

POLYNOMES ASSOCIES AUX ENDOMORPHISMES DE GROUPES LIBRES

Jacques Peyrière, Wen Zhi-ying & Wen Zhi-xiong

Abstract. - If σ is an endomorphism of F , the free group generated by a and b , there exists a unique polynomial map Φ_σ from \mathbf{C}^3 to \mathbf{C}^3 , with integral coefficients, such that, for any representation φ of F in $SL(2, \mathbf{C})$, one has

$$(\operatorname{tr} \varphi(\sigma(a)), \operatorname{tr} \varphi(\sigma(b)), \operatorname{tr} \varphi(\sigma(ab))) = \Phi_\sigma(\operatorname{tr} \varphi(a), \operatorname{tr} \varphi(b), \operatorname{tr} \varphi(ab)).$$

The following relation holds : $\Phi_{\sigma' \circ \sigma} = \Phi_\sigma \circ \Phi_{\sigma'}$. The kernel of Φ is shown to be generated by the inner automorphisms of F and the involution which takes a to a^{-1} and b to b^{-1} . If λ denotes the polynomial $x^2 + y^2 + z^2 - xyz - 4$, then $\lambda \circ \Phi_\sigma$ factorizes under the form $\lambda \cdot Q_\sigma$, where Q_σ is a polynomial with integral coefficients. Among other properties of Q_σ , it is proved that σ is an automorphism of E if and only if Q_σ equals 1 identically. The case of a free group with more than two generators is also studied but, in this case, results are less complete.

Résumé. - A chaque endomorphisme σ du groupe libre F engendré par a et b on associe une unique application polynomiale Φ_σ , à coefficients entiers, de \mathbf{C}^3 dans \mathbf{C}^3 telle que, pour toute représentation φ de F dans $SL(2, \mathbf{C})$ on ait

$$(\operatorname{tr} \varphi(\sigma(a)), \operatorname{tr} \varphi(\sigma(b)), \operatorname{tr} \varphi(\sigma(ab))) = \Phi_\sigma(\operatorname{tr} \varphi(a), \operatorname{tr} \varphi(b), \operatorname{tr} \varphi(ab)).$$

L'application Φ est un anti-homomorphisme du monoïde des endomorphismes de F dans le monoïde des applications polynomiales de \mathbf{C}^3 dans \mathbf{C}^3 , muni de la composition. Diverses propriétés de Φ sont établies. En particulier, son noyau est caractérisé. En outre, si λ désigne le polynôme $x^2 + y^2 + z^2 - xyz - 4$, le polynôme $\lambda \circ \Phi$ se factorise sous la forme $\lambda \cdot Q_\sigma$ où Q_σ est un polynôme à coefficients entiers. Il est établi, entre autre, que σ est un automorphisme de F si et seulement si Q_σ est identiquement égal à 1. Le cas d'un groupe libre à plus de deux générateurs est également abordé, mais avec des résultats moins complets.

AMS Classification : 20E05 - 20M05 - 16R99 - 15A24

KEYWORDS : Freegroups - finite automata - traces - PI rings - polynomial identities.

Jacques Peyrière, Wen Zhi-ying & Wen Zhi-xiong

Cet article répond à certaines questions posées dans [8]. Pour la commodité du lecteur, dans la première partie, les résultats de [8] sont repris, et dans certains cas précisés.

I. Introduction

On désigne dans les sections 1, 2, 3, 4 et 5 par F le groupe libre à deux générateurs, a et b . On note $\text{tr } A$ la trace de la matrice carrée A . Si φ est un homomorphisme de F dans $SL(2, \mathbb{C})$, on note $T\varphi$ le triplet $(\text{tr } \varphi(a), \text{tr } \varphi(b), \text{tr } \varphi(ab))$.

L'image de T est \mathbb{C}^3 tout entier : pour s'en persuader, il suffit de considérer les φ tels que $\varphi(a) = \begin{pmatrix} x & -1 \\ 1 & 0 \end{pmatrix}$ et $\varphi(b) = \begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & y \end{pmatrix}$.

Si σ et σ' sont des endomorphismes de F , on pose $\sigma\sigma' = \sigma' \circ \sigma$. On identifiera un élément σ de $\text{Hom}(F, F)$ au couple $(\sigma(a), \sigma(b)) \in F \times F$.

Si w est un élément de F , on désignera par \tilde{w} l'élément de \mathbb{Z}^2 , image de w par l'homomorphisme d'abélianisation. Si σ est un endomorphisme de F , il définit, par abélianisation, un endomorphisme de \mathbb{Z}^2 dont nous désignerons par $\tilde{\sigma}$ la matrice transposée. En d'autres termes, $\tilde{\sigma}$ est la matrice carrée indexée par $\{a, b\} \times \{a, b\}$ dont les coefficients d'interprètent de la façon suivante : si u et v appartiennent à $\{a, b\}$, $\tilde{\sigma}_{u,v}$ =somme des puissances de la lettre v dans $\sigma(u)$. On a évidemment $(\sigma\sigma')^\sim = \tilde{\sigma}\tilde{\sigma}'$.

On note λ le polynôme $\lambda(x, y, z) = x^2 + y^2 + z^2 - xyz - 4$. On sait que, pour $\varphi \in \text{Hom}(F, SL(2, \mathbb{C}))$, $\lambda(T\varphi)$ est nul si et seulement si $\varphi(a)$ et $\varphi(b)$ ont une direction propre commune.

LEMME 1. *Soit A et B deux éléments de $SL(2, \mathbb{C})$. On a*

$$AB + BA = \text{tr}(AB) - (\text{tr } A)(\text{tr } B) + A \text{tr } B + B \text{tr } A.$$

Démonstration. Le théorème de Cayley-Hamilton donne les relations suivantes :

$$\begin{aligned} A^{-1} &= \text{tr } A - A \\ B^{-1} &= \text{tr } B - B \\ (AB)^2 &= AB \text{tr}(AB) - 1. \end{aligned}$$

Par ailleurs, on a

$$\begin{aligned}
BA &= A^{-1}ABABB^{-1} \\
&= A^{-1}(AB \operatorname{tr}(AB) - 1)B^{-1} \\
&= \operatorname{tr}(AB) - (\operatorname{tr} A - A)(\operatorname{tr} B - B) \\
&= \operatorname{tr}(AB) - (\operatorname{tr} A)(\operatorname{tr} B) + A \operatorname{tr} B + B \operatorname{tr} A - AB.
\end{aligned}$$

LEMME 2. Soit $w \in F$. Il existe alors quatre polynômes, $P_w^{(j)} \in \mathbb{Z}[x, y, z]$ ($j = 1, 2, 3, 4$), tels que, pour tout $\varphi \in \operatorname{Hom}(F, SL(2, \mathbb{C}))$, on ait

$$\varphi(w) = P_w^{(1)}(T\varphi) + P_w^{(2)}(T\varphi)\varphi(a) + P_w^{(3)}(T\varphi)\varphi(b) + P_w^{(4)}(T\varphi)\varphi(ab).$$

Démonstration. Posons, pour simplifier, $\varphi(a) = A$, $\varphi(b) = B$ et $T\varphi = (x, y, z)$. On a alors, en vertu du théorème de Cayley-Hamilton et du lemme précédent,

$$\begin{aligned}
A^2 &= xA - 1 \\
A^{-1} &= x - A \\
B^2 &= yB - 1 \\
B^{-1} &= y - B \\
BA &= z - xy + yA + xB - AB.
\end{aligned}$$

En outre,

$$\begin{aligned}
ABA &= A(z - xy + yA + xB - AB) \\
&= A[z - yA^{-1} + xA^{-1}B] \\
&= -y + zA + xB.
\end{aligned}$$

Le lemme résulte alors de ces formules par récurrence sur la longueur de w , supposé réduit.

PROPOSITION 3. Soit $w \in F$. Il existe alors un unique polynôme $P_w \in \mathbb{Z}[x, y, z]$ tel que, pour tout $\varphi \in \operatorname{Hom}(F, SL(2, \mathbb{C}))$, on ait

$$\operatorname{tr} \varphi(w) = P_w(T\varphi).$$

Démonstration. L'existence résulte du lemme précédent :

$$\operatorname{tr} \varphi(w) = 2P_w^{(1)}(T\varphi) + P_w^{(2)}(T\varphi)\operatorname{tr} \varphi(a) + P_w^{(3)}(T\varphi)\operatorname{tr} \varphi(b) + P_w^{(4)}(T\varphi)\operatorname{tr} \varphi(ab).$$

L'unicité résulte de la surjectivité de T .

Cette proposition, avec une démonstration légèrement différente, figure dans [1].

