiques associés sont respectivement $\frac{1+\sqrt{10}}{3}, \frac{2+\sqrt{10}}{3}, \frac{2+\sqrt{10}}{2}$.

On notera que les nombres de Galois ne coïncident pas avec les nombres de Sturm décrits dans [CMPS], [A] et [BS].

3.4. **Algorithme de Schützenberger–Melançon.** Il y a un algorithme pour calculer le mot de Galois contenu dans une classe de conjugaison primitive. C'est un cas particulier d'un algorithme de Melançon [Me], qui calcule pour tout mot w l'unique puissance d'un mot de Hall conjugué à w, et ceci pour tout ensemble de Hall (cet algorithme généralise un algorithme de Schützenberger [S1]).

Nous l'énonçons ci-dessous ; on en déduit aisément un algorithme pour calculer le plus petit élément dans une classe homographique de nombres de Galois.

Une suite $\sigma = (h_1, \dots, h_n)$ de mots de Galois est dite *circulairement standard* si pour tout $i = 1, \dots, n$, soit h_i est une lettre, soit $h_i = h_i'h_i''$ (factorisation standard) et $h_i'' \geq h_1, \dots, h_n$. Une suite de lettres est clairement circulairement standard. Une *montée* est un couple (h_i, h_{i+1}) tel que $h_i < h_{i+1}$ (les indices sont pris modulo n) ; une montée est dite *légale* si $h_{i+1} \geq h_1, \dots, h_n$. Dans ce cas, on définit σ' par $\sigma' = (h_1, \dots, h_ih_{i+1}, \dots, h_n)$ si $i < n$ et $\sigma' = (h_nh_1, h_2, \dots, h_{n-1})$ si $i = n$. En itérant cette construction, on obtient à partir de toute suite de lettres, représentant un mot w, l'unique puissance d'un mot de Galois conjuguée à w. Si w est primitif, on obtient l'unique mot de Galois conjugué à w.

3.5. **Formes quadratiques.** Nous considérons des *formes quadratiques binaires indéfinies à coefficients entiers* (nous dirons simplement forme dans la suite) ; une telle forme s'écrit $ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$ non tous nuls, et son *discriminant* $\triangle = b^2 - 4ac$ est > 0. Nous considérons comme *équivalentes* deux formes proportionnelles, et aussi deux formes qui s'obtiennent l'une de l'autre par un changement de variable $(x, y) \mapsto (px + qy, rx + sy)$, où la matrice $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ est dans $SL_2(\mathbb{Z})$; on notera que cette équivalence n'est pas celle considérée généralement dans la littérature (par exemple [Bu, p. 5]).

Une forme est dite *réduite* si l'on a $|f| < 1, |s| > 1, fs < 0$, avec

$$f = \frac{\sqrt{\triangle} - b}{2a}, \quad s = \frac{-\sqrt{\triangle} - b}{2a}.$$

Bien sûr, f et s sont les racines de l'équation $ax^2 + bx + c = 0$. De manière équivalente, une forme est réduite si et seulement si $0 < \sqrt{\triangle} - b < 2|a| < \sqrt{\triangle} + b$ (voir [D1, p. 99–100], [Bu, p. 21]). On notera qu'alors b est > 0. Toute forme est équivalente à une forme réduite, non nécessairement unique ([D1, p. 101], [Bu, p. 22]). Les formes réduites équivalentes ont une structure cyclique naturelle : la forme $a'x^2 + b'xy + c'y^2$ est dite *adjacente à droite* de la forme $ax^2 + bxy + cy^2$ si $c = a'$ et s'il existe $\delta \in \mathbb{Z}$ tel que $b' = -b - 2\delta c$, $c' = a + b\delta + c\delta^2$ (ce qui signifie que $a'x^2 + b'xy + c'y^2$ s'obtient de $ax^2 + bxy + cy^2$ en y faisant le changement de variables $x \mapsto y$, $y \mapsto -x + \delta y$). La forme adjacente à droite est unique et tout forme réduite est adjacente à droite à une unique forme réduite ([D1, p. 103], [Bu, p. 22–33]). De plus, deux formes adjacentes ont même discriminant et les formes de même discriminant sont en nombre fini

([D1, p. 103], [Bu, p. 23]). Ainsi, une forme définit une suite bi-infinie périodique de formes, donc un cycle de telles formes. À ce cycle on associe le mot circulaire obtenu en considérant la suite des $|\delta|$, où δ est le paramètre ci-dessus. On obtient ainsi un mot circulaire primitif sur $\mathbb{P} = \{1, 2, 3, \ldots\}$, donc un mot de Galois.

