$SL(2,\mathbb{Z})$, les tresses à trois brins, le tore modulaire et $Aut^{+}(F_2)$.

d'après Emil Artin *et* Jacob Nielsen

à Valentin Poénaru pour son nonantième anniversaire,
de la part de son ami Jean Cerf.

Résumé

Le groupe spécial linéaire entier deux-dimensionnel agit sur le quotient par symétrie centrale du tore entier. La présentation d'Artin du groupe B_3 des tresses à trois brins produit alors une présentation de $SL(2,\mathbf{Z})$ de générateurs, les paraboliques $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Cette « présentation d'Artin » de $SL(2,\mathbf{Z})$ clarifie l'action de son groupe dérivé sur le demi-plan de Poincaré $\mathbf{H}$ et son quotient le tore modulaire, ainsi que le théorème de Nielsen donnant le groupe des automorphismes directs du groupe libre de rang 2 en produit semi-direct, amalgamé sur le sous-groupe d'indice 2 du centre de B_3, des automorphismes intérieurs par B_3.

Abstract

The action of $SL(2,\mathbf{Z})$ on the integer torus and its quotient by central symmetry and Artin's presentation of three strings braid group B_3, produces a presentation with parabolic generators $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. This braided presentation describes the action of the derived group on Poincaré's half plane and its quotient the modular torus, just as Nielsen's theorem giving the group of direct automorphisms of the free group on two generators as semi-direct product, amalgamated on the index 2 subgroup of the center of B_3, of inner automorphisms with B_3.

2020 *Mathematics Subject Classification :*
Primary: 20F36; Secondary: 20H05, 20F05, 20H05, 20E36, 57K20, 01A99.
Key Words and Phrases. Braid group, modular torus, Nielsen's theorem for $Aut^{+}(F_2)$.

Soit $Aut(F_2)$ le groupe d'automorphismes de $F_2 = \langle u, v \rangle$, le groupe libre à deux générateurs, et $Int(F_2)$ le sous-groupe normal des automorphismes intérieurs.

Le groupe d'Artin des tresses à trois brins $B_3 = \langle a, b \mid aba = bab =: s \rangle$, de centre $Z = \langle s^2 = ababab \rangle$ se représente aussi[1]comme sous-groupe de $Aut(F_2)$.

[1] via $a(u,v) = (u, u^{-1}v)$, $\quad b(u,v) = (vu, v)$ (Cf. la Proposition de l'Appendice B).

L'abélianisation $F_2 \to \mathbb{Z}^2$ induit $\rho : Aut(F_2) \to GL(2,\mathbb{Z})$. Le sous-groupe des automorphismes *directs* de F_2 est noté :

$$Aut^+(F_2) := \rho^{-1}(SL(2,\mathbb{Z})) \subset Aut(F_2) \ .$$

Nielsen a essentiellement montré :

Théorème. — *Le sous-groupe $Int(F_2)$ des intériomorphismes est le noyau de :*

$$\rho^+ := \rho_| : Aut^+(F_2) \to SL(2,\mathbb{Z})$$

et engendre avec B_3 le groupe des automorphismes directs :

$$Aut^+(F_2) = Int(F_2)B_3 \ .$$

Comme ρ^+ est surjectif et $\rho^+(s^2) = -I \neq 1$ il suit la *présentation* d'Artin :

$$(\mathfrak{A}) \qquad SL(2,\mathbb{Z}) \simeq B_3/\langle s^4\rangle \ = \ \langle a,b \mid aba = bab, (ababab)^2 = 1\rangle$$

Mais la preuve proposée en Appendice B de ce théorème de Nielsen nécessite cette présentation, présentation qui, indépendamment de la surjectivité de ρ^+, est obtenue au §1 grâce à l'action affine de $SL(2,\mathbb{Z})$ sur la sphère plate $\mathbb{S}$, quotient du tore entier $\mathbb{T} = \mathbb{R}^2/\mathbb{Z}^2$ par la symétrie centrale $-I : \mathbb{T} \to \mathbb{T}, x \mapsto -x$.

Le §2 décrit, à l'aide de $(\mathfrak{A})$, l'action sur le demi-plan de Poincaré du groupe dérivé G' du groupe modulaire $G = SL(2,\mathbb{Z})/\{\pm I\}$, de quotient le *tore modulaire.*

L'appendice A explicite l'image dans $B_3 = \pi_0(Diff(\mathbb{S};\mathbb{T}_2,\{\overline{0}\}))$ des générateurs de la présentation $(\mathfrak{A})$, l'appendice B établit, en sus du plongement de B_3 dans $Aut^+(F_2)$, les théorèmes de Nielsen de structure et caractérisation de $Aut^+(F_2)$, l'appendice C, grâce à une forme normale dans B_3, déduit du théorème de Nielsen la classification à conjugaison près des éléments de torsion de $SL(2,\mathbb{Z})$ et $Aut^+(F_2)$, l'appendice D introduit le groupe des *tresses diédrales* à trois brins DB_3 permettant d'obtenir des résultats analogues pour le groupe complet $Aut(F_2)$ des automorphismes du groupe libre à deux générateurs, l'appendice E traite du produit semi-direct de deux groupes amalgamé[2] sur un sous-groupe commun.

Enfin en postroduction, des commentaires bibliographiques sur les divers traitements de ces résultats dans la littérature.

Remerciements

Cette note doit tout aux relectures attentives de Danielle Bozonat, Daniel Marin, des éditeurs Athanase Papdopoulos et Louis Funar et surtout Greg McShane qui, en partageant ses tentatives contre la conjecture d'unicité de Frobenius pour les nombres de Markoff (Cf. [**H**]), a poussé le metteur en scène à comprendre le tore modulaire. Enfin n'oublions pas l'arbitre qui, avec patience et longueur de temps, a fourni la matière du quatrième de couverture.

[2] une notion, sans doute bien connue, mais que nous n'avons pas trouvée dans la littérature.

§1 Le morphisme $SL(2,\mathbb{Z}) \to B_3/Z$ et la présentation parabolique de $SL(2,\mathbb{Z})$.

Le groupe $SL(2,\mathbb{Z})$ agit sur l'espace vectoriel $V=\mathbb{R}^2$, respectant le réseau $\Lambda=\mathbb{Z}^2$, induisant un automorphisme du tore quotient $\mathbb{T}=V/\Lambda$. La suite exacte :

$$0 \to \Lambda \to V \to \mathbb{T} \to 0$$

fait apparaître Λ comme groupe fondamental de $\mathbb{T}$ et $\overline{M} : (\mathbb{T},0) \to (\mathbb{T},0)$, l'automorphisme induit par $M \in SL(2,\mathbb{Z})$, produit sur ce groupe fondamental la restriction $\pi_1(\overline{M},0) = M_| : \Lambda \to \Lambda$ de M à Λ.

Le centre $\{\pm I\} < SL(2,\mathbb{Z})$ fixe le sous-groupe de 2-torsion $\mathbb{T}_2 = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ et l'action de $SL(2,\mathbb{Z})$ passe au quotient en une action par homéomorphismes affines :

$$\pi : G = PSL(2,\mathbb{Z}) \to Affeo(\mathbb{T}/\{\pm I\}, \mathbb{T}_2, \{\overline{0}\})$$

du groupe modulaire $G=SL(2,\mathbb{Z})/\{\pm I\}$ sur la sphère plate à 3+1 points singuliers (d'angle π)[1] $(\mathbb{T}/\{\pm I\}, \mathbb{T}_2, \{0\}) =: (\mathbb{S}, \{m,n,p,\infty\}, \{\infty\}) =: (\mathbb{S}, R, \{\infty\})$.

D'où par lissage[2], fibration de Cerf et suite exacte d'une fibration :

$$\pi_0 : SL(2,\mathbb{Z}) \to \pi_0(Affeo(\mathbb{S},R,\{\infty\})) \to$$
$$\to \pi_0(Diff(\mathbb{S},R,\{\infty\})) = \pi_1(Pl(R\setminus\{\infty\}, \mathbb{S}\setminus\{\infty\}))/Z$$

où $Z = \langle ababab \rangle$ est le centre du groupe B_3 des tresses à trois brins d'Artin[3] :

$$B_3 = \pi_1(Pl(\{m,n,p,\}, \mathbb{S}\setminus\{\infty\})) = \langle a,b \mid aba = bab \rangle \ .$$

Si $A = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on a :

$$ABA=S=BAB,\ S^4=I,\ S^2=-I\neq I \quad \text{et (cf. Appendice A)} \quad \pi_0(A)=a, \pi_0(B)=b$$

d'où un morphisme $\sigma : B_3 \to SL(2,\mathbb{Z})$ défini sur les générateurs de la présentation d'Artin par $\sigma(a) = A, \sigma(b) = B$ qui, si on note $\overline{\rho} : B_3 \to B_3/Z$, vérifie $\pi_0 \circ \sigma = \overline{\rho}$.

Ainsi, si $s = aba = bab$, le morphisme σ induit un morphisme injectif :

$$\overline{\sigma} : B_3/\langle s^4 \rangle \ \to SL(2,\mathbb{Z})$$

---

[1] notés $p = \overline{(\frac{1}{2},0)}$, $n = \overline{(0,\frac{1}{2})}$, $m = \overline{(\frac{1}{2},\frac{1}{2})}$ et $\infty = \overline{(0,0)}$.

[2] Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on déforme, dans le commutant de $\{\pm I\}$, $\overline{M}$ au voisinage de R en $\overline{M}_c$, affine près de R de partie linéaire la « conformisée $\begin{pmatrix} a & -c \\ c & a \end{pmatrix}$ sur la première colonne », de M.

[3] a (resp. b) fixe p (resp. n) et échange, par demi-tour positif, n (resp. p) et m.

qui est isomorphisme puisqu'aussi surjectif car, si $M \in SL(2,\mathbb{Z})$ et $\pi_0(M)$ est représenté par $\mu \in B_3$, les matrices M et $\sigma(\mu)$ sont la π_1-action de relevés de deux difféomorphismes homotopes de $(\mathbb{S}, R, \{\infty\}) = (\mathbb{T}/\{\pm I\}, \mathbb{T}_2, \{0\})$ donc sont, soit égales et $M = \sigma(\mu)$, soit opposées et $M = \sigma(s^2\mu)$. $\square$

On vient d'établir les présentations :

$$SL(2,\mathbb{Z}) = \langle A, B \mid ABA(BAB)^{-1}, (ABABAB)^2 \rangle$$
$$G = PSL(2,\mathbb{Z}) = \langle A, B \mid ABA(BAB)^{-1}, ABABAB \rangle$$

et $SL(2,\mathbb{Z})$ et $PSL(2,\mathbb{Z})$ ont leurs abélianisés cycliques d'ordre 12 et 6. ∎

§2 Action du groupe dérivé $SL(2,\mathbb{Z})'$ sur le demi-plan de Poincaré.