THEOREME 4. Soit $\sigma \in \operatorname{Hom}(F, F)$. Il existe alors un unique $\Phi_\sigma \in (\mathbb{Z}[x, y, z])^3$ tel que, pour tout $\varphi \in \operatorname{Hom}(F, SL(2, \mathbb{C}))$ on ait

$$T(\varphi \circ \sigma) = \Phi_\sigma(T\varphi).$$

Démonstration. Cela résulte simplement de la proposition précédente, appliquée aux éléments $\varphi(a)$, $\varphi(b)$ et $\varphi(ab)$ de F .

PROPOSITION 5. *Quels que soient σ_1 et σ_2 dans $Hom(F, F)$, on a*

$$\Phi_{\sigma_1\sigma_2} = \Phi_{\sigma_1} \circ \Phi_{\sigma_2}.$$

Démonstration. On a

$$T(\varphi \circ \sigma_2 \circ \sigma_1) = \Phi_{\sigma_1}(T(\varphi \circ \sigma_2)) = \Phi_{\sigma_1} \circ \Phi_{\sigma_2}(T\varphi),$$

d'où le résultat à cause de l'unicité de $\Phi_{\sigma_1\sigma_2}$.

PROPOSITION 6. *Quels que soient $w \in F$ et $\sigma \in Hom(F, F)$, on a*

$$P_{\sigma(w)} = P_w \circ \Phi_{\sigma}.$$

Démonstration. Soit σ' l'élément de $Hom(F, F)$ ainsi défini : $\sigma'(a) = w$, $\sigma'(b) = b$. Alors P_w et $P_{\sigma(w)}$ sont les premières composantes de $\Phi_{\sigma'}$ et de $\Phi_{\sigma'\sigma}$ respectivement. Or $\Phi_{\sigma'\sigma} = \Phi_{\sigma'} \circ \Phi_{\sigma}$, d'où le résultat.

THEOREME 7. *Soit $\sigma \in Hom(F, F)$. Il existe alors un polynôme*

$$Q_{\sigma} \in \mathbb{Z}[x, y, z] \text{ tel que l'on ait } \lambda \circ \Phi_{\sigma} = \lambda \cdot Q_{\sigma}.$$

Démonstration. Soit $\varphi \in Hom(F, SL(2, \mathbb{C}))$ tel que $\lambda(T\varphi) = 0$. Alors $\varphi(a)$ et $\varphi(b)$ ont une direction propre commune. Il en est donc de même de $\varphi(\sigma(a))$ et de $\varphi(\sigma(b))$. Par suite $\lambda(\varphi_{\sigma}(T\varphi)) = 0$.

L'existence de Q_{σ} avait été conjecturée dans [3] et prouvée dans [8].

PROPOSITION 8. *Si σ_1 et σ_2 sont deux éléments de $Hom(F, F)$ on a*

$$Q_{\sigma_1\sigma_2} = Q_{\sigma_2} \cdot Q_{\sigma_1} \circ \Phi_{\sigma_2}.$$

Démonstration. On a

$$\lambda \circ \Phi_{\sigma_1\sigma_2} = (\lambda \circ \Phi_{\sigma_1}) \circ \Phi_{\sigma_2} = (\lambda \cdot Q_{\sigma_1}) \circ \Phi_{\sigma_2} = \lambda \cdot Q_{\sigma_2} \cdot Q_{\sigma_1} \circ \Phi_{\sigma_2}.$$

PROPOSITION 9. *Si w et w' sont deux éléments de F tels que $\tilde{w} = \tilde{w}'$, alors $P_w - P_{w'}$ est divisible par λ .*

Démonstration. Si φ est un homomorphisme de F dans $SL(2, \mathbb{C})$ tel que $\varphi(a)$ et $\varphi(b)$ ont une direction propre commune, on a $P_w(T\varphi) = P_{w'}(T\varphi)$, comme on peut le voir en trigonalisant simultanément $\varphi(a)$ et $\varphi(b)$. Par suite le polynôme $P_w - P_{w'}$ s'annule sur les zéros de λ .

Soit Ω la variété des zéros de λ . Le théorème 7 dit que Ω est stable par tout Φ_σ . La proposition 9 dit que la restriction de Φ_σ à Ω ne dépend que de l'abélianisé $\bar{\sigma}$ de σ .

PROPOSITION 10. Si $\sigma \in \text{Aut}(F)$, alors $\det \Phi'_\sigma = \pm 1$.

Démonstration. Différentions la relation $\Phi_{\sigma^{-1}} \circ \Phi_\sigma = \text{id}$ et prenons les déterminants. On obtient

$$\det(\Phi'_{\sigma^{-1}} \circ \Phi'_\sigma) \det(\Phi'_\sigma) = 1.$$

Comme ces déterminants sont des polynômes à coefficients entiers, ils sont nécessairement constants, égaux à ± 1 .

LEMME 11. Pour tout $\sigma \in \text{Hom}(F, F)$, on a $Q_\sigma(0, 0, 0) = 0$ ou 1.

Démonstration. Il suffit de considérer $\varphi \in \text{Hom}(F, SL(2, \mathbb{C}))$ tel que $\varphi(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et

$$\varphi(b) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Nous donnerons plus loin un résultat plus précis que celui-ci.

PROPOSITION 12. Si $\sigma \in \text{Aut } F$, on a $Q_\sigma = 1$.

Démonstration. Ceci résulte de la proposition 8 et du lemme 11.

II. Détermination du noyau de Φ .

Comme l'ont observé Kolar et Ali [3], les polynômes de Chebyshev interviennent naturellement dans ce contexte.

Considérons les deux suites de polynômes $\{t_n\}_{n \in \mathbb{Z}}$ et $\{u_n\}_{n \in \mathbb{Z}}$ satisfaisant la même relation de récurrence

$$\begin{aligned} t_{n+1}(x) + t_{n-1}(x) &= x t_n(x) \\ u_{n+1}(x) + u_{n-1}(x) &= x u_n(x) \end{aligned}$$

avec les conditions initiales

$$t_0(x) = 2, \quad t_1(x) = x, \quad u_0(x) = 0, \quad u_1(x) = 1.$$

Il est facile de vérifier les faits suivants :

$$\begin{aligned} t_{-n} &= t_n, & d^0 t_n &= |n| \\ u_{-n} &= -u_n, & d^0 u_n &= n - 1 \quad \text{si } n \geq 1 \\ t_n(2 \cos \varphi) &= 2 \cos n\varphi \\ u_n(2 \cos \varphi) &= \frac{\sin n\varphi}{\sin \varphi} \\ t_n(x) &= x u_n(x) - 2u_{n-1}(x). \end{aligned}$$

L'intérêt pour nous de ces polynômes vient du lemme suivant dont la démonstration par récurrence est immédiate.

LEMME 1. Si A est une matrice carrée telle que $A^\ell = xA - 1$, alors, pour tout $n \in \mathbb{Z}$, on a

$$A^n = u_n(x)A - u_{n-1}(x)$$

et, si A est une matrice 2×2 , $\text{tr } A^n = t_n(x)$.

LEMME 2. Soit $w = a^{m_1}b^{n_1}a^{m_2}b^{n_2} \dots a^{m_k}b^{n_k}$ un élément de F . On suppose que, si $k > 0$, on a $m_1m_2 \dots m_k n_1 \dots n_k \neq 0$, (si $k = 0$, par convention $w = e$). Alors $d_z^0 P_w = k$, (où d_z^0 désigne le degré par rapport à la variable z).

Démonstration. Elle se fait par récurrence sur k . Le lemme est vrai pour $k = 0$. Supposons-le vrai pour $k \leq \ell - 1$.

Soit $w = a^{m_1}b^{n_1}a^{m_2}b^{n_2} \dots a^{m_\ell}b^{n_\ell} = w_1 a^{m_\ell} b^{n_\ell}$. On a, si $T\varphi = (x, y, z)$,

$$\varphi(w) = \varphi(w_1)[u_{m_\ell}(x)\varphi(a) - u_{m_\ell-1}(x)][u_{n_\ell}(y)\varphi(b) - u_{n_\ell-1}(y)].$$

La trace de $\varphi(w)$ est donc combinaison linéaire à coefficients polynômiaux en x et y des traces de $\varphi(w_1 a b)$, $\varphi(w_1 a)$, $\varphi(w_1 b)$ et $\varphi(w_1)$. Puisque, pour calculer des traces de produits, on peut opérer des permutations circulaires, l'hypothèse de récurrence montre que les traces de $\varphi(w_1 a)$, $\varphi(w_1 b)$ et $\varphi(w_1)$ ont un degré en z inférieur ou égal à $\ell - 1$.