Pour récupérer une forme quadratique à partir de ce mot circulaire, on considère le nombre réel quadratique dont le développement en fraction continue correspond à ce mot circulaire, indéfiniment répété. Il est racine d'une équation $a + by + cy^2 = 0$, $a, b, c \in \mathbb{Z}$, et la forme quadratique cherchée est $ax^2 + bxy + cy^2$ (voir [D1, p. 104–108]).

Le fait que deux formes équivalentes dans notre sens donnent le même mot circulaire provient de ce que deux formes *proprement équivalentes* (i.e. on considère des formes obtenues l'une de l'autre par changement de variables dans $SL_2(\mathbb{Z})$) correspondent à la même chaîne ([D1, p. 108], [Bu, p. 24]).

Voyons deux exemples, tirés de [Bu, p. 29]. Nous représentons une forme $ax^2 + bxy + cy^2$ par (a, b, c). Supposons-la réduite, et que (a', b', c') lui est adjacente à droite. Alors le nombre δ qui permet de faire passer l'un à l'autre est égal à $-\frac{b+b'}{2c}$ (voir ci-dessus).

- $\triangle = 5$, le cycle de longueur 2 : $(1, 1, -1)$, $(-1, 1, 1)$. Le mot circulaire des δ est : $1, -1$ et par suite le mot circulaire est simplement 1, qui est le mot de Galois associé.
- $\triangle = 23$, le cycle de longueur 6 : $(5, 9, -12)$, $(-12, 15, 2)$, $(2, 17, -4)$, $(-4, 15, 6)$, $(6, 9, -10)$, $(-10, 11, 5)$. Les δ sont sucessivement : $1, -8, 4, -2, 1, -2$. Le mot de Galois est 184212.

3.6. **Nombres de Markoff.** Soit A une suite bi-infinie sur $\mathbb{P}$:

$$A = \ldots a_{-2}a_{-1}a_0a_1a_2 \ldots$$

Définissons $\lambda_i(A) = a_i + [0, a_{i+1}, a_{i+2}, \ldots] + [0, a_{i-1}, a_{i-2}, \ldots]$ et $M(A) = \sup\{\lambda_i(A) \mid i \in \mathbb{Z}\}$.

Pour des raisons liées à la théorie de Markoff des approximations de fractions continues et des minima de formes quadratiques, on est amené à considérer des suites bi-infinies de la forme $A = {}^\infty W^\infty$, où W est un mot obtenu d'un mot de Christoffel supérieur w sur l'alphabet $\{1, 2\}$ en lui appliquant la substitution $1 \mapsto 11, 2 \mapsto 22$. Les *mots de Christoffel supérieurs* sont des mots primitifs définis dans [BS] (ce sont les mots notés t'_{pq} p. 59). Pour usage ultérieur, notons qu'un mot de Christoffel supérieur de longueur ≥ 2 s'écrit toujours $w = 2m1$, où m est un palindrome (i.e. m est égal à son image miroir $\tilde{m}$) ; le *mot de Christofffel inférieur* associé (t_{pq} dans la référence ci-dessus) est alors $1m2$, et ce mot est conjugué à w. Par ailleurs, dans la classe de conjugaison associée, $1m2$ est le plus petit et $2m1$ est le plus grand dans l'ordre lexicographique usuel (avec $1 < 2$).

Proposition 3.3. *Soit $A = {}^\infty W^\infty$ comme ci-dessus, où $w = 2m1$ est le mot de Christoffel supérieur envoyé sur W par la substitution $1 \mapsto 11, 2 \mapsto 22$. Alors $A = {}^\infty(\underline{2}2M11)^\infty = {}^\infty(11M2\underline{2})^\infty$ et les indices i tels que $M(A) = \lambda_i(A)$ sont ceux qui sont soulignés et ceux obtenus par la période de A ; ici M est l'image de m sous la substitution $1 \mapsto 11, 2 \mapsto 22$.*

Preuve. Comme $1m2$ et $2m1$ sont conjugués, $11M22$ et $22M11$ le sont aussi, et A est à la fois égal à ${}^\infty(22M11)^\infty$ et ${}^\infty(11M22)^\infty$. Si i, i' sont respectivement les deux positions soulignées dans l'énoncé, on a $\lambda_i(A) = \lambda_{i'}(A)$, car $\lambda_i(A) = \lambda_{-i}(\tilde{A})$, où $\tilde{A}$ est l'image miroir de A.