Soit dans le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C} | \Im(z) > 0\}$ les translatés par les puissances de A du domaine fondamental usuel de l'action de $G = PSL(2,\mathbb{Z})$:

$$\mathcal{B}_n = A^{-n}\big(\{z \in \mathbb{C} \mid \Im(z) > 0, -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2}, |z| \geq 1\}\big) \ .$$

L'union $\tilde{H} = \cup \mathcal{B}_n$ quotientée par l'image dans G du sous-groupe $\langle A^{-6}S^2 \rangle$ du groupe dérivé[1] $SL(2,\mathbb{Z})'$ de $SL(2,\mathbb{Z})$ est un hexagone hyperbolique pointé qui, par identification de ses côtés opposés, produit un tore symétrique pointé $\mathcal{T}$, identifications par les images dans G des éléments suivants du groupe dérivé :

$$f_n = A^{-n}A^{-3}SA^n = A^{-(n+3)}SA^n = A^{-(n+1)}A^{-1}BA^{(n+1)}$$
$$f_{n+1}f_{n-1} = A^{-(n+4)}SA^{(n+1)}A^{-(n+2)}SA^{n-1} = A^{-(n+3)}BAA^{(n+1)}A^{-(n+2)}SA^{n-1}$$
$$= A^{-(n+3)}BSA^{n-1} = A^{-(n+3)}SAA^{n-1} = A^{-(n+3)}SA^n = f_n \ .$$

De plus $A^{-6}S^2 = f_n f_{n-3} = (f_{n-1}f_{n-2}^{-1})(f_{n-1}^{-1}f_{n-2}) = [f_{n-1}^{-1}, f_{n-2}]$.

Ainsi[2] $\mathcal{T}$ est quotient de $\mathbb{H}$ par le sous-groupe de G engendré par les f_n :

$$\langle f_n ; n \in \mathbb{Z} \rangle \ = \ \langle f_{-2}, f_{-1} \rangle$$

qui est[3] d'indice 6 dans le groupe modulaire G (l'indice de son l'abélianisé G').

Comme $\langle f_n ; n \in \mathbb{Z} \rangle \subset G'$, ce sous-groupe est le groupe dérivé de G :

$$G' = PSL(2,\mathbb{Z})' \ = \ \langle f_{-2}, f_{-1} \rangle$$

---

[1] car, dans l'abélialisé on a : $\overline{A} = \overline{B}$ donc $\overline{S} = \overline{A}^3$, ainsi $\overline{A^{-6}S^2} = \overline{1}$.

[2] notant par abus $f_n \in G$ les images dans le groupe modulaire G des $f_n \in SL(2,\mathbb{Z})$.

[3] car $\cup_{n=0}^{5} \mathfrak{B}_n$, union de 6 translatés du domaine fondamental usuel de $SL(2,\mathbb{Z})$, est un domaine fondamental de ce sous-groupe $\langle f_n ; n \in \mathbb{Z} \rangle$.

et le tore modulaire est $\mathcal{T}$, de parabolique de cusp, le commutateur[4] de f_{-1}^{-1} et f_{-2}. $\square$

Comme $-I = S^2 \in SL(2,\mathbb{Z})$ est d'abélianisé $\overline{A}^6 \neq 0$, $-I \notin SL(2,\mathbb{Z})'$, ainsi le quotient $SL(2,\mathbb{Z}) \to G$ est injectif sur le groupe dérivé $SL(2,\mathbb{Z})'$ et ce groupe dérivé est engendré[5]par $f_{-2} = BA^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ et $f_{-1} = A^{-1}B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. ∎

APPENDICE A

Description de $\mathbb{T}/\{\pm I\}$ et vérification de $\pi_0(A) = a, \pi_0(B) = b$.

En identifiant (V,Λ) au plan complexe muni du réseau de Gauß $(\mathbb{C},\mathfrak{G})$ où $\mathfrak{G} = \mathbb{Z} + i\mathbb{Z}$, la fonction $\wp : \mathbb{C} \to \mathbb{C}$ de Weierstraß :

$$\wp(z) = \frac{1}{z^2} + \sum_{\gamma \in \mathfrak{G}\setminus\{0\}} \frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}$$

paire et invariante par $\mathfrak{G}$, identifie $\mathbb{T}/\{\pm I\}$ à $\mathbb{C} \cup \{\infty\}$ avec $\wp(\overline{0}) = \infty$ et[1] :

$$\wp(m) = \wp(\frac{1}{2}(1+i)) = 0,\ \wp(p) = \wp(\frac{1}{2}) = -\wp(\frac{1}{2}i) = -\wp(n) \in]0,+\infty[\ .$$

Les deux «sous-groupes de coordonnées» $\mathbf{t} = \mathbb{R}/\mathbb{Z}$, $\mathbf{u} = \mathbb{R}i/\mathbb{Z}i$ et les deux «sous-groupes diagonaux» $\Delta_+ = \mathbb{R}(1+i)/\mathbb{Z}(1+i)$ et $\Delta_- = \mathbb{R}(1-i)/\mathbb{Z}(1-i)$, points fixes d'isométries conformes[2] du réseau $\mathfrak{G}$ commutant à $-I$, vont dans des droites et sont d'images[3] les demi-axes réels tronqués et les demi-axes imaginaires :

$$\wp(\mathbf{t}) = H^+_{\wp(p)} := [\wp(p), +\infty[\cup\{\infty\},\ \wp(\mathbf{u}) = H_-^{\wp(n)} :=]-\infty, \wp(n)] \cup \{\infty\} \subset \mathbb{R}\cup\{\infty\}$$
$$\wp(\Delta_+) = V_- :=]-\infty, 0]\, i \cup \{\infty\},\ \wp(\Delta_-) = V^+ :=\ [0, +\infty[\, i \cup \{\infty\} \subset \mathbb{R}i \cup \{\infty\}$$

Ainsi l'action de $A = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ fixe $H^+_{\wp(p)}$ et envoie $H_-^{\wp(n)}, V_-$ sur $V^+, H_-^{\wp(n)}$ respectivement, c'est le «demi-tour» positif a.

Et l'action de $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ fixe $H_-^{\wp(n)}$ et envoie $H^+_{\wp(p)}, V^+$ sur $V_-, H^+_{\wp(p)}$ respectivement, c'est le «demi-tour» positif b. ∎

---

[4] avec la convention $[a,b] = a^{-1}b^{-1}ab$ de Bourbaki, Hall...

[5] librement puisque c'est le groupe fondamental d'un tore pointé.

[1] comme $\wp(iz) = -\wp(z)$ et $m - im \in \Lambda$ on a $\wp(m) = 0$ et $\wp(n) = -\wp(p)$. Ainsi $\wp^{-1}(0) = m + \Lambda$, donc comme $\wp(\overline{z}) = \overline{\wp(z)}$ et, près de 0, on a $\wp(z) \sim \frac{1}{z^2}$, on a $\wp(]0,p]) \subset]0,+\infty[$.

[2] $z \mapsto \pm\overline{z}$ et $z \mapsto \pm i\overline{z}$ qui toutes deux fixent l'origine 0.

[3] remarquer de nouveau que, près de 0, on a $\wp(z) \sim \frac{1}{z^2}$.

APPENDICE B

Les théorèmes de Nielsen de structure et caractérisation de $Aut^+(F_2)$.

Soit $F_2 = \langle u, v\rangle$ le groupe libre à deux générateurs notés u, v.

On identifie le groupe libre F_2 à son groupe d'automorphismes intérieurs par :

$$\varphi : F_2 \to Int(F_2),\ x \mapsto \varphi_x : y \mapsto xyx^{-1} = y^{x^{-1}} =: {}^x y$$

et note $Y = \langle s^4\rangle$ le sous-groupe d'indice 2 du centre $Z = \langle s^2\rangle$ de B_3 identifié, par $s^4 \mapsto \varphi_{[u,v]} \in Int(F_2)$, au sous-groupe cyclique infini $Y = \langle \varphi_{[u,v]}\rangle \subset Int(F_2)$.

Proposition. — *Les endomorphismes $\alpha, \beta : F_2 \to F_2$ définis par :*

$$\alpha(u, v) = (u, u^{-1}v) \quad \beta(u, v) = (vu, v)$$

sont des isomorphismes d'inverses définis par :

$$\alpha^{-1}(u, v) = (u, uv), \quad \beta^{-1}(u, v) = (v^{-1}u, v)$$

vérifiant la relation de tresse $\alpha\beta\alpha = \beta\alpha\beta =: s\ : (u, v) \mapsto (v^u, u^{-1})$, avec de plus : $s^2\ : (u, v) \mapsto (u^{-1}, v^{-1})^{vu}$ et $s^4\ : (u, v) \mapsto (u, v)^{v^{-1}u^{-1}vu} = (u, v)^{[v,u]} = \varphi_{[u,v]}(u, v)$.

Ainsi α, β définissent un morphisme injectif :

$$\Psi : B_3 \to Aut(F_2),\ \Psi(a) = \alpha, \Psi(b) = \beta\ .$$

Par abus, on identifiera B_3 au sous-groupe $\Psi(B_3)$ de $Aut(F_2)$. Soit :

$$\psi : B_3 \to Aut(Int(F_2)),\ \psi(x) : h \mapsto x \circ h \circ x^{-1}\ .$$

Le sous-groupe $H = Int(F_2)B_3 \subset Aut^+(F_2)$ est[1] produit semi-direct suivant ψ :

$$H = Int(F_2) \rtimes_{\psi,Y} B_3 \subset Aut^+(F_2)$$

de $Int(F_2)$ par B_3 amalgamé sur Y (identifiant $\varphi_{[u,v]}$ à s^4).

Démonstration de la Proposition. — Que α^{-1} soit inverse de α suit de :

$$\alpha\alpha^{-1}(u, v) = \alpha(u, uv) = (u, uu^{-1}v) = (u, v)$$

donc $\alpha\alpha^{-1} = Id$, de même on établit $\alpha^{-1}\alpha = Id = \beta\beta^{-1} = \beta^{-1}\beta$. □

Pour les relations, notant $s = \alpha\beta\alpha$, $s' = \beta\alpha\beta$, on a :

$$s(u, v) = \alpha\beta(u, u^{-1}v) = \alpha(vu, u^{-1}v^{-1}v) = \alpha(vu, u^{-1}) = (u^{-1}vu, u^{-1}) = (v^u, u^{-1})$$

$s'(u, v) = \beta\alpha(vu, v) = \beta(u^{-1}vu, u^{-1}v) = (v^{vu}, u^{-1}v^{-1}v) = (v^u, u^{-1}) = s(u, v)$, ainsi :

$$s^2(u, v) = s(v^u, u^{-1}) = ((u^{-1})^{v^u}, (v^{-1})^u) = ((u^{-1})^{vu}, (v^{-1})^u) = (u^{-1}, v^{-1})^{vu}$$

$$s^4(u, v) = s^2((u^{-1}, v^{-1})^{vu}) = (u, v)^{vu(v^{-1}u^{-1})^{vu}} = (u, v)^{[v,u]} = \varphi_{[u,v]}(u, v)$$

[1] Cf. **Corollaire** de l'appendice E.