Ainsi donc le degré en z du polynôme

$$\text{tr } \varphi(w) - \text{tr}(\varphi(w_1 a b))u_{m_\ell}(x)u_{n_\ell}(y)$$

est strictement inférieur à ℓ .

Répétant le même argument aux autres facteurs de w , on obtient que le degré en z du polynôme

$$\text{tr } \varphi(w) - \text{tr}(\varphi[(ab)^\ell]) \prod_{j=1}^{\ell} [u_{m_j}(x)u_{n_j}(y)]$$

est au plus $\ell - 1$.

Mais $\text{tr } \varphi(ab)^\ell = t_\ell(z)$ est un polynôme en z de degré ℓ . Ceci achève la démonstration.

LEMME 3. Si $w \in F$ est tel que $P_w = \alpha z$ ($\alpha \in \mathbb{Z}$), alors $\alpha = 1$ et l'on a $w = uabu^{-1}$ ou $w = ua^{-1}b^{-1}u^{-1}$ pour un $u \in F$.

Démonstration. Si $\alpha = 0$, le lemme précédent montre que la réduction cyclique de w est e , a^m ou b^n . Dans aucun de ces cas on obtient $P_w = 0$. Donc $\alpha \neq 0$.

Le lemme précédent montre alors que la réduction cyclique de w est $a^m b^n$ (avec $mn \neq 0$). Alors le lemme 1 montre que l'on a

$$\begin{aligned} P_w(x, y, z) &= u_m(x)u_n(y)z - yu_{m-1}(x)u_n(y) - xu_m(x)u_{n-1}(y) \\ &\quad + 2u_{m-1}(x)u_{n-1}(y). \end{aligned}$$

Or $u_m(x)u_n(y) = \alpha$ implique $|m| = |n| = 1$ et $\alpha = mn$. Si $mn = -1$, alors l'un des deux termes $yu_{m-1}(x)u_n(y)$ ou $xu_m(x)u_{n-1}(y)$ reste seul, ce qui est impossible. Donc $m = n = \pm 1$, d'où le lemme.

- 1°) Si $P_w = \alpha x$, on a $\alpha = 1$ et $w = uau^{-1}$ ou $w = ua^{-1}u^{-1}$.
 2°) Si $P_w = \alpha y$, on a $\alpha = 1$ et $w = ubu^{-1}$ ou $w = ub^{-1}u^{-1}$.

Démonstration. Supposons que l'on ait $P_w = \alpha x$. Considérons l'élément $\sigma \in \text{Hom}(F, F)$ ainsi défini : $\sigma(a) = ab$, $\sigma(b) = b^{-1}$. On a $\Phi_\sigma(x, y, z) = (z, y, x)$, donc, en vertu de la proposition I.3, on a $P_{\sigma(w)}(x, y, z) = P_w \circ \Phi_\sigma(x, y, z) = \alpha z$. On en déduit (lemme précédent) que $\alpha = 1$ et que $\sigma(w) = uabu^{-1}$ ou $\sigma(w) = ua^{-1}b^{-1}u^{-1}$. Mais σ est un isomorphisme : $\sigma^{-1}(a) = ab$, $\sigma^{-1}(b) = b^{-1}$. On a donc $w = \sigma^{-1}(u)a\sigma^{-1}(u^{-1})$ ou $w = \sigma^{-1}(u)b^{-1}a^{-1}b\sigma^{-1}(u^{-1})$.

Pour démontrer la seconde assertion, on utilise de la même façon l'isomorphisme (a^{-1}, ab) .

THEOREME 5. Pour $\sigma \in \text{Hom}(F, F)$ les propriétés suivantes sont équivalentes :

- 1°) $\Phi_\sigma = id$
 2°) σ est soit un automorphisme intérieur, soit un automorphisme intérieur composé avec l'involution (a^{-1}, b^{-1}) .

Démonstration. Il est clair que la seconde propriété implique la première. Supposons que l'on ait $\Phi_\sigma = id$. Il résulte du lemme précédent que l'on a

$$\sigma(a) = u a^\epsilon u^{-1} \quad \text{avec} \quad \epsilon = \pm 1 \text{ et } u \in F$$

et

$$\sigma(b) = v b^\eta v^{-1} \quad \text{avec} \quad \eta = \pm 1 \text{ et } v \in F.$$

On sait par ailleurs (proposition I-9) que λ divise $P_{\sigma(ab)} - P_{a^\epsilon b^\eta}$. Comme $P_{\sigma(ab)} = z$ et $P_{a^{-1}b} = P_{ab^{-1}} = xy - z$ on a $\epsilon = \eta$. Quitte à composer avec l'involution (a^{-1}, b^{-1}) , on peut supposer que l'on a $\epsilon = \eta = 1$.

Supposons que les mots uau^{-1} et vbv^{-1} soient réduits. Si $u = v = e$, il n'y a rien à démontrer. Sinon, supposons que $|u| \geq |v|$ (où $|u|$ désigne la longueur de u). On a alors $u = u'b^n$ avec $n \neq 0$, la dernière lettre de u' étant a , si $|u'| > 0$. Dans ces conditions on a

$$\sigma(ab) = u'b^n ab^{-n} u'^{-1} vbv^{-1}$$

d'où

$$z = P_{(ab^{-n}u'^{-1}vbv^{-1}u'b^n)}.$$

Utilisant une nouvelle fois le lemme 3, on obtient que $u'^{-1}v = b^k$. L'irréductibilité de vbv^{-1} implique alors $u' = v$. Ceci montre que σ est un automorphisme intérieur.

III. Applications polynomiales laissant λ invariant. Caractérisation des σ tels que $Q_\sigma = 1$.

On désigne par R un domaine d'intégrité de caractéristique nulle et par \mathcal{A} l'ensemble des $\psi \in (R[x, y, z])^3$ tels que $\lambda \circ \psi = \lambda$.

L'ensemble \mathcal{A} contient $\{\Phi_\sigma ; \sigma \in \text{aut } F\}$. Il sera commode de considérer les éléments suivants de $\text{aut } F$:

$$\alpha = (b, a), \quad \beta = (a, b^{-1}), \quad \gamma = (ab, b^{-1}).$$

Les Φ correspondants sont :

$$\begin{aligned}\Phi_\alpha(x, y, z) &= (y, x, z) \\ \Phi_\beta(x, y, z) &= (x, y, xy - z) \\ \Phi_\gamma(x, y, z) &= (z, y, x).\end{aligned}$$

On considèrera aussi les applications polynomiales suivantes :

$$\rho(x, y, z) = (-x, -y, z)$$

et

$$\theta(x, y, z) = (-x, y, -z).$$

Ces applications polynomiales sont également dans \mathcal{A} .

Nous allons montrer que \mathcal{A} est engendrée par $\Phi_\alpha, \Phi_\beta, \Phi_\gamma, \rho$ et θ .

LEMME 1. *Si $\psi = (\psi_1, \psi_2, \psi_3)$ appartient à \mathcal{A} , alors on a, pour $i = 1, 2, 3$, $d^0 \psi_i \geq 1$.*

Démonstration. Si, par exemple, ψ_3 était constant, égal à c , on aurait

$$\psi_1^2 + \psi_2^2 - c\psi_1\psi_2 = x^2 + y^2 + z^2 - xyz - c^2.$$

Or, le premier membre de cette expression est réductible dans un corps, extension convenable de R , alors que le second membre ne l'est pas.

Notons $\deg \psi$ la somme $d^0 \psi_1 + d^0 \psi_2 + d^0 \psi_3$ et posons

$$\mathcal{L} = \{\psi \in \mathcal{A} ; \deg \psi = 3\}.$$

LEMME 2. *\mathcal{L} est le groupe engendré par Φ_α, Φ_γ et ρ .*

Démonstration. Appelons les variables x_1, x_2, x_3 au lieu de x, y, z . Soit $\psi \in \mathcal{L}$. On a $\psi_j(x) = \ell_j + u_j$ où ℓ_j est un polynôme homogène de degré 1 et $u_j \in R$. On a

$$\sum_{j=1}^3 (\ell_j + u_j)^2 - (\ell_1 + u_1)(\ell_2 + u_2)(\ell_3 + u_3) = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 x_3.$$

L'identification des termes de degré 3 donne $\ell_j = v_j x_{\tau(j)}$ où $v_j \in R$, et $\tau \in \mathcal{S}_3$ et $v_1 v_2 v_3 = 1$. L'identification des termes quadratiques donne alors $u_1 = u_2 = u_3 = 0$, $v_1^2 = v_2^2 = v_3^2 = 1$.

Il est des lors facile de se convaincre que ψ est dans le groupe engendré par Φ_α, Φ_β et ρ .