Il suffit donc de montrer que $\lambda_i(A) > \lambda_j(A)$ pour toute autre position j située sur la première des deux lettres 11 ou 22 de la factorisation canonique de $22M11$ en produit de 11 et 22. Nous utilisons pour ce faire le fait que l'ordre lexicographique alterné correspond à l'ordre des fractions continues. Comme $2m1$ (respectivement $1m2$) est le plus grand (respectivement petit) des conjugués de $2m1$ et $1m2$ dans l'ordre lexicographique usuel on a que pour toute factorisation $A = {}^\infty P^\infty$, où la première lettre de P est en position j, $(22M11)^\infty > P^\infty$ et ${}^\infty P > {}^\infty(22M11)$ pour l'ordre lexicographique, qu'il soit alterné ou usuel, à cause des duplications des lettres. Par conséquent $[a_i, a_{i+1}, a_{i+2}, \ldots] > [a_j, a_{j+1}, a_{j+2}, \ldots]$ et $[a_{i-1}, a_{i-2}, a_{i-3}, \ldots] < [a_{j-1}, a_{j-2}, a_{j-3}, \ldots]$. Cette dernière inégalité implique $[0, a_{i-1}, a_{i-2}, \ldots] > [0, a_{j-1}, a_{j-2}, \ldots]$, d'où $\lambda_i(A) > \lambda_j(A)$. ■

Dans les hypothèses de la proposition, nous pouvons maintenant donner les valeurs de $M(A)$. Pour cela rappelons la définition des *polynômes continuants* : $P(x_1, \ldots, x_n)$ est le coefficient $1,1$ de la matrice produit

$$(*) \qquad \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix}.$$

De manière équivalente, on a la récurrence

$$P(x_1, \ldots, x_n) = P(x_1, \ldots, x_{n-1})x_n + P(x_1, \ldots, x_{n-2}),$$

avec les conditions initiales $P(\ ) = 1, P(x_1) = x_1$. Si w est un mot sur l'alphabet $\mathbb{P}$, nous écrirons simplement $P(w)$ pour $P(x_1, \ldots, x_n)$, où $w = x_1 \ldots x_n$. Exemple : $P(21111) = P(2111) + P(211) = 2 \cdot P(211) + P(21) = 3 \cdot P(21) + 2 \cdot P(2) = 5 \cdot P(2) + 3 \cdot P(\ ) = 5 \cdot 2 + 3 \cdot 1 = 13$.

Considérons encore l'homomorphisme μ du monoïde libre $\{1, 2\}^*$ sur le monoïde multiplicatif des matrices, qui envoie 1 sur $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ et 2 sur $\left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)$.

Corollaire 3.1. *Soit A, W, w comme ci-dessus, en excluant le cas $w = 1$. Alors $W = 2W'$ et $M(A)$ est égal à $\sqrt{9 - \frac{4}{c^2}}$ où*

$$c = P(W') = (\mu w)_{21} = \frac{1}{3} tr(\mu w).$$

Les nombres c ainsi obtenus s'appellent les nombres de Markoff ; par exemple, 13 est un nombre de Markoff. Une conjecture importante sur ces nombres est la suivante : la fonction $w \mapsto c$ de l'ensemble des mots de Christoffel supérieurs sur l'ensemble des nombres de Markoff est injective. Cette conjecture est mentionnée par Frobenius en 1913 [F, p. 601], par Cusick et Flahive [CF, p. 11] et par Conway et Guy [CG, p. 188] (sous une formulation différente). On notera que les *coordonnées de Frobenius* (voir [F, par. 8], [CF, p. 24]) du nombre de Markoff c ci-dessus ne sont autres que les nombres de 1 et de 2 dans le mot de Christoffel w.

Nous utiliserons le résultat bien connu suivant.

Lemme 3.1. *Soit u un mot primitif sur $\mathbb{P}$ et $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ son image sous l'homomorphisme qui envoie i sur $\left(\begin{smallmatrix} i & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $\varepsilon = ad - bc = \pm 1$. Alors la somme des nombres réels dont les développements en fractions continues sont u^∞ et $0\ \tilde{u}^\infty$ est égale à $\frac{\sqrt{(a+d)^2 - 4\varepsilon}}{c}$.*

Preuve. Il est bien connu que, si α, β désignent respectivement ces deux nombres, alors α est un nombre de Galois et $-\beta$ est son conjugué. Il s'agit donc de calculer $\alpha - \beta$. Par ailleurs, on a $\alpha = \frac{a\alpha + b}{c\alpha + d}$, donc $c\alpha^2 + (d-a)\alpha - b = 0$. Donc $\alpha - \beta = \frac{\sqrt{\triangle}}{c}$, où $\triangle = (d-a)^2 + 4bc = d^2 - 2ad + a^2 + 4ad - 4\varepsilon = (a+d)^2 - 4\varepsilon$. ■

Le résultat élémentaire suivant nous sera aussi bien utile.