□

Comme[2] ker(Ψ) ⊂ $ker(\rho \circ \Psi) \subset ker(\rho^+ \circ \Psi) = \langle s^4 \rangle$, celui de la présentation d'Artin ($\mathfrak{A}$), l'intériomorphisme $s^4 = \varphi_{[u,v]}$ étant d'ordre infini, Ψ est injectif.

□ ∎

Désormais on renote la paire de générateurs de F_2 en $t = (t_1, t_2) := (u, v)$.

Définitions et notations. Soit $W = W(T) = T_{i_0}^{\epsilon_0} \cdots T_{i_k}^{\epsilon_k} \cdots T_{i_n}^{\epsilon_n}$, $(i_j, \epsilon_j) \in \{1,2\} \times \{-1,1\}$ un mot non vide en les indéterminées[3] T_1, T_2 et leurs *inverses* T_1^{-1}, T_2^{-1}, son *mot inverse* est $W^{-1} = W^{-1}(T) = T_{i_n}^{-\epsilon_n} \cdots T_{i_k}^{-\epsilon_k} \cdots T_{i_0}^{-\epsilon_0}$. Le mot vide est noté $1 := \emptyset$.

Si $k > 0, i_{k-1} = i_k$, $\epsilon_{k-1} + \epsilon_k = 0$ et $\{j_0, \ldots, j_{n-2}\} = \{0, \ldots, n\} \setminus \{k-1, k\}$, dans le même ordre, $W' = W_{k,k+1} = T_{i_{j_0}}^{\epsilon_{j_0}} \cdots T_{i_{j_{n-2}}}^{\epsilon_{j_{n-2}}}$ est dit *réduction élémentaire* de W.

On notera plus visuellement si[4] $1 < k < n$, $W_{k-1,k} = T_{i_0}^{\epsilon_0} \cdots \{T_{i_{k-1}}^{\epsilon_{k-1}} T_{i_k}^{\epsilon_k}\} \cdots T_{i_n}^{\epsilon_n}$.

Une *réduction* de W est un mot W'' tel qu'il y a $W = W_0, \cdots, W_p = W''$une suite de mots telle que pour $1 \leq k \leq p, W_k$ est réduction élémentaire de W_{k-1}.

Si un mot $W = ABC$ est juxtaposé de trois mots A, B, C avec A (resp. B, C) se réduisant sur 1, on notera $W = \{A\}BC$ (resp. $A\{B\}C, AB\{C\}$).

Un mot W, est *équivalent* à W', noté $W \approx W'$ s'il y a $W = W_0, \ldots, W_r = W'$ avec W_l réduction élémentaire de W_{l-1} ou W_{l+1} (supposant $l > 0, l < r$ dans le premier et le second cas).

Un mot $W = T_{i_0}^{\epsilon_0} \cdots T_{i_n}^{\epsilon_n}$ est dit *réduit* s'il n'a pas de réduction élémentaire.

Un mot $W = T_{i_0}^{\epsilon_0} \cdots T_{i_n}^{\epsilon_n}$ est *cycliquement réduit* s'il est réduit et si $T_{i_0}^{\epsilon_0} \neq T_{i_n}^{-\epsilon_n}$.

Pour tout mot W il y a un unique[5] mot réduit, noté $\widetilde{W}$, réduction de W. Cette *réduction réduite* de W ne dépend que de la classe d'équivalence de W.

Le nombre $n+1$ de termes de $W = T_{i_0}^{\epsilon_0} \cdots T_{i_n}^{\epsilon_n}$ est la *longueur* $l_T(W) = l(W)$ du mot W.

En substituant les générateurs t_1, t_2 de F_2 dans les indéterminées T_1, T_2, on a les mêmes définitions et notations pour les éléments du groupe libre à deux générateurs :

$$w = t_{i_0}^{\epsilon_0} \cdots t_{i_n}^{\epsilon_n} \in F_2, (i_j, \epsilon_j) \in \{1,2\} \times \{-1,1\}$$

Définition. Un endomorphisme $x_0 : F_2 \to F_2$ induit un endomorphisme :

$$\overline{x_0} = ab(x) : \mathbb{Z}^2 = ab(F_2) \to ab(F_2) = \mathbb{Z}^2$$

de l'abélianisé $\mathbb{Z}^2$. On dira que l'endomorphisme x_0 est *direct* si $det(\overline{x_0}) > 0$.

Théorème (de Nielsen, 1917). — *i) Un endomorphisme surjectif x du groupe libre à deux générateurs F_2 est un automorphisme.*

---

[2] car $\rho(\alpha) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $\rho(\beta) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in SL(2, \mathbb{Z})$, donc $\Psi(B_3) \subset Aut^+(F_2)$.

[3] non-commutatives, on notera $T = (T_1, T_2)$ la paire de ces indéterminées.

[4] et $W_{0,1} = \{T_{i_0}^{\epsilon_0} T_{i_1}^{\epsilon_1}\} T_{i_2} \cdots T_{i_n}^{\epsilon_n}, W_{n-1,n} = T_{i_0}^{\epsilon_0} \cdots T_{i_{n-2}}^{\epsilon_{n-2}} \{T_{i_{n-1}} T_{i_n}^{\epsilon_n}\}$.

[5] sans unicité de la réduction $\{II^{-1}\}I$ et $I\{I^{-1}I\}$ sont deux réductions de $II^{-1}I$ à $\widetilde{II^{-1}I} = I$. Pour une démonstration, voir Théorème 1 et Lemme 1 de [**Se**].

ii) Le groupe d'automorphismes directs du groupe libre F_2 est produit semi-direct suivant ψ amalgamé sur le sous-groupe Y d'indice 2 dans le centre de B_3 :

$$Aut^+(F_2) = Int(F_2) \rtimes_{<\varphi_{[t_1,t_2]} = s^4>} B_3 \ .$$

iii) Le groupe $Int(F_2)$ des automorphismes intérieurs de F_2 est le noyau de :

$$\rho : Aut(F_2) \to Aut(\mathbb{Z}^2) = GL(2, \mathbb{Z}) \ .$$

iv) Un endomorphisme $\varphi : F_2 \to F_2, \varphi(t_i) = X_i, i = 1, 2$ est un automorphisme direct ssi il préserve à conjugaison près le commutateur $[t_1, t_2]$ des générateurs :

$$(Cw) \qquad [X_1, X_2] = X_1^{-1} X_2^{-1} X_1 X_2 = [t_1, t_2]^w = w^{-1}[t_1, t_2]w \ .$$

De plus, il est dans B_3 si et seulement si $[X_1, X_2] = [t_1, t_2]$, c.à.d. on a (C_1).

Remarques. — (1) *i)* vaut pour tout groupe libre de type fini[6] F: le gradué central descendant de F étant engendré par son terme de degré 1, un endomorphisme surjectif x de F est surjectif au niveau du gradué central descendant $gr_{\mathfrak{c}}(F)$ donc, puisque chaque terme est de dimension finie, injectif et, puisqu'un élément non nul de F se détecte dans $gr_{\mathfrak{c}}(F)$, x est aussi injectif donc un isomorphisme. □

(2) Le point *iii)* est particulier à la dimension 2 :

$$\psi : F_3 = \langle t_1, t_2, t_3 \rangle \to F_3, \ \psi(t_1) = t_1^{t_2} = t_2^{-1} t_1 t_2, \ \psi(t_2) = t_2, \ \psi(t_3) = t_3$$

est dans le noyau de $\rho_3 : Aut(F_3) \to GL(3, \mathbb{Z})$ mais n'est pas intérieur[7]. □

(3) Les éléments de H et B_3 vérifient les conditions[8](C_w) et (C_1). □

(4) Si x vérifie (C_1), alors $x = \varphi_w b$ où $w \in F_2, b \in B_3$ et, si ${}^w[t_1, t_2] = [t_1, t_2]$, alors $w = [t_1, t_2]^n \in \langle [t_1, t_2] \rangle$, ainsi le « De plus$\cdots$ » suit[9] de *iv)* et *ii)*. □

Dans la suite on dira « Nielsen $*$ » pour « le point $*$ du Théorème de Nielsen ».

Définitions. La *taille* d'un endomorphisme x défini par la paire de mots réduits[10] : $X = (X_1, X_2)$, $x(t_i) = X_i(t)$, $i = 1, 2$ est $|x| := l_T(X_1) + l_T(X_2)$. L'endomorphisme x est *minimal* si sa taille $|x|$ est minimale dans la double classe HxH.

Soit $M = X_{i_0}^{\epsilon_0} \cdots X_{i_n}^{\epsilon_n}$ un mot réduit en une paire d'indéterminées notée abusivement $X = (X_1, X_2)$ et $N = N(T)$, le mot (non réduit), obtenu après avoir substitué dans X la paire $X = (X_1(T), X_2(T))$ définissant x.

---

[6] nous donnerons cependant ici aussi une démonstration de *i)* « à la Nielsen ».

[7] si $\psi = \varphi_w$ alors w doit commuter à t_2, donc $w = t_2^n$ pour un $n \in \mathbf{Z}$, mais il doit aussi commuter à t_3, ainsi $n = 0$ et $\varphi_w = \varphi_1 = Id \neq \psi$ car $\psi(t_1) \neq t_1$. □

[8] $t \mapsto t^w$ étant un morphisme, l'isomorphisme intérieur $\varphi_{w^{-1}}$, on a $[t_1^w, t_2^w] = [t_1, t_2]^w$ et : $[\alpha(t_1), \alpha(t_2)] = [t_1, t_1^{-1} t_2] = t_1^{-1}(t_1^{-1} t_2)^{-1} t_1 t_1^{-1} t_2 = t_1^{-1}(t_2^{-1} t_1) t_1 t_1^{-1} t_2 = [t_1, t_2]$ et : $[\beta(t_1), \beta(t_2)] = [t_2 t_1, t_2] = (t_2 t_1)^{-1} t_2^{-1} (t_2 t_1) t_2 = t_1^{-1} t_2^{-1} t_2^{-1} t_2 t_1 t_2 = [t_1, t_2]$. □

[9] En effet, comme $\varphi_{[t_1,t_2]^n} = s^{4n}$, on a $x = s^{4n} b \in B_3$. □

[10] en la paire d'indéterminées $T = (T_1, T_2)$.

Il y a des mots réduits[11] $C_0, D_0, \cdots, C_k, D_k, \cdots, C_{n-1}, D_{n-1}, C_n$ tels que :

$$X_{i_0}^{\epsilon_0} = C_0 D_0, \text{ pour } 0 < k < n, X_{i_k}^{\epsilon_k} = D_{k-1}^{-1} C_k D_k, \text{ et } X_{i_n}^{\epsilon_n} = D_{n-1}^{-1} C_n$$

comme mots réduits et, pour $0 < k \leq n$, le mot $C_{k-1}C_k$ est réduit, ils peuvent être définis inductivement dans cet ordre en partant de la gauche[12] ou de la droite.