LEMME 3. Soit $\psi = (\psi_1, \psi_2, \psi_3) \in \mathcal{A}$ tel que $\deg \psi > 3$. Alors, il existe $\sigma \in \langle \alpha, \beta, \gamma \rangle$, le groupe engendré par α, β et γ , tel que $\deg(\Phi_\sigma \circ \psi) < \deg \psi$.

Démonstration. Puisque Φ_α et Φ_γ sont des transpositions distinctes de deux composantes, quitte à remplacer ψ par $\Phi_\sigma \circ \psi$, avec $\sigma \in \langle \alpha, \gamma \rangle$, on peut supposer que $d^0 \psi_3 \geq d^0 \psi_2 \geq d^0 \psi_1 \geq 1$.

Puisque $\deg \psi > 3$, on a $d^0 \psi_3 \geq 2$. Or $(\psi_3 - \psi_1 \psi_2) \psi_3 + \psi_2^2 + \psi_1^2 = x^2 + y^2 + z^2 - xyz$. Si l'on avait $d^0 \psi_3 \neq d^0 \psi_1 \psi_2$ on aurait $3 = \sup(d^0 \psi_3, d^0 \psi_1 \psi_2) + d^0 \psi_3 \geq 4$. On a donc $d^0 \psi_3 = d^0 \psi_1 \psi_2$, d'où $d^0 \psi_3 > d^0 \psi_2$. Si l'on avait $d^0(\psi_3 - \psi_1 \psi_2) = d^0 \psi_3$, on aurait $2d^0 \psi_3 = 3$, donc on a $d^0(\psi_3 - \psi_1 \psi_2) < d^0 \psi_3$. Ceci montre que $\deg \Phi_\beta \circ \psi < \deg \psi$. Ceci achève la démonstration du lemme.

THEOREME 4. \mathcal{A} est le groupe engendré par $\Phi_\alpha, \Phi_\beta, \Phi_\gamma$ et ρ .

Démonstration. Il suffit d'appliquer de façon répétitive le lemme précédent pour se ramener au lemme 2.

THEOREME 5. L'ensemble des $\sigma \in \text{Hom}(F, F)$ tels que $Q_\sigma = 1$ est l'ensemble des automorphismes de F .

Démonstration. Dire que $Q_\sigma = 1$ équivaut à dire $\Phi_\sigma \in \mathcal{A}$. Si $\Phi_\sigma \in \mathcal{A}$, le lemme 3 permet de montrer l'existence d'un $\tau \in \langle \alpha, \beta, \gamma \rangle$ tel que $\Phi_\tau \circ \Phi_\sigma \in \{\theta, \rho\}$. Mais, en vertu des lemmes II.3 et II.4, on a alors $\Phi_\tau \circ \Phi_\sigma = \text{id}$. Il en résulte (théorème II.5) que $\tau \circ \sigma$ est un automorphisme, donc aussi σ .

LEMME 6. Si i_w désigne l'automorphisme intérieur $u \rightarrow wuw^{-1}$ de F . On a

$$i_a = \beta\alpha\beta\gamma\beta\gamma\alpha\beta \quad \text{et} \quad i_b = \alpha i_a \alpha.$$

Démonstration. Elle se fait par vérification directe.

THEOREME 7. L'ensemble des automorphismes de F est le groupe engendré par α, β et γ .

Démonstration. Soit $\sigma \in \text{Aut } F$. Alors $\Phi_\sigma \in \mathcal{A}$. Comme précédemment, il existe $\tau \in \langle \alpha, \beta, \gamma \rangle$ tel que $\Phi_\tau \circ \Phi_\sigma = \text{id}$. Le théorème II.1 montre alors que $\tau \circ \sigma$ est soit un automorphisme intérieur, soit un automorphisme intérieur composé avec (a^{-1}, b^{-1}) , qui n'est autre que $(\alpha\beta)^2$. Le théorème résulte alors du lemme précédent.

Remarque. Ce théorème est un résultat ancien de Nielsen [5] [6], mais la démonstration que nous en donnons ne fait pas appel à la délicate théorie de la réduction de Nielsen.

IV. Étude des relations $\Phi_\sigma = \Phi_\tau$ et $Q_\sigma = 0$.

Notons F^* l'ensemble des éléments w de F qui sont image d'un générateur par un automorphisme de F .

THEOREME 1. *Soit σ et τ deux endomorphismes de F tels que $\sigma(a)$, $\sigma(b)$ et $\sigma(ab)$ soient dans F^* . Alors les assertions suivantes sont équivalentes :*

1°) $\Phi_\sigma = \Phi_\tau$

2°) $\tau(a)$, $\tau(b)$ et $\tau(ab)$ sont conjugués respectivement à $\sigma(a)$ ou $\sigma(a)^{-1}$, $\sigma(b)$ ou $\sigma(b)^{-1}$, $\sigma(ab)$ ou $\sigma(ab)^{-1}$.

Démonstration. Il est clair que la seconde assertion implique la première, et ce sans qu'il soit nécessaire de faire d'hypothèses sur σ .

Supposons que l'on ait $\Phi_\sigma = \Phi_\tau$ et $\sigma(a) = \mu(a)$, $\sigma(b) = \nu(b)$ et $\sigma(ab) = \xi(ab)$ (où μ , ν et ξ sont des automorphismes de F). On a alors $\Phi_{\mu^{-1}\sigma} = \Phi_{\mu^{-1}\tau}$, d'où en vertu du lemme II.4, $\mu^{-1}\tau(a) = ua^{\pm 1}u^{-1}$ pour un $u \in F$. Par suite $\tau(a) = \mu(u)\sigma(a)^{\pm 1}\mu(u)^{-1}$. On opère de même pour $\tau(b)$ et $\tau(ab)$.

THEOREME 2. *Pour des automorphismes σ et τ de F , les assertions suivantes sont équivalentes :*

1°) $\Phi_\sigma = \Phi_\tau$

2°) $\tilde{\sigma} = \pm \tilde{\tau}$

3°) $\tau = \sigma i_w$ ou $\tau = \sigma(\alpha\beta)^2 i_w$ pour un $w \in F$.

Démonstration. L'équivalence des assertions 1°) et 3°) est une simple reformulation du théorème II.1. L'équivalence de ces assertions avec la seconde résulte de la caractérisation, en termes de leurs matrices, des automorphismes intérieurs de F ([6]).

PROPOSITION 3. *Si σ est un endomorphisme de F , non injectif, il existe deux entiers m et n et un élément w de F tel que $\sigma(a) = w^m$ et $\sigma(b) = w^n$.*

Démonstration. On utilise la théorie de la réduction de Nielsen ([6],[7]). Etant donné $\sigma \in \text{Hom}(F, F)$ arbitraire, il existe un automorphisme μ de F tel que l'une des éventualités suivantes se produise :

1°) Le couple $(\sigma\mu(a), \sigma\mu(b))$ est réduit au sens de Nielsen,

2°) $\sigma\mu(a)$ est réduit au sens de Nielsen et $\sigma\mu(b) = e$.

3°) $\sigma\mu(a) = \sigma\mu(b) = e$.

Dans le premier cas $\sigma\mu$ est injectif, d'où la proposition.

LEMME 4. *Soit $\psi = (\psi_1, \psi_2, \psi_3) \in (R[x, y, z])^3$ (où R est un domaine d'intégrité de caractéristique nulle) tel que l'on ait $\lambda \circ \psi = 0$. Alors, il existe $\tau \in \text{Aut } F$ tel que $\Phi_\tau \circ \psi$ ait sa première composante constante.*

Démonstration. On peut évidemment supposer que l'on a $d^0\psi_1 \leq d^0\psi_2 \leq d^0\psi_3$. La relation $\lambda \circ \psi = 0$ s'écrit $\psi_3(\psi_3 - \psi_1\psi_2) = 4 - \psi_1^2 - \psi_2^2$, d'où l'on déduit $d^0(\psi_3 - \psi_1\psi_2) \leq d^0\psi_2$. Supposons que l'on ait $d^0(\psi_3 - \psi_1\psi_2) \geq d^0\psi_3$. On a alors $d^0\psi_2 = d^0\psi_3$ et $d^0\psi_1 + d^0\psi_2 + d^0\psi_3 \leq 2d^0\psi_3$ et, donc, $\psi_1 = c \in R$. Par une procédure de descente analogue à celle de la démonstration du théorème II.4, par composition par divers Φ_τ on peut faire décroître $\deg \psi$ tant que l'une de ses composantes n'est pas constante.