Lemme 3.2. *Si M est une matrice 2×2 symétrique, alors la matrice*

$$N = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} M \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

satisfait à $3N_{21} = tr(N)$.

Preuve. On a

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ q & r \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 10p + 9q + 2r & 5p + 7q + 2r \\ 4p + 4q + r & 2p + 3q + r \end{pmatrix}$$

et la trace de cette matrice est $12p + 12q + 3r = 3(4p + 4q + r)$. ■

Preuve du corollaire 3.1. Comme $w \neq 1, w$ commence par 2 et W aussi. La proposition montre que $M(A) = \lambda_i(A)$ avec la position i indiquée. On applique alors le lemme 3.1 avec $u = W$: on a $M(A) = \frac{1}{c}\sqrt{(a+d)^2 - 4\varepsilon}$ où $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est l'image de W par l'homomorphisme qui envoie 1 sur $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et 2 sur $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Mais le carré de ces matrices est respectivement $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)$. Donc $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \mu w$.

Mais $w = 2v1$, où v est un palindrome. Donc μv est une matrice symétrique puisque $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)$ le sont. Le lemme 3.2 montre qu'alors $a + d = 3c$. D'où $M(A) = \frac{1}{c}\sqrt{9c^2 - 4}$, car $\varepsilon = 1$.

Enfin, il est bien connu que le produit $(*)$ est égal à

$$\begin{pmatrix} P(x_1, \dots, x_n) & P(x_1, \dots, x_{n-1}) \\ P(x_2, \dots, x_n) & P(x_2, \dots, x_{n-1}) \end{pmatrix},$$

ce qui conclut la preuve. ■

Remarque 3.1. Pour $w = 1$, on obtient aussi le nombre de Markoff 1, égal à $c = \frac{1}{3}(a+d)$ pour la matrice $\mu w = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.

Remarque 3.2. Comme les matrices $\mu 1$ et $\mu 2$ sont symétriques, on a aussi $c = \frac{1}{3}\mathrm{tr}(\mu\tilde{w})$, et $\tilde{w}$ est le mot de Christoffel inférieur associé au mot de Christoffel supérieur w.

Nous obtenons aussi un résultat de Harvey Cohn [C].

Corollaire 3.2. *Les nombres de Markoff sont obtenus comme le tiers de la trace des matrices images des mots de Christoffel supérieurs sur* $\{1,2\}$ *sous l'homomorphisme envoyant* 1 *sur* $\left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)$ *et* 2 *sur* $\left(\begin{smallmatrix} -1 & 2 \\ -4 & 7 \end{smallmatrix}\right)$.

Preuve. Avec les notations du corollaire 3.1, on a $c = \frac{1}{3}\mathrm{tr}(\mu w)$, pour tout nombre de Markoff c et w le mot de Christoffel supérieur approprié. Le déterminant de μw est 1, donc $\mathrm{tr}(\mu w) = (\mathrm{tr}(\mu w)^{-1}) = \mathrm{tr}\ ({}^t(\mu w)^{-1})$. Comme $A \mapsto {}^tA^{-1}$ est un automorphisme de $GL_2(\mathbb{Z})$, on a que $c = \frac{1}{3}\mathrm{tr}\,(\mu' w)$, où μ' envoie 1 sur $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)^{-1}$ et 2 sur $\left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)^{-1}$. Il suffit maintenant de remarquer que $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)$ et que cette matrice conjugue $\left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)^{-1}$ et $\left(\begin{smallmatrix} -1 & 2 \\ -4 & 7 \end{smallmatrix}\right)$: on a en effet $\left(\begin{smallmatrix} -1 & 2 \\ -4 & 7 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)$. ■

3.7. **Spectre de Cassaigne.** Dans [Ca] est considéré l'ensemble des nombres réels $\alpha = [a_0, a_1, a_2, \ldots]$ tels que $\alpha \geq [a_i, a_{i+1}, a_{i+2}, \ldots]$ pour tout $i \in \mathbb{N}$; cet ensemble est lui-même lié à un ensemble de mots bi-infinis étudié dans [AC]. Dans cet ensemble, les nombres de Galois qu'il contient sont denses (voir [Ca, p. 12]). Par définition, ces nombres de Galois sont exactement les nombres de Galois maximums dans leur classe d'homographie.