Un endomorphisme direct est dit *admissible* s'il est surjectif ou satisfait (C_w).

LEMME. — *Si l'endomorphisme x est admissible minimal alors pour $0 \leq i \leq n$ le mot $C_i \neq \emptyset$ est non vide donc $C_0 \cdots C_n$ est la réduction réduite $\widetilde{N}$ du mot N.*

Les C_i, $i = 0, \ldots n$ (non vides, d'après ce LEMME) sont dits *subsistants* de N.

Démonstration du Théorème. — *iii*) Comme $Int(F_2) \subset ker(\rho) \subset Aut^+(F_2)$ et, d'après la présentation $(\mathfrak{A})$, on a $B_3 \cap ker(\rho) = Y$, le point *iii*) suit de *ii*). □

i) et *ii*) Soit x_0 admissible et $x = k \circ x_0 \circ h$, $h, k \in H$, minimal pour la taille $|x|$ de x dans la double classe Hx_0H de x_0 suivant H.

Si $\tau \in Aut(F_2), \tau(t_i) = t_{3-i}$, $i = 1, 2$ alors $det(\overline{\tau}) = -1$ et $|x\tau| = |x|$ donc, quitte à prendre $x\tau$, il suffit dans *i*), de considérer un endomorphisme surjectif direct.

Par surjectivité de x il y a une paire[13] $Y = (Y_1, Y_2)$ telle que $\widetilde{Y_k}(T) = T_k$ pour $k = 1, 2$. Ainsi, par le LEMME, Y_1 et Y_2 sont de longueur 1, donc aussi X_1 et X_2.

L'endomorphisme admissible minimal x étant direct on a :

$$\text{soit } X = T, \; x(t) = (t_1, t_2) = t$$

$$\text{soit } X = (T_1^{-1}, T_2^{-1}), \; x(t) = (t_1^{-1}, t_2^{-1}) = s^2(t)^{t_1^{-1}t_2^{-1}} : x = \varphi_{t_2 t_1} s^2 \in H$$

$$\text{soit } X = (T_2^{\epsilon}, T_1^{-\epsilon}), \; x(t) = (t_2^{\epsilon}, t_1^{-\epsilon}) = \left(s^{\epsilon}(t)^{t_1^{-1}}\right) : x = \varphi_{t_1} s^{\epsilon} \in H, \; \epsilon = -1, 1.$$

Dans tous ces cas l'endomorphisme admissible minimal $x = kx_0h$ est dans le sous-groupe H, donc x_0, est dans $H = Int(F_2) \rtimes_{<\varphi_{[t_1,t_2]} = s^4>} B_3$, d'où *i*) et *ii*). □

iv) D'après la REMARQUE (3) on peut demander à l'endomorphisme x, parmi ceux minimisant la taille $|x|$ dans la double classe Hx_0H, de minimiser aussi $l(w)$. Alors[14] $l(t_2w) = l(w)+1 = l(t_1w)$ et $w^{-1}[t_1, t_2]w$ est réduction réduite de $[X_1, X_2]$.

---

[11] en la paire d'indéterminées T, certains de ces mots C_i, D_j pouvant être vides.

[12] $C_0\{D_0D_0^{-1}\}E_1X_{i_2}^{\epsilon_2} \cdots X_{i_n}^{\epsilon_n}$ est la plus grande suite de réductions élémentaires entre $X_{i_0}^{\epsilon_0}$ et $X_{i_1}^{\epsilon_1}$ dans $X_{i_0}^{\epsilon_0} \cdots X_{i_n}^{\epsilon_n}$, puis $C_0C_1\{D_1D_1^{-1}\}E_2X_{i_3}^{\epsilon_3} \cdots X_{i_n}^{\epsilon_n}$ est la plus grande suite de réductions élémentaires entre E_1 et $X_{i_2}^{\epsilon_2}$ dans $C_0E_1X_{i_2}^{\epsilon_2} \cdots X_{i_n}^{\epsilon_n} \ldots$

[13] de mots réduits en la paire d'indéterminées $X = (X_1, X_2)$.

[14] Sinon pour un $i \in \{1, 2\}, w = t_i^{-1}w', l(w') = l(w) - 1$ et, comme pour $i = 1, 2$ on a : $[t_1, t_2]^{t_i^{-1}} = [t_2^{3-2i}, t_1^{2i-3}] = [k^{-1}(t_1), k^{-1}(t_2)]$, où $k = k_i = (s^{2i-3})^{t_1^{-1}}$ et $x' = kx, w'' = k(w')$, on a : $x' \in Hx \subset HxH$, $|x'| = |x|$, $l(w'') = l(w') < l(w)$ et $[x'(t_1), x'(t_2)] = k([x(t_1), x(t_2)] = k([t_1, t_2]^{t_i^{-1}w'}) = k([k^{-1}(t_1), k^{-1}(t_2)]^{w'}) = ([kk^{-1}(t_1), kk^{-1}(t_2)]^{k(w')} = [t_1, t_2]^{w''}$, contredisant que x minimise $|x|$, puis $l(w)$ dans la double classe HxH. □

Si $w\neq 1$, donc $w=w'a$, $a=t_k^{\pm 1}$, alors, par le LEMME, $X_i=X_i''a$ pour $i=1,2$ et $x'=\varphi_a x = x^{a^{-1}}$, défini par $(X_1', X_2') = (\widetilde{aX''}_1, \widetilde{aX_2''})$, vérifie $[X_1', X_2']=[t_1, t_2]^{w'}$ et $|x'| \leq |x|$ contredisant la minimalité de $|x|$, puis $l(w)$ dans la double classe Hx_0H.

On a donc $(C1)$ $[X_1, X_2] = [t_1, t_2]$ et le LEMME donne les égalités réduites :

$$X_1^{-1} = t_1^{-1}D_0,\ X_2^{-1} = D_0^{-1}t_2^{-1}D_1,\ X_1 = D_1^{-1}t_1D_2,\ X_2 = D_2^{-1}t_2$$

On a $l(X_i^{-1})=l(X_i)$, $i=1,2$ donc $l(D_0)=l(D_1)+l(D_2)=l(D_1)+l(D_0)+l(D_1)$, ainsi $l(D_1)=0$ et $X_1=t_1D_2=D_0^{-1}t_1$, $X_2X_1=(D_0^{-1}t_2^{-1})^{-1}(t_1^{-1}D_0)^{-1}=t_2t_1$.

Comme $l(X_1)+l(X_2)=|x|\leq|x\beta|=l(\widetilde{X_2X_1})+l(X_2)=2+l(X_2)$, on a $l(D_2)\leq 1$.

Comme les X_i sont réduits, $t_1^{-1}\neq D_2\neq t_2$, or on ne peut avoir[15] $D_2\in\{t_1, t_2^{-1}\}$. Ainsi $D_2=1$, donc $X_1=t_1, X_2=t_2$, $x=1$ et $x_0=k^{-1}xh^{-1}=k^{-1}h^{-1}\in H$. □ ∎

Démonstration du Lemme. — Rappelons que (X_1, X_2) est la paire de mots en la paire $T=(T_1, T_2)$ d'indéterminées telle que l'endomorphisme x est donné par $x(t_i)=X_i(t), i=1,2$. Si, pour un $1\leq k\leq n$, $i_k\neq i_{k-1}$, on note :

$$U = X_{i_{k-1}}^{\epsilon_{k-1}},\ V = X_{i_k}^{\epsilon_k},\ \nu = \epsilon_{k-1},\ \epsilon = \epsilon_{k-1}\epsilon_k\ .$$

AFFIRMATION 1. — *Il y a $h\in H$ tel que xh minimise encore la taille dans la double classe Hx_0H et est défini par l'un des deux cas :*

i) (cas I) (U, V)

ii) (cas II) (V, U) .

Démonstration. — Quitte[16] à changer x en $x\varphi_{t_1}s$, on peut supposer $\epsilon=+1$. Alors, si $\nu=-1$, $h=\varphi_{t_2t_1}s^2$ convient et si $\nu=1$, $\{U, V\}=\{X_1, X_2\}$. ∎

Par abus, on renomme désormais le xh donné par l'AFFIRMATION 1 en x.

COMPLÉMENT 1. — *Suivant le cas I ou II, les paires de mots réduits :*

(cas I) $(U, \widetilde{UV}),\ (U, \widetilde{VU}),\ (\widetilde{VU}, V)$

(cas II) $(\widetilde{UV}, U),\ (\widetilde{VU}, U),\ (V, \widetilde{VU})$

définissent des endomorphismes de la double classe Hx_0H de x_0, à savoir :

$$x\alpha^{-1},\ \varphi_U^{-1}x\alpha^{-1},\ x\beta \quad \text{resp.} \quad x\beta,\ \varphi_U^{-1}x\beta,\ x\alpha^{-1} \qquad \square$$

Démonstration pour les subsistants extrêmes C_0, C_n. — Si $C_0=\emptyset$ est vide on a $X_{i_0}^{\epsilon_0}=D_0$ et, comme le mot M est réduit, $i_1\neq i_0$.

[15] sinon $X_1=t_1^2$ ou $X_2=t_2^2$ et, dans le terme de degré 2 du gradué central descendant $[F_2, F_2]/\big[[F_2, F_2], F_2\big]\simeq\mathbb{Z}$, la classe du commutateur $[X_1, X_2]$ serait divisible par 2 contredisant que, d'après la condition $(C1)$, elle est celle de son générateur.

[16] puisque $x\varphi_{t_1}s\in xH\subset Hx_0H$, étant défini par $t\mapsto(X_2, X_1^{-1})$, a même taille que x.

Alors[17] $l(\widetilde{UV}) = l(V) - l(U) < l(V)$ et suivant le cas I ou II, d'après le complément de l'Affirmation 1, l'endomorphisme $x\alpha^{-1}$ ou $x\beta$ contredit que xh minimise la taille dans la double classe Hx_0H. □

Ainsi le subsistant initial $C_0 \neq \emptyset$ est non vide. En considérant le mot inverse $M^{-1} = X_{i_n}^{-\epsilon_n} \cdots X_{i_0}^{-\epsilon_0}$ on établit de même que $C_n \neq \emptyset$ est non vide. □

Démonstration pour les subsistant intérieurs. — Supposons, pour un $0 < k < n$, $C_k = \emptyset$ vide, alors $X_{i_k}^{\epsilon_k} = D_{k-1}^{-1} D_k$ et D_k, D_{k-1}^{-1}, ne pouvant être subsitant final, ou inital, vide du mot $M_{k-} = X_{i_0} \cdots X_{i_k}$ou $M_{k+} = X_{i_k} \cdots X_{i_n}$, on a : $D_k \neq \emptyset \neq D_{k-1}$.