THEOREME 5. *Pour $\sigma \in \text{Hom}(F, F)$, $Q_\sigma \equiv 0$ si et seulement si σ n'est pas injectif.*

Démonstration. Supposons σ non injectif. En vertu de la proposition 3, il existe $\mu \in \text{Aut } F$ tel que $\sigma\mu(b) = e$. Or, on sait que $Q_{\sigma\mu} = Q_\mu Q_\sigma \circ \Phi_\mu$. Or, il est facile de vérifier que $Q_{\sigma\mu} = 0$. Comme $Q_\mu \equiv 1$, cela implique $Q_\sigma \equiv 0$.

Supposons maintenant que l'on ait $Q_\sigma \equiv 0$. En vertu du lemme précédent, il existe $\tau \in \text{Aut } F$ tel que la première composante de $\Phi_{\tau\sigma}$ soit constante. Le lemme II.2 montre alors que $\tau\sigma(a) = e$, ce qui prouve que σ n'est pas injective.

V. Autres propriétés des polynômes Q_σ .

THEOREME 1. *Pour tout $\sigma \in \text{End } F$, on a les faits suivants :*

1. $Q_\sigma(2\epsilon, 2\eta, 2\epsilon\eta) = (\det \sigma)^2$ pour tous $\epsilon, \eta \in \{-1, 1\}$.
2. λ divise le polynôme $\det \Phi'_\sigma - (\det \sigma)Q_\sigma$.

Démonstration. Observons d'abord que si p et q sont deux entiers rationnels on a

$$P_{a^p b^q}(x, y, z) = zu_p(x)u_q(y) - xu_p(x)u_{q-1}(y) - yu_{p-1}(x)u_q(y) + 2u_{p-1}(x)u_{q-1}(y).$$

Si ϵ et η valent ± 1 , il est facile de vérifier que

$$P_{a^p b^q}(2\epsilon, 2\eta, 2\epsilon\eta) = 2\epsilon^p \eta^q$$

et de calculer le gradient de $P_{a^p b^q}$:

$$P'_{a^p b^q}(2\epsilon, 2\eta, 2\epsilon\eta) = (\epsilon p(p - q), \eta q(q - p), \epsilon \eta p q) \epsilon^p \eta^q.$$

Considérons maintenant un élément de σ de $\text{End } F$ dont la matrice est $\tilde{\sigma} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$.

Ce qui précède montre que le point $(2, 2, 2)$ est point fixe pour Φ_σ et que l'ensemble $\{(2\epsilon, 2\eta, 2\epsilon\eta) ; \epsilon, \eta \in \{-1, 1\}\}$ est globalement invariant par Φ_σ .

Démontrons la première assertion. Différentions deux fois la relation $\lambda \circ \Phi_\sigma = \lambda \cdot Q_\sigma$ au point $\omega = (2\epsilon, 2\eta, 2\epsilon\eta)$. On obtient

$${}^t \Phi'_\sigma(\omega) \lambda''(\Phi(\omega)) \Phi'_\sigma(\omega) = \lambda''(\omega) Q_\sigma(\omega)$$

en ayant tenu compte de ce que $\lambda(\omega)$, $\lambda'(\omega)$ et $\lambda'(\Phi'_\sigma(\omega))$ sont nuls. Par ailleurs, $\Phi'_\sigma - (P_{a^p b^q}, P_{a^r b^s}, P_{a^{p+r} b^{q+s}})$ est un multiple de λ . Par conséquent, on obtient $\Phi'_\sigma(\omega)$ en différentiant en ω la fonction $(P_{a^p b^q}, P_{a^r b^s}, P_{a^{p+r} b^{q+s}})$. Tous calculs faits on obtient la première assertion.

Pour démontrer la seconde assertion, nous allons montrer que la polynôme $\det \Phi'_\sigma - (\det \sigma)Q_\sigma$ s'annule en suffisamment de points de Ω .

Considérons le point $\omega(t, u) = (2 \cos t, 2 \cos u, 2 \cos(t + u))$ de Ω . Son image par Φ_σ est le point $\omega(pt + qu, rt + su)$ que nous noterons $\omega \circ \tilde{\sigma}(t, u)$.

Par différentiation de la relation $\Phi_\sigma \circ \omega = \omega \circ \tilde{\sigma}$, on obtient

$$(\Phi'_\sigma \circ \omega) \cdot \frac{\partial \omega}{\partial t} \wedge (\Phi'_\sigma \circ \omega) \cdot \frac{\partial \omega}{\partial u} = (\det \sigma) \left(\frac{\partial \omega}{\partial t} \circ \tilde{\sigma} \right) \wedge \left(\frac{\partial \omega}{\partial u} \circ \tilde{\sigma} \right).$$

Par ailleurs, on établit facilement la relation

$$\frac{\partial \omega}{\partial t} \wedge \frac{\partial \omega}{\partial u} = -\lambda' \circ \omega$$

où l'on a fait les identifications nécessaires.

La relation $\lambda \circ \Phi_\sigma = \lambda \cdot Q_\sigma$ donne par différentiation, en observant que $\lambda \circ \omega = 0$,

$$(\lambda' \circ \Phi_\sigma \circ \omega)(\Phi'_\sigma \circ \omega)V = (Q_\sigma \circ \omega)(\lambda' \circ \omega) \cdot V$$

où V est un vecteur arbitraire. Compte tenu des relations précédentes, ceci s'écrit encore

$$\det \left(\frac{\partial \omega}{\partial t} \circ \tilde{\sigma}, \frac{\partial \omega}{\partial u} \circ \tilde{\sigma}, (\Phi'_\sigma \circ \omega) \cdot V \right) = (Q_\sigma \circ \omega) \det \left(\frac{\partial \omega}{\partial t}, \frac{\partial \omega}{\partial u}, V \right)$$

d'où

$$\det \left((\Phi'_\sigma \circ \omega) \cdot \frac{\partial \omega}{\partial t}, (\Phi'_\sigma \circ \omega) \cdot \frac{\partial \omega}{\partial u}, (\Phi'_\sigma \circ \omega) \cdot V \right) = (\det \sigma)(Q_\sigma \circ \omega) \det \left(\frac{\partial \omega}{\partial t}, \frac{\partial \omega}{\partial u}, V \right).$$

Ceci montre l'égalité $\det(\Phi'_\sigma \circ \omega) = (\det \sigma)(Q_\sigma \circ \omega)$ en chaque point où le gradient de ω n'est pas nul.

THEOREME 2.

1. $Q_\sigma(0, 0, 0)$ vaut 0 ou 1 selon que $\det \sigma$ est pair ou impair.
2. $\Phi_\sigma(0, 0, 0) = (0, 0, 0)$ si et seulement si $\det \sigma$ est impair.
3. $Q'_\sigma(0, 0, 0) = 0$.
4. Si $\det \sigma$ est impair, $Q''_\sigma(0, 0, 0)$ est diagonal négatif.

Démonstration.

Nous allons calculer $\Phi_\sigma(0, 0, z)$. Pour ce faire, considérons $\varphi \in \text{Hom}(F, SL(2, \mathbf{C}))$ tel que $\varphi(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\varphi(b) = \begin{pmatrix} 0 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix}$, avec $\lambda + \lambda^{-1} = z$. On a évidemment $\varphi(a)^2 = \varphi(b)^2 = -1$ et, donc tout produit d'un certain nombre de $\varphi(a)$ et de $\varphi(b)$ est

reductible à l'une des formes $\pm\varphi((ab)^n)$, $\pm\varphi((ab)^na)$, $\pm\varphi((ba)^n)$ ou $\pm\varphi((ba)^nb)$ dont les traces respectives sont $\pm t_n(z)$, 0 , $\pm t_n(z)$ et 0 (où t_n est un polynôme de Chebyshev de première espèce, cf. II).

Ceci nous conduit à définir le procédé suivant de réduction d'un élément de F : on remplace autant de fois qu'il est possible a^2 et b^2 par -1 . Ainsi le mot aba^2b^3 donne $-a$.

Réduisons ainsi les mots $\sigma(a)$ et $\sigma(b)$. On obtient respectivement $\epsilon\bar{\sigma}(a)$ et $\eta\bar{\sigma}(b)$ où ϵ et η valent ± 1 . Nous pouvons dresser le tableau suivant qui donne, pour les différentes valeurs possibles de $\bar{\sigma}(a)$ et $\bar{\sigma}(b)$, en première ligne, $\Phi_\sigma(0,0,z)$ et, en seconde, $Q_\sigma(0,0,z)$ en termes des polynômes de Chebyshev t et u en la variable z .