Ces nombres sont donc ceux dont le développement en fraction continue est de la forme w^∞, où w est un mot de Lyndon généralisé pour la suite d'ordre $(<_n)_{n\in\mathbb{N}}$, sur $\mathbb{P}$, avec $<_n$= l'ordre naturel sur $\mathbb{P}$ si n est impair, = l'ordre opposé si n pair. Ces w constituent une variante des mots de Galois, en prenant l'ordre opposé.

3.8. **Factorisations de Viennot.** Selon [L], une *factorisation de Viennot* du monoïde libre A^* est une factorisation complète $A^* = \prod_{i\in I} l_i^*$, où I est totalement ordonné, où le produit est décroissant, et où $l_i \in A^+$, avec en plus la condition suivante : $i < j \Rightarrow \exists k$ tel que $l_i l_j = l_k$.

Les mots de Lyndon usuels forment une factorisation de Viennot. Cependant, dans cet article dédié à Viennot, nous devons avouer que les mots de Galois ne forment pas une factorisation de Viennot : par exemple 121 et 3 sont des mots de Galois, on a $(121)^\infty < 3^\infty$, mais 1213 n'est pas un mot de Galois, puisque c'est son conjugué 1312 qui est un mot de Galois.

Références

[A] Allauzen, C., *Une description simple des nombres de Sturm*, Journal de Théorie des Nombres de Bordeaux 10, 1998, 237–241.

[AC] Allouche, J.-P., Cosnard, M., *Itération de fonctions unimodales et suites engendrées par automates*, Comptes Rendus de l'Académie des Sciences, Paris, Série I, Mathématique 296, 1983, 159–162.

[B] Bergman, G.M., *Centralizers in free associative algebras*, Transactions of the American Mathematical Society 137, 1969, 327–344.

[BS] Berstel, J., Séébold, P., *Sturmian words dans : M. Lothaire*, Algebraic Combinatorics on words, Cambridge, 2002, 45–110.

[Bu] Buell, D.A., *Binary quadratic forms, classical theory and modern computations*, Springer Verlag, 1989.

[C] Cohn, H., *Markoff forms and primitive words*, Mathematische Annalen 196, 1972, 8–22.

[CMPS] Crisp, D., Moran, W., Pollington, A., Shine, P., *Substitution invariant cutting sequences*, Journal de Théorie des Nombres de Bordeaux 5, 1993, 123–137.

[Ca] Cassaigne, J., *Limit values of the recurrence quotient of Sturmian sequences*, Theoretical Computer Science 218, 1999, 3–12.

[CF] Cusick, T.W., Flahive, M.E., *The Markoff and Lagrange spectra*, Amer. Math. Soc., 1989.

[CG] Conway, J.H., Gay, R.K., *The book of numbers*, Copernicus, Springer–Verlag, 1998.

[D1] Dickson, L.E., *Introduction to the theory of numbers*, Dover, 1957.

[D2] Dickson, L.E., *Studies in the theory of numbers*, Chelsea, New York 1930 (2ème éd. en 1957).

[Du] Duval, J.-P., *Factorizing words over and ordered alphabet*, Journal of Algorithms 4, 1983, 363–381.

[F] Frobenius, G.F., *Über die Markoffschen Zahlen*, Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin 1913, 4 58–487 ; aussi dans : Frobenius, G.F., *Gesammelte Abhandlungen*, Springer–Verlag 1968, vol. 3, 598–627, éd. J.-P. Serre.

[L] Lothaire, M., *Combinatorics on words*, Addison–Wesley, 1983.

[M1] Markoff, A.A., *Sur les formes quadratiques binaires indéfinis*, Mathematische Annalen 15, 1879, 381–496.

[M2] Markoff, A.A., *Sur les formes quadratiques binaires indéfinies*, Mathematische Annalen 17, 1880, 379–399.

[Me] Melançon, G., *Combinatorics of Hall trees and Hall words*, Journal of Combinatorial Theory A, 59, 1992, 285–308.

[R] Reutenauer, C., *Free Lie algebras*, Oxford University Press, 1993.

[S] Shirshov, A.I., *Bases of free Lie algebras*, Algebra *i* Logika 1, 1962, 14–19.

[S1] Schützenberger, M.-P., *Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées*, séminaire P. Dubreil, Faculté des Sciences, Paris, 1978.

[S2] Schützenberger, M.-P., *On a factorization of free monoids*, Proceedings of the American Mathematical Society, 16, 1965, 21–24.

[V] Viennot, X.G., *Algèbres de Lie libres et monoïdes libres*, Lecture Notes in Mathematics 691, Springer.

[Va] Vallée, B., *Algorithms for computing signs of* 2×2 *determinants : dynamics and average-case analysis*, Lecture Notes in Computer Science 1284, 486–499, 1997.