Affirmation 2. — *$i_{k-1} \neq i_k \neq i_{k+1}$ (donc[18]$i_{k-1} = i_{k+1}$) et $\epsilon_{k-1} = \epsilon_{k+1}$.*

Démonstration. — Si $i_{k-1} = i_k = i_{k+1}$, alors, puisque Z est réduit, on a : $\epsilon_{k-1} = \epsilon_k = \epsilon_{k+1}$ et[19]$D_{k-2}^{-1} C_{k-1} D_{k-1} = D_{k-1}^{-1} D_k = D_k^{-1} C_{k+1} D_{k+1}$.

Suivant que $l(D_{k-1}) \leq l(D_k)$ ou $l(D_{k-1}) \geq l(D_k)$, on a $X_{i_k}^{\epsilon_k} = D_{k-1}^{-1} E D_{k-1}$ ou $X_{i_k}^{\epsilon_k} = D_k^{-1} E D_k$, on notera selon le cas $D = D_{k-1}$ ou D_k.

Comme[20] on a $X_{i_k}^{\epsilon_k} \neq 1$ donc $E \neq \emptyset$, $X_{i_{k-1}}^{\epsilon_{k-1}} X_{i_k}^{\epsilon_k} X_{i_{k+1}}^{\epsilon_{k+1}} = D^{-1} E^3 D$ et le terme E central, celui qui est dans $X_{i_k}^{\epsilon_k} = D^{-1} E D$, ne peut disparaître. □

Si $i_{k-1} = i_k \neq i_{k+1}$ ou $i_{k-1} \neq i_k = i_{k+1}$, quitte à considérer le mot inverse M^{-1}, on supposera que l'on est dans le second cas $i_k = i_{k+1}$ alors, avec les notations précédant l'Affirmation 1 et car M est réduit, on a $X_{i_{k-1}}^{\epsilon_{k-1}} X_{i_k}^{\epsilon_k} X_{i_{k+1}}^{\epsilon_{k+1}} = UVV$.

Comme $\emptyset \neq D_k$, $D_k = D'_k a$, $a = t_i^{\pm 1}$ dernière lettre du V central donc a^{-1} est première du V de droite et[21] de D_{k-1}^{-1} donc a est aussi dernière lettre de U.

Ainsi $l(V^{a^{-1}}) = l(V) - 2 < l(V)$, $l(U^{a^{-1}}) \leq l(U)$ et $\varphi_a x \in Hx_0H$ contredit que $|x|$ minimise la taille dans la double classe Hx_0H. □

Si $\epsilon_{k-1} = -\epsilon_{k+1}$ on a $X_{i_{k-1}}^{\epsilon_{k-1}} X_{i_k}^{\epsilon_k} X_{i_{k+1}1}^{\epsilon_{k+1}} = UVU^{-1}$, donc D_{k-1} et D_k sont segments finaux de $U = (U^{-1})^{-1}$, contredisant[22] que $V = D_{k-1}^{-1} D_k$ est réduit. ∎

Ainsi, posant $D = D_{k-1}^{-1}$, $E = D_k$, on a[23] $V = DE$ et $U_- D^{-1} = U = E^{-1} U_+$.

Quitte à prendre l'inverse $(UVU)^{-1} = U^{-1} V^{-1} U^{-1}$ du mot UVU et à renommer $(U, V, D, E) := (U^{-1}, V^{-1}, E^{-1}, D^{-1})$, on supposera $l(D) \leq l(E)$.

---

17 avec les notations ci-dessus avec $k = 1$.

18 c'est ici que $x \in End(F_2)$, plutôt que $End(F)$ (F un groupe libre de type fini), est crucial!

19 avec les conventions $D_{-1} = \emptyset = D_{n+1}$.

20 par l'hypothèse faite sur x_0 (celle de i) ou iv) du théorème).

21 puisque D_{k-1}^{-1} est segment initial du V central.

22 puisque $D_{k-1} \neq \emptyset \neq D_k$.

23 avec les notations $U = X_{i_{k-1}}^{\epsilon_{k-1}}$, $V = X_{i_k}^{\epsilon_k}$ de l'Affirmation 1 car, par l'Affirmation 2, $i_{k-1} \neq i_k$.

Fin de la démonstration du LEMME:

Si $l(U_+)<l(E)$ (donc $l(\widetilde{VU})<l(V)$), suivant le cas I ou II, $\varphi_U^{-1}x\alpha^{-1}$ ou $\varphi_U^{-1}x\beta$ contredit encore que x minimise la taille dans la double classe Hx_0H. $\square$

Ainsi $l(U_+)\geq l(E)\geq l(D)$ et il y a un mot, éventuellement vide, F tel que U_+ a l'expression réduite $U_+=FD^{-1}$ et donc $U=E^{-1}FD^{-1}$, ainsi :

$$\varphi_D^{-1}(V)=(DE)^D=ED \text{ et } \varphi_D^{-1}(U)=(E^{-1}FD^{-1})^D=D^{-1}E^{-1}F$$

donc $\varphi_D^{-1}(\widetilde{VU})=\varphi_D^{-1}(V)\varphi_D(U)=F$ et $l(\varphi_D^{-1}(V))=l(V),\ l(\varphi_D^{-1}(\widetilde{VU}))<l(U)$.

Donc, suivant le cas I ou II, que x minimise la taille dans Hx_0H est encore contredit par l'endomorphisme surjectif $\varphi_D^{-1}x\beta$ ou $\varphi_D^{-1}x\alpha^{-1}$.

Aucun subsistant C_k ne pouvant ainsi être vide, le Lemme est établi. $\square$ ∎

APPENDICE C
Forme normale dans B_3 et classes de conjugaison de torsion.

On utilise les notations du §**1** : $B_3=\langle a,b\,;\,aba=bab\rangle$ groupe des tresses à trois brins, d'après la Proposition de l'appendice B, identifié à $\Psi(B_3)\subset Aut^+(F_2)$.

Ainsi $s=aba=bab$: $(u,v)\mapsto(v,u^{-1})^u$, $c=s^2=ababab$, $(u,v)\mapsto(u^{-1},v^{-1})^{vu}$ et $d=c^2$, $(u,v)\mapsto(u,v)^{[v,u]}$ qui engendrent respectivement le centre $Z=\langle c\rangle$ de B_3 et son sous-groupe d'indice 2, $Y=\langle d\rangle\subset\langle c\rangle=Z$.
On note $A,B,S,C\in SL(2,\mathbb{Z})$ leurs images par $\varrho:=\rho^+\circ\Psi : Aut^+(F_2)\to SL(2,\mathbb{Z})$.

PROPOSITION. — *Soit une tresse à trois brins $w\in B_3$. Alors il y a : $n\in\mathbb{Z}$, $\nu_1,\nu_2\in\{0,1\}$ et $W(a^{-1},b)$, un mot du monoïde engendré par a^{-1} et b, t.q. :*

$$w=s^{\nu_1}W(a^{-1},b)s^{\nu_2}c^n$$

De plus, si $w\notin\langle s\rangle$, cette écriture est uniquement[1] *déterminée par w.*

Démonstration. — Il y a $\frac{1}{2}2^4$ choix de signes[2] pour les coefficients de $M=\varrho(w)$, ainsi il y a $\nu\in\{0,1\}^3$ avec $M_\nu=S^{-\nu_1}\varrho(w)S^{-\nu_2}C^{-\nu_0}$ à coefficients positifs ou nuls.

Par une classique[3] suite de soustraction de lignes[4], on ramène M à $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ et donc $\varrho(w)$ est le produit $W(A^{-1},B)$ en sens inverse des matrices inverses A^{-1},B.

---

[1] si $w=s^m\in Z$ il n'y a pas unicité : $c^n=s^{2n}=s1sc^{n-1}$ (resp. $s1c^n=s^{2n+1}=1sc^n$).

[2] comme $det(\varrho(x))=1>0$ la moitié des choix $\pm$ pour chacun des quatre coefficients.

[3] soit $M=\begin{pmatrix}e&f\\g&h\end{pmatrix}$, $\|M\|=e+f+g+h$. Si $e=g$ et $f>h$ (resp. $f<h$) on note $M_1=AM$ (resp. $B^{-1}M$). Si $e>g$ (resp. $e<g$) alors $f\geq h$ (resp. $f\leq h$) et on pose $M_1=AM$ (resp. $B^{-1}M$). Dans tous les cas M_1 est à coefficients positifs ou nuls avec $\|M_1\|<\|M\|$(sinon $e\geq g+1, h\geq f+1$ et $det(M)\geq(g+1)(f+1)-fg=g+f+1>1$, sauf si $M=Id\ldots$)

[4] multiplication à gauche par A ou B^{-1}, la note précédente implique l'unicité du processus.

D'après $(\mathfrak{A})$ l'élément $w' = s^{\nu_1} W(a^{-1}, b) s^{\nu_2} c^{\nu_0}$ vérifiant $\varrho(w) = \varrho(w')$ diffère de w par une puissance paire de c : $w = w' c^{2m} = s^{\nu_1} W(a^{-1}, b) s^{\nu_2} c^{\nu_0 + 2m}$. ∎

Définition. La *taille normale* de $w \in B_3$ est l'ordre lexicographique de la paire

$$t_n(w) = (2\nu_1 + \nu_2,\, l(W)) \ .$$

COROLLAIRE. — *Un élément w_0 de taille normale minimale dans la classe de conjugaison w^{B_3} de l'élément $w \in B_3$ est de taille soit :*

i) $t_n(w_0) = (0,0)$, et $w_0 = c^n$ *est central.*

ii) $t_n(w_0) = (0,m)$, $m \neq 0$ et $w_0 = W c^n$, $W \neq 1$ cycliquement réduit.

iii) $t_n(w_0) = (1,0)$ *et* $w_0 = s c^n = s^{2n+1}$.

iv) $t_n(w_0) = (1,1)$, et soit $w_0 = a^{-1} s^{2n+1}$, soit $w_0 = b s^{2n+1}$.

COMPLÉMENT. — *L'image de w_0 dans $B_3/Y = SL(2,\mathbb{Z})$ est :*

Dans le cas i), $\overline{w_0} = \overline{c}^n$ *d'ordre* 2 *si n est impair, trivial si n est pair.*

Dans le cas ii), $\overline{w_0} = \overline{W} \overline{c}^n$ *d'ordre infini.*

Dans le cas iii), $\overline{w_0} = \overline{s}^{2n+1}$ *d'ordre* 4 *et conjugué à l'un de* $\overline{s}, \overline{s}^{-1}$.

Dans le cas iv) d'ordre 6 *ou* 3 *et conjugué à l'un de* $\overline{b}\overline{a}, (\overline{b}\overline{a})^{-1}$ ou $(\overline{b}\overline{a})^2, (\overline{b}\overline{a})^{-2}$.

Dans les cas iii) et iv) les choix sont deux à deux non conjugués[5].