$\bar{\sigma}(b)$	$(ab)^n$	$(ab)^na$	$(ba)^n$	$(ba)^nb$
$\bar{\sigma}(a)$				
$(ab)^m$	(t_m, t_n, t_{m+n}) 0	$(t_m, 0, 0)$ u_m^2	(t_m, t_n, t_{m-n}) 0	$(t_m, 0, 0)$ u_m^2
$(ab)^ma$	$(0, t_n, 0)$ u_n^2	$(0, 0, -t_{m-n})$ u_{m-n}^2	$(0, t_n, 0)$ u_n^2	$(0, 0, t_{m+n+1})$ u_{m+n+1}^2

$(ba)^m$	(t_m, t_n, t_{m-n}) 0	$(t_m, 0, 0)$ u_m^2	(t_m, t_n, t_{m+n}) 0	$(t_m, 0, 0)$ u_m^2
$(ba)^mb$	$(0, t_n, 0)$ u_n^2	$(0, 0, t_{m+n+1})$ u_{m+n+1}^2	$(0, t_n, 0)$ u_n^2	$(0, 0, -t_{m-n})$ u_{m-n}^2

On observe que $Q_\sigma(0,0,z) = u_\nu(z)^2$ où $\nu = \det \bar{\sigma}$. Il est clair, par ailleurs, que $\det \sigma$ et $\det \bar{\sigma}$ ont même parité. La première assertion résulte alors de ce que $u_n(0) = \sin \frac{n\pi}{2}$.

La seconde assertion résulte de l'examen du tableau, compte tenu de ce que $t_n(0) = 2 \cos \frac{n\pi}{2}$.

La troisième assertion résulte simplement de la parité de u_n^2 .

Démontrons la dernière assertion. D'abord, il est facile de déterminer $\Phi_\sigma(x,0,0)$ et $\Phi_\sigma(0,y,0)$. En effet soit $\tau = (a^{-1}, ab) \in \text{End } F$. On a $\Phi_\tau(x,y,z) = (x,z,y)$ et par conséquent $\Phi_{\sigma\tau}(x,y,z) = \Phi_\sigma(x,z,y)$, ce qui permet par le procédé précédent de déterminer $\Phi_\sigma(0,y,0)$. De la même façon pour calculer $\Phi_\sigma(x,0,0)$ on utilise $\tau = (ab, b^{-1})$.

Supposons que $\det \sigma = 1 \pmod{2}$. Ce qui précède montre que deux des composantes de chacune des fonctions $\Phi_\sigma(x,0,0)$, $\Phi_\sigma(0,y,0)$ et $\Phi_\sigma(0,0,z)$ sont nulles alors que les

troisièmes sont de la forme $\pm p_{n_1}(x), \pm p_{n_2}(y), \pm p_{n_3}(z)$ respectivement, les entiers n_1, n_2, n_3 étant impairs. Par ailleurs, en vertu du théorème 1, compte tenu de $Q_\sigma(0,0,0) = 1$, on a $\det \Phi'_\sigma(0,0,0) = 1 \pmod{2}$. Comme $p'_{n_i}(0) = n_i \sin \frac{n_i \pi}{2} \neq 0$ (pour $i = 1, 2, 3$), on en déduit que la matrice $\Phi'_\sigma(0,0,0)$ a un terme non nul et un seul aussi bien dans chaque ligne que dans chaque colonne et que ses termes non nuls sont, au signes près, n_1, n_2 et n_3 . Autrement dit ${}^t \Phi'_\sigma(0,0,0) \Phi'_\sigma(0,0,0)$ est une matrice diagonale dont les éléments diagonaux sont des carrés de nombres impairs.

Différentions maintenant deux fois à l'origine la relation $\lambda \circ \Phi_\sigma = \lambda \cdot Q_\sigma$. On obtient

$${}^t \Phi'_\sigma(0,0,0) \lambda''(0) \Phi'_\sigma(0,0,0) = \lambda''(0) - 4Q''_\sigma(0,0,0)$$

en ayant tenu compte des relations $\lambda(0,0,0) = -4$ et $\lambda'(0,0,0) = 0$. La conclusion résulte

$$\text{de } \lambda''(0) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Prenons un exemple : $\sigma = (aba^2b^2a, aba^3bab)$. Calculons $\Phi_\sigma(0,0,z)$. La réduction de σ donne $(aba, -(ab)^3)$ donc

$$\Phi_\sigma(0,0,z) = (0, -t_3(z), 0) = (0, 3z - z^3, 0)$$

et

$$Q_\sigma(0,0,z) = u_3(z)^2 = (z^2 - 1)^2.$$

Pour calculer $\Phi_\sigma(x,0,0)$, multiplions σ par (ab, b^{-1}) , on obtient $(babab, bab)$, qui est réduit. Donc

$$\Phi_\sigma(x,0,0) = (0,0, -t_1(x)) = (0,0, -x)$$

et

$$Q_\sigma(x,0,0) = u_1(x)^2 = 1.$$

De façon analogue, on obtient

$$\Phi_\sigma(0,y,0) = (p_3(y), 0, 0) = (y^3 - 3y, 0, 0)$$

et

$$Q_\sigma(0,y,0) = (y^2 - 1)^2.$$

Ensuite on a

$$-2Q''_\sigma(0,0,0) = \begin{pmatrix} 0 & 0 & -1 \\ -3 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & -3 & 0 \\ 0 & 0 & 3 \\ -1 & 0 & 0 \end{pmatrix} - I \text{ d'où } Q''_\sigma(0,0,0) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix}.$$

Avant de passer à la généralisation partielle de ce qui précède, nous avons besoin d'un certain nombre de lemmes sur $SL(2, \mathbf{C})$.

LEMME 1. Soit A et B deux éléments de $SL(2, \mathbf{C})$. On a

$$ABA = A \operatorname{tr} AB - B^{-1}$$

et $\operatorname{tr}(ABA) = (\operatorname{tr} A)(\operatorname{tr} AB) - (\operatorname{tr} B)$.

Démonstration. On a, par Cayley-Hamilton, $AB + (AB)^{-1} = \operatorname{tr} AB$, d'où

$$ABA + B^{-1} = A \operatorname{tr} AB.$$

LEMME 2 (Formule de Fricke). Si A et B sont deux éléments de $SL(2, \mathbf{C})$, on a

$$\operatorname{tr}(ABA^{-1}B^{-1}) = (\operatorname{tr} A)^2 + (\operatorname{tr} B)^2 + (\operatorname{tr} AB)^2 - (\operatorname{tr} A)(\operatorname{tr} B)(\operatorname{tr} AB) - 2.$$

Démonstration. Une utilisation répétée du théorème de Cayley-Hamilton suivie de celle du lemme précédent donne

$$\begin{aligned} ABA^{-1}B^{-1} &= AB(\operatorname{tr} AB - BA) \\ &= AB \operatorname{tr} AB - A(B \operatorname{tr} B - 1)A \\ &= AB \operatorname{tr} AB - (A \operatorname{tr} AB - B^{-1})\operatorname{tr} B + A \operatorname{tr} A - 1 \end{aligned}$$

d'où le résultat, en prenant les traces des deux membres.

Considérons maintenant trois éléments A_1, A_2, A_3 de $SL(2, \mathbf{C})$ dont les traces sont respectivement x_1, x_2 et x_3 . On note y_1, y_2 et y_3 les traces de A_2A_3, A_3A_1 et A_1A_2 .

LEMME 3. On a $\operatorname{tr} A_1A_2A_3 + \operatorname{tr} A_1A_3A_2 = x_1y_1 + x_2y_2 + x_3y_3 - x_1x_2x_3$.

Démonstration. En vertu du lemme I.1, on a

$$A_2A_3 + A_3A_2 = y_1 - x_2x_3 + x_3A_2 + x_2A_3$$

d'où

$$A_1A_2A_3 + A_1A_3A_2 = (y_1 - x_2x_3)A_1 + x_3A_1A_2 + x_2A_1A_3,$$

d'où le résultat.

LEMME 4. On a

$$\begin{aligned} (\operatorname{tr} A_1A_2A_3)(\operatorname{tr} A_1A_3A_2) &= \\ &= x_1^2 + x_2^2 + x_3^2 + y_1^2 + y_2^2 + y_3^2 - x_1x_2y_3 - x_2x_3y_1 - x_3x_1y_2 + y_1y_2y_3 - 4. \end{aligned}$$

Démonstration. Utilisant le lemme 1 de deux façons, on obtient

$$\begin{aligned} A_1 A_2 A_3 A_1 A_3 A_2 &= (A_1 \operatorname{tr}(A_1 A_2 A_3) - A_3^{-1} A_2^{-1}) A_3 A_2 \\ &= A_1 A_2 (y_2 A_3 - A_1^{-1}) A_2 \end{aligned}$$

d'où

$$\begin{aligned} A_1 A_3 A_2 \operatorname{tr}(A_1 A_2 A_3) &= A_3^{-1} A_2^{-1} A_3 A_2 + y_2 A_1 A_2 A_3 A_2 - A_1 A_2 A_1^{-1} A_2 \\ &= A_3^{-1} A_2^{-1} A_3 A_2 + y_2 A_1 (y_1 A_2 - A_3^{-1}) - A_1 (A_2 \operatorname{tr}(A_2 A_1^{-1}) - A_1) \\ &= A_3^{-1} A_2^{-1} A_3 A_2 + y_2 A_1 (y_1 A_2 - x_3 + A_3) - A_1 A_2 (x_1 x_2 - y_3) \\ &\quad + x_1 A_1 - 1, \end{aligned}$$

d'où le résultat.