Démonstration. — Si $t_n(w) = (k,m) \geq (2,1)$ alors $w = sWc^n$, ou $sWsc^n$ et le conjugué $w^s = Wsc^n$ ou $w^s = Wc^{n+1}$ est de taille normale $(k-1,m)$ ou $(k-3,m)$.

Si $w = Wsc^n$ a une écriture de taille $(1,m)$, $m > 1$ alors W a l'une des formes :

$$W = a^{-1} W' a^{-1},\ a^{-1} W' b,\ b W' a^{-1},\ b W' b$$

avec $l(W') = l(W) - 2 < l(W)$ et dans les quatre cas les conjugués :

$$w^{a^{-1}} = a a^{-1} W' a^{-1} abac^n a^{-1} = W' bc^n,\ \ w^{a^{-1}} = a a^{-1} W' babac^n a^{-1} = W' sc^n$$
$$w^b = b^{-1} b W' a^{-1} abac^n b = W' sc^n,\ \ w^b = b^{-1} b W' babac^n b = W' a^{-1} c^{n+1}$$

ont une écriture de taille normale inférieure :

$$(0, m-1),\ (1, m-2),\ (1, m-2),\ (0, m-1) \ .$$

Dans le cas *iv)* si n est pair : $a^{-1} s^{2n+1} \equiv a^{-1} s = a^{-1} aba = ba \mod Y$, $bs^{2n+1} \equiv bs = baba = (ba)^2 \mod Y$ et si n est impair $a^{-1} s^{2n+1} \equiv a^{-1} s^3 = a^{-1} abababa ba = babababa = (ba)^4 \mathrm{mod}\ K$, $bs^{2n+1} \equiv bs^3 = bababababa = (ba)^5 \mod K$. ∎

[5] car $S, S^{-1}, BA = M, M^{-1}, M^2, M^{-2}$ sont distinctes dans l'abélianisé de $B_3/Y = SL(2,\mathbb{Z})$.

FORMULES DANS $Aut^+(F_2) = Int(F_2) \rtimes_\psi B_3$). — *i)* $\sigma\varphi_x = \varphi_{\sigma(x)}\sigma$

ii) $(\varphi_x\sigma)(\varphi_y\tau) = \varphi_{x\sigma(y)}\sigma\tau$

iii) $(\varphi_x\sigma)^{\varphi_y\tau} = \varphi_{\tau^{-1}(y^{-1}x\sigma(y))}\sigma^\tau$.

Démonstration. — *ii)* suit de *i)* et *iii)* suit de *ii)* et *i)* :

$$\varphi_x\sigma\varphi_y\tau = \varphi_x\varphi_{\sigma(y)}\sigma\tau = \varphi_{x\sigma(y)}\sigma\tau$$

$$(\varphi_y\tau)^{-1}\varphi_x\sigma\varphi_y\tau = \tau^{-1}\varphi_{y^{-1}}\varphi_{x\sigma(y)}\sigma\tau = \tau^{-1}\varphi_{y^{-1}x\sigma(y)}\sigma\tau = \varphi_{\tau^{-1}(y^{-1}x\sigma(y))}\tau^{-1}\sigma\tau$$

Quant à *i)*, pour tout $t \in F_2$ on a :

$$\sigma\varphi_x(t) = \sigma(xtx^{-1}) = \sigma(x)\sigma(t)\sigma(x)^{-1} = \varphi_{\sigma(x)}(\sigma(t)) = (\varphi_{\sigma(x)}\sigma)(t) \ .$$

∎

REMARQUE. — *Les éléments suivants σ, ι, ζ de $Aut^+(F_2)$:*

$$\sigma = \varphi_{vu}s^2 : (u,v) \mapsto (u^{-1}, v^{-1})$$

$$\iota = \varphi_u s : (u,v) \mapsto (v, u^{-1}), \ (\iota^2 = \sigma)$$

$$\zeta := \varphi_u\beta s : (u,v) \mapsto (v, v^{-1}u^{-1}), \quad \zeta^{-1}(u,v) = (v^{-1}u^{-1}, u)$$

sont d'ordre fini, respectivement $2, 4$ *et* 3 *et d'images dans* $SL(2,\mathbb{Z})$ *:*

$$\rho(\sigma) = -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \rho(\iota) = S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \rho(\zeta) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \rho(\zeta^{-1}) = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

De plus $\zeta^\sigma = \varphi_v\zeta$ *et* $\sigma^{\zeta^{-1}} = \varphi_{v^{-1}}\sigma$.

Démonstration. — D'après la Proposition de l'Appendice B on a les relations : $s^2(u,v) = (u^{-1}, v^{-1})^{vu}$; $s(u,v) = (v, u^{-1})^u$, d'où les cas de σ et ι et :
$\zeta(u,v) = \varphi_u\beta((v,u^{-1})^u) = \varphi_u(v^{vu}, (u^{-1}v^{-1})^{vu}) = (v^v, (u^{-1}v^{-1})^v) = (v, v^{-1}u^{-1})$,
expression en u et v de la permutation cyclique des générateurs de la présentation symétrique $F_2 = \langle u, v, w \mid uvw \rangle$ d'où l'ordre de ζ et l'expression de ζ^{-1}. □

$$\zeta^\sigma(u,v) = \sigma^{-1}\zeta\sigma(u,v) = \sigma\zeta(u^{-1}, v^{-1}) = \sigma(v^{-1}, uv) = (v, u^{-1}v^{-1}) = \varphi_v\zeta(u,v)$$

$$\sigma^{\zeta^{-1}}(u,v) = \zeta\sigma\zeta^{-1}(u,v) = \zeta\sigma(v^{-1}u^{-1}, u) = \zeta(vu, u^{-1}) = (v^{-1}u^{-1}v, v^{-1}) = \varphi_{v^{-1}}\sigma(v) \ .$$

∎

COCOROLLAIRE. — *i) Les éléments de torsion de* $SL(2,\mathbb{Z})$ *sont d'ordre* $6, 4, 3, 2$, *une classe de conjugaison pour ceux d'ordre* 2, *deux pour les autres :*

$$M = BA = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} S, S^{-1}, M^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, M^{-2} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, -I \ .$$

ii) Tout relevé dans $Aut^+(F_2)$, avec même ordre, d'un élément d'ordre 2, 4 *ou* 3 *de $SL(2,\mathbb{Z})$ est respectivement conjugué à σ, ι ou ι^{-1}, ζ ou ζ^{-1}.*

Il n'y a pas d'élément d'ordre 6 *dans $Aut^+(F_2)$.*

Démonstration. — *i)* est une paraphrase du COMPLÉMENT. □

ii) Si $\gamma \in Aut^+(F_2)$ est d'ordre k et $\gamma' \in Aut^+(F_2)$ est tel que $\rho(\gamma') = \rho(\gamma)$ alors, d'après Nielsen *iii)* il y a $x \in F_2$ tel que $\gamma' = \varphi_x\gamma$.

D'après la FORMULE *ii)*, γ' est d'ordre k si et seulement si :

$$x \in X_\gamma := \{x \in F_2 \,|\, x\gamma(x)\cdots\gamma^{k-2}(x)\gamma^{k-1}(x) = 1\}$$

et, d'après la FORMULE *iii)* et Nielsen *iii)*, l'élément $\varphi_y\tau$ conjugue $\gamma'' = \varphi_{x'}\gamma$ à γ' si et seulement si : $\gamma^\tau = \varphi_z\gamma$ pour un $z \in F_2$ et $\tau^{-1}(y^{-1}x'\gamma(y))z = x$.

Si $\tau=1$ on a $z=1$ et x est dans l'orbite de x' pour l'action à droite :

$$\cdot_\gamma : X_\gamma \times F_2 \to X_\gamma,\ x \cdot_\gamma w = w^{-1}x\gamma(w)\ .$$

D'après *i)* et Nielsen *iii)*, les éléments d'ordre 2, 3, 4 de $Aut^+(F_2)$ sont conjugés à l'un de : $\varphi_{x_\sigma}\sigma$, $(\varphi_{x_\zeta}\zeta)^{\pm 1}$, $(\varphi_{x_\iota}\iota)^{\pm 1}$ avec des $x_\gamma \in X_\gamma$, $\gamma = \sigma, \zeta, \iota$.

Soit $x_\gamma \in X_\gamma$ de longueur $l(x_\gamma) = \min\{l(w \cdot_\gamma x_\iota \,|\, w \in F_2\} = l$ minimale dans l'orbite de x_γ pour l'action de $\cdot_\gamma$ avec $\gamma=\sigma,\zeta,\ \iota$.

Démonstration des cas d'ordre non divisible par 3 *dans ii).* — Si $l = 0$, $\varphi_{x_\gamma}\gamma$ est, suivant le cas, σ ou $\iota^{\pm 1}$. □

Sinon, γ envoyant les générateurs sur des éléments de longueur 1, $\gamma(x_\gamma)$, en mot réduit, s'obtient en remplaçant dans x_γ chaque lettre par son image par γ.

Le mot $x_\gamma\gamma(x_\gamma)\cdots\gamma^{k-1}(x_\gamma) = 1$ n'étant pas réduit, soit x_γ est de longueur $l(x_\gamma) \geq 2$ avec a, z pour première et dernière lettre vérifiant $\gamma(a) = z^{-1}$, donc $l(x_\gamma \cdot_\gamma a) = l(x_\gamma) - 2$, contredisant la minimalité de $l(x_\gamma)$ dans l'orbite de x_γ. □

Donc $l(x_\gamma) = 1$, $x_\gamma = a$ et $\gamma(a) = a^{-1}$, impossible si $\gamma = \iota$, et si $\gamma = \sigma$, comme ι agit transitivement sur $\{u^{\pm 1}, v^{\pm 1}\}$ les quatre cas $x_\sigma = \varphi_t\sigma$, $t \in \{u^{\pm 1}, v^{\pm 1}\}$ sont conjugués entre eux par les puissances de ι : $(\varphi_t\sigma)^{\iota^k} = \varphi_{\iota^{-k}(t)}\sigma$, $k = 1, 2, 3, 4$ et, comme[6] $\sigma^{\zeta^{-1}} = \varphi_{v^{-1}}\sigma$, l'élément $\varphi_{x_\sigma}\sigma$ est aussi conjugué à σ. □ ▮

Démonstration du cas d'ordre 3 *dans ii).* —

Par confort notationnel on identifie les générateurs de la présentation symétrique de $F_2 = \langle u, v, w \,|\, uvw\rangle$ à $\overline{1}, \overline{2}, \overline{3} \in \mathbb{Z}/3\mathbb{Z}$, ainsi :

$$F_2 = \langle \mathbb{Z}/3\mathbb{Z} \,|\, (i-1)i(i+1)\rangle,\ \zeta : F_2 \to F_2, \zeta(i) = i + 1\ .$$

Comme pour tout générateur $i \in \mathbb{Z}/3\mathbb{Z}$, on a : $i^{-1} = (i+1)(i-1)$, tout élément de $w \in F_2$ a une écriture $w = i_1 \cdots i_n$ en uniquement les générateurs (et pas leurs

[6] par la dernière relation de la **Remarque**.

inverses) $\overline{1},\overline{2},\overline{3}\in\mathbb{Z}/3\mathbb{Z}$, écriture unique si elle est *réduite*, c.à.d. ne contient, pour un $i\in\mathbb{Z}/3\mathbb{Z}$, le sous-mot $(i-1)i(i+1)$, on note alors $l^+(w)=n$, sa *longueur*.