COROLLAIRE 5. *Les nombres $\operatorname{tr}(A_1 A_2 A_3)$ et $\operatorname{tr}(A_1 A_3 A_2)$ sont les racines de l'équation suivante, dont l'inconnue est z :*

$$z^2 - p(X, Y)z + q(X, Y) = 0$$

où

$$p(X, Y) = x_1 y_1 + x_2 y_2 + x_3 y_3 - x_1 x_2 x_3$$

et

$$q(X, Y) = x_1^2 + x_2^2 + x_3^2 + y_1^2 + y_2^2 + y_3^2 - x_1 x_2 y_3 - x_2 x_3 y_1 - x_3 x_1 y_2 + y_1 y_2 y_3 - 4.$$

Nous venons de définir les polynômes p et q en les variables $X = (x_1, x_2, x_3)$ et $Y = (y_1, y_2, y_3)$. Posons

$$\Lambda(X, Y, z) = z^2 - p(X, Y)z + q(X, Y).$$

PROPOSITION 6. *Le polynôme Λ est irréductible dans $\mathbf{C}[X, Y, z]$.*

Démonstration. Si Λ était décomposable, le polynôme $p^2 - 4q$ serait un carré dans $\mathbf{C}[X, Y]$. Il en serait de même du polynôme $(p^2 - 4q)(0, 0, 0, y_1, y_2, y_3)$ dans $\mathbf{C}[y_1, y_2, y_3]$. Or $(p^2 - 4q)(0, 0, 0, y_1, y_2, y_3)$ est de degré 3, c'est donc impossible.

Notons V la sous-variété algébrique de \mathbf{C}^7 , ensemble des zéros de Λ . Elle est irréductible.

Désignons par T l'application de $[SL(2, \mathbf{C})]^3$ dans \mathbf{C}^7 ainsi définie :

$$T(A_1, A_2, A_3) = (\operatorname{tr} A_1, \operatorname{tr} A_2, \operatorname{tr} A_3, \operatorname{tr} A_2 A_3, \operatorname{tr} A_3 A_1, \operatorname{tr} A_1 A_2, \operatorname{tr} A_1 A_2 A_3).$$

Il résulte du corollaire 5 que l'image de T est contenue dans la variété V .

PROPOSITION 7. *L'image de T est la variété V .*

Démonstration. Donnons-nous un point $(x_1, x_2, x_3, y_1, y_2, y_3, z) \in V$. Nous avons à construire trois matrices A_1, A_2, A_3 telles que $T(A_1, A_2, A_3) = (x_1, x_2, x_3, y_1, y_2, y_3, z)$. Nous allons distinguer plusieurs cas

- l'une des expressions $\lambda(x_1, x_2, y_3), \lambda(x_2, x_3, y_1), \lambda(x_3, x_1, y_2)$ n'est pas nulle.

Traisons le cas où $\lambda(x_1, x_2, y_3) \neq 0$. Prenons $A_1 = \begin{pmatrix} x_1 & 1 \\ -1 & 0 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & -\tau^{-1} \\ \tau & x_2 \end{pmatrix}$,
 $A_3 = \begin{pmatrix} t & u \\ v & x_3 - t \end{pmatrix}$. Nous devons en outre avoir

$$\begin{aligned} tx_1 + v - u &= y_2 \\ -\tau^{-1}v + \tau u + x_2(x_3 - t) &= y_1 \\ \tau t + (x_2 - \tau^{-1}x_1)v + \tau^{-1}(x_3 - t) &= z \\ \tau + \tau^{-1} &= y_3 \\ t(x_3 - t) - uv &= 1. \end{aligned}$$

Les trois premières équations forment un système linéaire en t, u, v dont le déterminant, compte tenu de la quatrième équation, vaut $-\lambda(x_1, x_2, y_3)$, qui est non nul par hypothèse. La compatibilité avec la dernière équation est assurée par la relation

$$\Lambda(x_1, x_2, x_3, y_1, y_2, y_3, z) = 0.$$

- $\lambda(x_1, x_2, y_3) = \lambda(x_2, x_3, y_1) = \lambda(x_3, x_1, y_2) = 0$ et l'un au moins des $|x_i|$ est différent de 2.

Traisons le cas $|x_i| \neq 2$.

On vérifie que l'on peut prendre les trois matrices soit sous la forme

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} u & 1 \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} v & 0 \\ w & v^{-1} \end{pmatrix},$$

soit sous la forme

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} u & 0 \\ 1 & u^{-1} \end{pmatrix} \begin{pmatrix} v & w \\ 0 & v^{-1} \end{pmatrix}.$$

- Enfin dans le dernier cas, on peut choisir pour A_1, A_2, A_3 les matrices $\pm I, \pm I, \pm I$.

PROPOSITION 8. *Les conditions suivantes sont équivalentes :*

1. A_1, A_2, A_3 ont une direction propre commune.
2. $\lambda(x_1, x_2, y_3) = \lambda(x_2, x_3, y_1) = \lambda(x_3, x_1, y_2) = 0$ et $\text{tr } A_1 A_2 A_3 = \text{tr } A_1 A_3 A_2$.
3. $\lambda(x_1, x_2, y_3) = \lambda(x_2, x_3, y_1) = \lambda(x_3, x_1, y_2) = \delta(X, Y) = 0$
où $\delta = p^2 - 4q$.

Démonstration. Clairement les assertions **2** et **3** sont équivalentes et sont impliquées par la première.

Supposons donc que l'on ait $\lambda(x_1, x_2, y_3) = \lambda(x_2, x_3, y_1) = \lambda(x_3, x_1, y_2) = 0$ et que A_1, A_2, A_3 n'aient pas de direction propre commune. Comme les opérateurs A_1, A_2, A_3 ont deux à deux une direction propre commune, on peut dans une base convenable les représenter par des matrices de la forme

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} u & \xi \\ 0 & u^{-1} \end{pmatrix} \text{ et } \begin{pmatrix} v & 0 \\ \zeta & v^{-1} \end{pmatrix} \text{ avec } \zeta\xi \neq 0 \text{ et } t \neq \pm 1.$$

On vérifie alors que $\text{tr } A_1 A_2 A_3 = tuv + (tuv)^{-1} + \zeta\xi t$ et $\text{tr } A_1 A_3 A_2 = tuv + (tuv)^{-1} + \zeta\xi t^{-1}$. Et donc $\text{tr } A_1 A_2 A_3 \neq \text{tr } A_1 A_3 A_2$. Ceci achève la démonstration.

Nous pouvons maintenant envisager de généraliser la section I au cas d'un groupe libre ayant un nombre fini de générateurs. Nous considérons d'abord le cas de F_3 , le groupe libre engendré par a_1, a_2, a_3 . Si φ est un homomorphisme de F_3 dans $SL(2, \mathbf{C})$, nous poserons

$$T\varphi = T(\varphi(a_1), \varphi(a_2), \varphi(a_3)).$$

PROPOSITION 9. *Si $w \in F_3$, il existe un polynôme $P \in \mathbb{Z}[X, Y, z]$, unique modulo Λ , tel que pour tout $\varphi \in \text{Hom}(F_3, SL(2, \mathbf{C}))$ on ait*

$$\text{tr } \varphi(w) = P(T\varphi).$$

Démonstration. L'existence se démontre par application répétée du théorème de Cayley-Hamilton et du lemme I.1. L'unicité résulte de la proposition 7.

THEOREME 10. *Si σ est un endomorphisme de F_3 , il existe une unique application polynomiale Φ_σ de V dans V telle que, pour tout $\varphi \in \text{Hom}(F_3, SL(2, \mathbf{C}))$ on ait*

$$T(\varphi \circ \sigma) = \Phi_\sigma(T\varphi).$$

Démonstration. Il suffit d'appliquer la proposition précédente aux éléments $\sigma(a_1), \sigma(a_2), \sigma(a_3), \sigma(a_2 a_3), \sigma(a_3 a_1), \sigma(a_1 a_2)$ et $\sigma(a_1 a_2 a_3)$ de F_3 .