Soit $x=i_1\cdots i_n\in X_\zeta$ avec $l^+(x)$ minimale dans l'orbite de x pour l'action $\cdot_\zeta$

Affirmation. — $n=l^+(x)\leq 1$

Démonstration. — On a $x\zeta(x)\zeta^2(x)=1$ donc, soit $l^+(x)\leq 1$, soit il y a réduction entre[7] x et $\zeta(x)$. Comme $(i_1i_2)(i_1+1)(i_2+1)$ ne se réduit pas, on a $l(x)=n>2$.

Comme $\zeta(x)=(i_1+1)\cdots(i_n+1)$, $i_n=i_1$ et soit $i_2=i_1+1$, soit $i_{n-1}=i_1-1$.

Dans le premier cas[8] $x\cdot_\zeta(i_n-1)^{-1}=i_1(i_1+1)i_3\cdots i_{n-1}i_1\cdot_\zeta(i_1-1)^{-1}=(i_1-1)i_1(i_1+1)i_3\cdots i_{n-1}=i_3\cdots i_{n-1}$, contredisant $l^+(x)$ minimal dans l'orbite.

Dans le second $x\cdot_\zeta i_1=i_1i_2\cdots i_{n-2}(i_1-1)i_1\cdot_\zeta i_1=i_2\cdots i_{n-2}(i_1-1)i_1(i_1+1)=i_2\cdots i_{n-2}$, contredisant encore $l^+(x)$ minimal dans l'orbite de x. ∎

Ainsi soit $x=1$ et $\zeta'=\zeta$, soit $\zeta'=\varphi_{\bar{i}}\zeta$, cependant[9] $\zeta^\sigma=\varphi_{\bar{1}}\zeta$ et, pour $k=1,2,3$, $(\varphi_{\bar{i}}\zeta)^{\zeta^{-k}}=\varphi_{\zeta^k(\bar{i})}\zeta=\varphi_{\overline{i+k}}\zeta$ et ζ' est encore conjugué à ζ. ∎ ∎

Démonstration de la non existence d'élément d'ordre 6 dans ii). — Soit ω un élément d'ordre 6 de $Aut^+(F_2)$. Les éléments d'ordre 3 de $Aut^+(F_2)$ étant conjugués à ζ ou ζ^{-1} et, dans $SL(2,\mathbb{Z})$, ceux d'ordre 6 à M ou M^{-1}, on suppose ω d'abélianisé M et de carré $\omega^2=\zeta=\varphi_u\beta s$, le cas M^{-1} suit par passage à l'inverse.

Ainsi $\omega=\varphi_x\beta\alpha$ et :

$$\omega^2=\varphi_x\beta\alpha\varphi_x\beta\alpha=\varphi_x\varphi_{\beta\alpha(x)}\beta\alpha\beta\alpha=\varphi_{x\beta\alpha(x)}\beta s=\varphi_{x\beta\alpha(x)}\varphi_{u^{-1}}\zeta=\varphi_{x\beta\alpha(x)u^{-1}}\zeta\ .$$

Mais $N=I+M=\begin{pmatrix}2&-1\\1&1\end{pmatrix}$ ne peut avoir $\overline{u}=e_1=\begin{pmatrix}1\\0\end{pmatrix}$ dans son image[10], à plus forte raison, dans le groupe libre $F_2=\langle u,v\rangle$, l'équation : $x\beta\alpha(x)u^{-1}=1$, dont $(I+M)(X)-U=0$ est l'équation induite dans l'abélianisé $\mathbb{Z}^2$, n'a pas de solution, donc il n'y a pas d'hypothétique ω d'ordre 6 dans $Aut^+(F_2)$. ∎ ∎ ∎

[7] l'image par ζ^{-1} d'une réduction entre $\zeta(x)$ et $\zeta^2(x)$ est une réduction entre x et $\zeta(x)$.

[8] Si $n=3,4,5$, $i_3\cdots i_{n-1}$(resp. $i_2\cdots i_{n-2}$) sont $\emptyset, i_3, i_3i_{n-1}=i_3i_4$ (resp. $\emptyset, i_2, i_2i_{n-2}=i_2i_3$).

[9] d'après la **Remarque.**

[10] l'unique préimage par N de e_1 dans $\mathbf{Q}^2$ est $\frac{1}{3}e_1-\frac{1}{3}e_2\notin\mathbf{Z}^2$.

APPENDICE D

Le groupe des tresses diédrales à trois brins DB_3 et $Aut(F_2)$.

Le goupe à deux éléments $\Delta = \{1, d\}$ agit sur le groupe des tresses à trois brins B_3 par $a^d = b^{-1}, b^d = a^{-1}$.

Définition. Le groupe des *tresses diédrales à trois brins* DB_3 est l'extension triviale de Δ par B_3 muni de l'action précédente. :

$$1 \to B_3 \to DB_3 = B_3 \rtimes \Delta \to \Delta \to 1 \ ,$$

il a donc la présentation :

$$DB_3 = \langle a, b, d \,|\, d^2, aba(bab)^{-1}, bdad \rangle \ .$$

Proposition. — *L'endomorphisme $\delta : F_2 \to F_2$ défini par $\delta(u,v) = (v,u)$ est un isomorphisme d'ordre 2 vérifiant les relations*

$$\alpha^\delta = \beta^{-1}, \quad \beta^\delta = \alpha^{-1} \ ,$$

il permet donc d'étendre le morphisme :

$$\Psi : B_3 \to Aut^+(F_2), \ \Psi(a) = \alpha, \ \Psi(b) = \beta$$

de l'appendice B en un morphisme injectif :

$$\Phi : DB_3 \to Aut(F_2), \ \Phi(a) = \Psi(a) = \alpha, \ \Phi(b) = \Psi(b) = \beta, \ \Phi(d) = \delta \ .$$

Démonstration. — Comme $\delta^2 = 1$, il suffit d'établir $\alpha^\delta = \beta^{-1}$:
$\alpha^\delta(u,v) = \delta^{-1}\alpha\delta(u,v) = \delta\alpha(v,u) = \delta(u^{-1}v,u) = (v^{-1}u,v) = \beta^{-1}(u,v)$. ∎

Il sera alors aisé à la lectrice d'établir, pour $Aut(F_2)$, la version originelle :

Théorème$'$ (de Nielsen, 1917). — *i) Un endomorphisme surjectif du groupe libre à deux générateurs F_2 est un automorphisme.*

ii) Le groupe des automorphismes de F_2 est produit semi-direct amalgamé :

$$Aut(F_2) = Int(F_2) \rtimes_{<\varphi_{[u,v]} = \Phi(s^4)>} \Phi(DB_3) \ .$$

iii) Le groupe $Int(F_2)$ des automorphismes intérieurs de F_2 est le noyau de :

$$\rho : Aut(F_2) \to Aut(\mathbb{Z}^2) = GL(2, \mathbb{Z}) \ .$$

iv) Un endomorphisme φ du groupe libre à deux générateurs F_2 défini par $\varphi(t_i) = X_i, i = 1, 2$ est un automorphisme de F_2 si et seulement si il préserve à conjugaison et inverse près le commutateur des générateurs :

$$(C'w) \qquad [X_1, X_2] = X_1^{-1}X_2^{-1}X_1X_2 = ([t_1,t_2]^{\pm 1})^w = w^{-1}[t_1,t_2]^{\pm 1}w \ .$$

De plus, il est dans $\Phi(DB_3)$ ssi $[X_1,X_2] = [t_1,t_2]^{\pm 1}$, c. à d. on a $(C'1)$

et la détermination à conjugaison près des torsions de $GL(2,\mathbb{Z})$ et $Aut(F_2)$:

coCorollaire. — *i) Les éléments de torsion de $GL(2,\mathbb{Z})$ sont d'ordre $2, 3, 4$ ou 6, trois classes de conjugaison pour ceux d'ordre 2, une seule pour les autres :*

$$-I, D=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, SD=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \ M^2=\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \ S \text{ ou } M=\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \ .$$

ii) Tout relevé dans $Aut^+(F_2)$, avec même ordre, d'un élément d'ordre $2, 3, 4$ de $GL(2,\mathbb{Z})$ est respectivement conjugué à σ, δ, $\iota\delta$, ζ ou ι.

Il n'y a pas d'élément d'ordre 6 dans $Aut(F_2)$. ▮ ▮ ▮

APPENDICE E

Un exercice de théorie des groupes : produits semi-directs amalgamés.

On rapelle que, si K, L sont des groupes et $\psi : L \to Aut(K)$ est un morphisme de groupes, le produit semi-direct de K par L suivant ψ est $K \rtimes_\psi L$, le produit $K \times L$ muni de la loi :

$$(k,l)\cdot(k',l') = (k\psi(l)(k'), ll') \ .$$

Il contient $K\times\{1\}, \{1\}\times L \subset K\rtimes_\psi L$ comme sous-groupes qu'abusivement, on note encore $K = K\times\{1\}, L = \{1\}\times L < K\rtimes_\psi L$ avec $K\cap L = \{1\}$, le premier K étant normal et la restriction $\pi_{|L} : L \subset K\rtimes_\psi L \to K\rtimes_\psi L/K$ à L du morphisme quotient est un isomorphisme.

De plus $(k,l)^{-1} = (\psi(l^{-1})(k^{-1}), l^{-1})$ et, si $l \in L, \psi(l) : K = K\times\{1\} \to K\times\{1\} = K$ est la restriction à $K\times\{1\}$ de la conjugaison par l dans $K\rtimes_\psi L, (k,1) \mapsto (1,l)(k,1)(1,l)^{-1} = \psi(l)(k)$.

Le but de cet appendice est une version sans l'hypothèse $K\cap L = \{1\}$ de la classique :

Proposition. — Soit $K < G$ un sous-groupe d'un groupe G et $L < N(K)$ un sous-groupe du normalisateur de K avec $K\cap L = \{1\}$.

On note $\psi : L \to Aut(K), \psi(l)(k) = lkl^{-1}$.

Alors $K\rtimes_\psi L$ est, par $(k,l) \mapsto kl$, isomorphe au sous-groupe $KL \subset G$.