COROLLAIRE 11. *Si σ et τ sont deux endomorphismes de F_3 , et si l'on pose $\sigma\tau = \tau \circ \sigma$, on a $\Phi_{\sigma\tau} = \Phi_\sigma \circ \Phi_\tau$.*

PROPOSITION 12. *Soit Ω la sous-variété de V définie par $\Lambda(X, Y, z) = 0, \lambda(x_1, x_2, y_3) = \lambda(x_2, x_3, y_1) = \lambda(x_3, x_1, y_2) = \delta(X, Y) = 0$. Alors Ω est invariante par toute application Φ_σ .*

Démonstration. Ceci résulte de la proposition 8.

Les calculs sur F_n , le groupe libre engendré par a_1, a_2, \dots, a_n , sont moins explicites. Soit I l'ensemble des parties non vides de $\{1, 2, \dots, n\}$. Un élément i de I est la donnée de ses éléments i_1, i_2, \dots, i_k ordonnés en croissant. Pour chaque $\varphi \in \text{Hom}(F_n, SL(2, \mathbf{C}))$, on note $T\varphi$ la collection $\{\text{tr } \varphi(a_{i_1} a_{i_2} \dots a_{i_k})\}_{i \in I}$, qui ne dépend que de la classe de la

représentation φ . On sait que l'ensemble des classes de représentations est une variété algébrique [2]. Sa dimension est $3(n-1)$. On peut le voir en observant que, sauf cas exceptionnels, on peut, étant donné $\varphi \in \text{Hom}(F_n, SL(2, \mathbf{C}))$, fixer une base de \mathbf{C}^2 de façon que les matrices de $\varphi(a_1)$ et $\varphi(a_2)$ aient la forme $\begin{pmatrix} x_1 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & -t^{-1} \\ t & x_2 \end{pmatrix}$. Les autres éléments $\varphi(a_3), \dots, \varphi(a_n)$ dépendent alors de $3(n-2)$ paramètres. Une application répétée du théorème de Cayley-Hamilton et de la proposition I.1 montre alors l'analogie de la proposition 9 : étant donné $w \in F_n$, il existe un polynôme $P \in \mathbb{Z}[(x_i)_{i \in I}]$, unique modulo un certain idéal définissant une sous-variété algébrique de dimension $3(n-1)$ de \mathbf{C}^I , tel que, pour tout $\varphi \in \text{Hom}(F_n, SL(2, \mathbf{C}))$, on ait $\text{tr } \varphi(w) = P(T\varphi)$.

Pour chaque $\sigma \in \text{End}(F_n)$ on définit de même que précédemment une application Φ_σ . Les applications Φ_σ laissent invariante une variété (celle qui est définie, en termes de traces, par le fait que n matrices 2×2 aient une direction propre commune).

Des résultats analogues sur F_n ont déjà été obtenus par Kolar et Nori [4]. On doit cependant observer qu'ils utilisent beaucoup trop de variables et qu'ils ne se sont pas préoccupés des questions d'unicité.

Dans deux articles à venir, l'un des auteurs donne un procédé général pour obtenir des relations entre les traces de matrice $p \times p$ et de leurs produits et traite le cas où au lieu de considérer les représentations d'un groupe libre dans $SL(2, \mathbf{C})$ on envisage des représentations dans $SL(3, \mathbf{C})$.

Terminons par une dernière remarque. Au lieu de considérer des représentations de F dans $SL(2, \mathbf{C})$, on peut utiliser des représentations dans $GL(2, \mathbf{C})$. En effet, à cause de l'homogénéité, le lemme I.1 est valable sans restriction sur les déterminants. Par ailleurs, pour une matrice 2×2 , A , le théorème de Cayley-Hamilton s'écrit

$$A^2 - A(\text{tr } A) + \frac{1}{2}[(\text{tr } A)^2 - \text{tr } A^2] = 0.$$

Donc, si A_1, A_2, \dots, A_n sont n matrices 2×2 inversibles, par une méthode analogue à celle que nous avons développée, tout produit de la forme $X_1^{n_1} X_2^{n_2} \dots X_k^{n_k}$ (avec $n_j \in \mathbb{Z}$ et $X_j \in \{A_1, A_2, \dots, A_n\}$ pour $j = 1, 2, \dots, n$) a une trace qui s'exprime comme fraction rationnelle à coefficients entiers en les traces des produits $\{A_{i_1} A_{i_2} \dots A_{i_k}\}_{i \in I}$ et les traces des matrices $\{A_j^2\}_{j=1,2,\dots,n}$.

Note ajoutée sur épreuves.

Au moment de corriger les épreuves, les auteurs ont eu connaissance d'un certain nombre de travaux antérieurs ([9] à [15]) sur le même sujet.

L'existence de P_w a été prouvée par Horowitz [9]. L'application induite Φ_σ a été considérée (seulement dans le cas où σ est un isomorphisme) également par Horowitz [10] qui a aussi déterminé le noyau de Φ . La considération du polynôme Q_σ est nouvelle.

Certaines démonstrations données ici sont plus simples que celles de Horowitz, bien qu'il y ait des recouvrements. Alors que Horowitz n'utilise que des relations entre traces, nos calculs prennent place dans l'algèbre introduite par Procesi [13] et Razmyslov [14], ce qui simplifie considérablement les calculs. D'ailleurs, Magnus [12] fait allusion à la

complexité des démonstrations de certaines identités (par exemple, les lemmes 3 et 4 de la section VI) et demande s'il est possible de les simplifier. Signalons qu'une description complète de l'idéal des relations entre traces a été donnée par Whittimore [15] dans le cas d'un groupe libre à quatre générateurs.

Les articles [11], [13] et [14] traitent des identités pour les matrices $n \times n$.

Références bibliographiques

- [1] J.-P. ALLOUCHE & J. PEYRIERE *Sur une formule de récurrence sur les traces de produits de matrices associées à certaines substitutions*. C. R. Acad. Sc. Paris 302 (II) (1986), 1135-1136.
- [2] Marc CULLER & Peter B. SHALEN *Varieties of group representations and splittings of 3-manifolds*. Ann. of Math. 117 (1983), 109-146.
- [3] M. KOLAR & M. K. ALI Preprint, University of Lethbridge, January 22, 1990 ; *Trace maps associated with general two-letter substitution rules*. Phys. Rev. A, submitted.
- [4] M. KOLAR & F. NORI *Trace maps of general substitutional sequences*. Phys. Rev. B 42 (1990), 1062-1065.
- [5] B. H. NEUMANN *Die Automorphismengruppe der freien*. Math. Ann. 107 (1933), 367-386.
- [6] J. NIELSEN *Die Isomorphismen der allgemeinen unendlichen Gruppe mit zwei Erzeugenden*. Math. Ann. 78 (1918), 385-397.
- [7] J. NIELSEN *Die Isomorphismen der freien Gruppen*. Math. Ann. 91 (1924), 169-209.
- [8] J. PEYRIERE *On the trace map for products of matrices associated with substitutive sequences*. J. Stat. Phys. 62 (1991), 411-414.
- [9] R. D. HOROWITZ *Characters of Free Groups Represented in the Two-Dimensional Special Linear Group*. Comm. Pure and Applied Math. XXV (1972), 635-649.
- [10] R. D. HOROWITZ *Induced automorphisms on Fricke Characters of Free Groups*. Trans. Amer. Math. Soc. 208 (1975), 41-50.
- [11] U. LERON *Trace Identities and Polynomial Identities of $n \times n$ Matrices*. J. of Algebra 42 (1976), 369-377.
- [12] W. MAGNUS *Rings of Fricke Characters and Automorphism Groups of Free Groups*. Math. Z. 170 (1980), 91-103.

- [13] C. PROCESI *The Invariant Theory of $n \times n$ Matrices*. Advances in Math. 19 (1976), 306–381.
- [14] JU. P. RAZMYSLOV *Trace Identities of Full Matrix Algebras over a Field of Characteristic Zero*. Izv. Akad. Nauk SSSR ser. Mat. 38 (1974) No. 4 (en russe); English translation : Math. USSR Izvestija 8 (1974), 727–760.
- [15] A. WHITTEMORE *On Special Linear Characters of Free Groups of Rank $n \geq 4$* . Proc. Amer. Math. Soc. 40 (1973), 383–388.

J. PEYRIERE
CNRS URA D0757
Université de Paris Sud
Mathématiques - Bâtiment 425
91405 ORSAY CEDEX (France)

WEN Zhi-ying & WEN Zhi-xiong
Université de Wuhan
Mathématiques
WUHAN, Hubei
(République Populaire de Chine)