Soit K, L, M trois groupes, $\psi : L \to Aut(K), \kappa : M \to K, \lambda : M \to L$ trois morphismes de groupes avec κ, λ injectifs, $\lambda(M) \triangleleft L$ normal dans L et ψ respectant l'image $\kappa(M)$, c.à.d. induisant $\psi_M : L \to Aut(\kappa(M))$, et tant ψ_M que $\psi\circ\lambda$ sont intérieurs au sens fort suivant[1] :

$$\psi_M(l)(\kappa(m)) = \kappa\circ\lambda^{-1}(l\lambda(m)l^{-1}), \ \ \psi(\lambda(m))(k) = \kappa(m)k\kappa(m)^{-1} \ .$$

[1] notant abusivement $\lambda^{-1} : \lambda(M) \to M$ l'inverse de la bijection $\lambda' : M \to \lambda(M), m \mapsto \lambda(m)$.

On note $\mu : M \to K \rtimes_\psi L, \mu(m) = (\kappa(m)^{-1}, \lambda(m))$.

Identifiant, au moyen de κ et λ, le groupe M à un *sous-groupe commun* à K *et* L, ainsi que K, L aux sous-groupes $K \times \{1\}, \{1\} \times L$ de $K \rtimes_\psi L$, on a :

$$\mu : M \to K \rtimes_\psi L,\ \mu(m) = (m^{-1}, m)\ ,$$

$$\psi_M(l)(m) = lml^{-1} =: {}^l m, \quad \psi(m)(k) = mkm^{-1} =: {}^m k\ ,$$

$$(k,l) = kl, \quad (k,l)(k',l') = (k({}^l k'), ll'), \quad (k,l)^{-1} = (l^{-1}k^{-1}l, l^{-1}) =: ((k^{-1})^l, l^{-1})\ .$$

LEMME. — *μ est un morphisme d'image $\mu(M) \triangleleft K \rtimes_\psi L$, un sous-groupe normal.*

Définition. Le groupe quotient $K \rtimes_\psi L/\mu(M)$, noté $K \rtimes_{\psi,\eta=\kappa} L$ (ou[2] $K \rtimes_{\psi,M} L$), est le *produit semi-direct suivant ψ de K et L amalgamé par $\eta = \kappa$ (ou sur M).*

COROLLAIRE. — *Soit $K < G$ un sous-groupe d'un groupe G et $L < N(K)$ un sous-groupe du normalisateur de K. Alors, si $\psi : L \to Aut(K), \psi(l)(k) = lkl^{-1}$ est la restriction à $L < G$ de la conjugaison dans G, l'application :*

$$p : K \rtimes_\psi L \to KL < G,\ (k,l) \mapsto kl$$

est un morphisme de noyau $M = K \cap L$ et induit un isomorphisme :

$$\overline{p} : K \rtimes_{\psi,M} L \to KL\ .$$

Démonstration. — $p(k,l)p(k',l') = klk'l' = klk'l^{-1}ll' = p((k,l)(k',l'))$, et p est morphisme. □
$1 = p(k,l) = kl$ ssi $K \ni k = l^{-1} \in L$, donc $l \in K \cap L = M$, c.a.d. $(k,l) = (m^{-1}, m) \in \mu(L)$. □ ∎

Démonstration du Lemme. — $\mu(m)\mu(m') = (m^{-1}, m)(m'^{-1}, m') = (m^{-1}({}^m m'^{-1}), mm') = (m'^{-1}m^{-1}, mm') = ((mm')^{-1}, mm') = \mu(mm')$ donc μ est un morphisme de groupes. □

$${}^{kl}\mu(m) = kl(m^{-1}, m)(kl)^{-1} = (k({}^l m^{-1}), lm)l^{-1}k^{-1} = (k({}^l m^{-1}), lm)(l^{-1}k^{-1}ll^{-1}) =$$

$$= (k({}^l m^{-1})({}^{lm}((k^{-1})^l)), lml^{-1}) = (klm^{-1}l^{-1}lml^{-1}k^{-1}lm^{-1}l^{-1}, {}^l m) =$$

$$({}^l m^{-1}, {}^l m) = \mu({}^l m) \in \mu(M)\ .$$

et le sous-groupe $\mu(M)$ est normal dans $K \rtimes_\psi L$. □ ∎

[2] comme ci-dessus, identifiant M à $\kappa(M), \cdots$

Les seuls calculs $ABA = BAB$, $f_{n+1}f_{n-1} = f_n$ et $\pi_0(A) = a, \pi_0(B) = b$ plutôt que ceux et les récurrences à base d'algorithme d'Euclide du traitement classique (p. 9-19 de [**Ra**]) profitent de ce que la suffisance des relations est donnée par la présentation du groupe des classes d'isotopie de difféomorphismes de la sphère plate $(\mathbb{S}, \{m, n, p, \infty\}, \{\infty\}) = (\mathbb{T}/\{\pm I\}, \mathbb{T}_2, \{0\})$ respectant points d'ordre 2 et 1, présentation déduite de celle du groupe des tresses à trois brins d'Artin ([**A**]).

Près d'un quart de siècle plus tard[1], Artin concédait que (dans son article de 1925) "*Most of the proofs are entirely intuitive*", renvoyant pour les relations de B_n au quasiment simultané[2]traitement algébrique de F. Bohnenblust via l'action de B_n sur le groupe libre F_n (le groupe fondamental du plan privé de n points).

Depuis, l'établissement de ces relations[3] a fait couler beaucoup d'encre.

Un traitement clair et rigoureux est donné par l'école d'Orsay via la méthode des espaces fonctionnels[4] et les théorèmes de fibration de Cerf ([**Ce**]).[5]

Dans son introduction à la K-théorie algébrique ([**Mi**]) Milnor prouve[6] que le noyau du morphisme canonique $\phi\colon St(2,\mathbb{Z}) \to SL(2,\mathbb{Z})$ du groupe de Steinberg[7] sur le groupe spécial linéaire en dimension 2 est un groupe cyclique infini.

Exprimant la présentation de $St(2,\mathbb{Z})$ au moyen de $\alpha = x_{1,2}^{-1}, \beta = x_{2,1}$, il reconnaît $St(2,\mathbb{Z}) \simeq B_3$, le noyau de ϕ étant le sous-groupe d'indice 2 du centre de ce groupe, non de tresses, mais groupe fondamental du complémentaire du nœud de trèfle[8] et, rappelant l'argument de Quillen pour construire un difféomorphisme de $M = SL(2,\mathbb{R})/SL(2,\mathbb{Z})$ sur le complémentaire du nœud de trèfle[9], obtient que le groupe fondamental de M est $St(2,\mathbb{Z}) \simeq B_3 = \widetilde{SL}(2,\mathbb{Z})$, préimage de

---

[1] *Theory of Braids* Ann. of Math. 48 (1947), p. 101-126.

[2] *The algebraic braid group.* Ann. Math. 48 (1947), p. 127-136.

[3] tant celles du groupe des tresses que le passage au groupe des classes d'isotopies d'homéomorphismes ou difféomorphismes respectant une partie finie de la sphère.

[4] L'espace des plongements de n points dans le plan est stratifié avec une seule strate ouverte qui est contractile, les générateurs du groupe fondamental correspondant aux traversées des strates de codimension 1 et les relations aux contournements des strates de codimension 2.

[5] voir la rédaction de Valentin Poénaru, Exposé 2, p. 21-31 de [**FLP**].

[6] chaque étape est simple, une fois assimilé le début du §5 et beaucoup de §8, §9 et §10...!

[7] $St(2,\mathbf{Z}) =< x_{12}, x_{21} \mid x_{21}^{x_{12}^{-1}x_{21}x_{12}^{-1}} = x_{12}^{-1} >$ et $\phi(x_{12}) = e_{12} = A^{-1}, \phi(x_{21}) = e_{21} = B$.

[8] Artin ([**A**], p. 53), voir aussi [**FLP**] le corollaire p. 25 de l'exposé 2 de V. Poénaru.

[9] L'espace des réseaux de $\mathbf{R}^2 \simeq \mathbf{C}$ s'identifie d'une part à $GL(2,\mathbf{R})/GL(2,\mathbf{Z})$ et d'autre part, via l'équation $(W_\Lambda)\colon (\wp')^2 = 4(\wp)^3 - u\wp - v$ de la fonction de Weierstraß du réseau $\Lambda \subset \mathbf{C}$, $\wp(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$, $u = g_2 = 60\sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{\lambda^4}$, $v = g_3 = 140\sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{\lambda^6}$, au complémentaire dans $\mathbf{C}^2$ du discriminant $\{\Delta_\Lambda(u,v) = 27u^2 - v^3 = 0\}$. Ainsi l'espace des réseaux unimodulaires $SL(2,\mathbf{R})/SL(2,\mathbf{Z})$, puisque Δ_Λ est quasi homogène, s'identifie au complémentaire $\big(\mathbf{C}^2 \setminus \{\Delta_\Lambda = 0\}\big) \cap \{|u|^2 + |v|^2 = 1\}$ du nœud de trèfle dans la sphère unité de $\mathbf{C}^2$.

$SL(2,\mathbb{Z})$ dans le revêtement universel $\widetilde{SL}(2,\mathbb{R})$ du groupe spécial linéaire réel $SL(2,\mathbb{R})$, établissant à nouveau la présentation tressée d'Artin, mais avec la réserve *(which is of course classical)*. Sans doute pensait-il à un traitement comme dans l'Appendice A de la monographie de C. Kassel et V. Turaev ([**KT**]) inspiré de celui de Reidemeister ([**Re**]) de la présentation du groupe modulaire.

Voir B_3 comme préimage de $SL(2,\mathbb{Z})$ dans le revêtement universel de $SL(2,\mathbb{R})$ faisait partie du folklore (voir Serre dans son cours de 1968-69 ([**Se**], p. 20).

L'intérêt pour le théorème de Nielsen *iii*) a été ravivé depuis les années 50 puis 80-90 par l'intervention du tore modulaire en arithmétique, topologie des surfaces et décompte des géodésiques simples sur les surfaces hyperboliques[10].

S'ils attribuent le résultat à Nielsen et son article ([**N**] de 1917), tant Magnus, Karass et Solitar ([**MKS**], p. 169) que Lyndon et Shupp ([**LS**], p. 25), montrent[11] $ker(Aut(F_2)\to GL(2,\mathbb{Z}))=Int(F_2)$ en utilisant la présentation de $Aut(F_n)$ publiée par Nielsen[12] sept ans après.

Le court (13 pages) article originel de Nielsen ([**N**]) n'est pas de lecture aisée :

Nielsen signale que Dehn lui a communiqué *iv*) avec une preuve différente[13].

Si l'analogue de *iii*) et *iv*) est clairement dégagé en fin de I et début de II, ce n'est que page 9 après une intrication de démonstrations et énoncés intermédiaires.

---

[10] Voir [**Co**], l'article synthèse [**H**] de Haas et la note [**McR**].

[11] Via référence à Chang ([**Ch**] pour Lyndon et Shupp, qui proposent aussi une démonstration fautive : si $Int(F_2) =: I < K := \ker(\rho)$, utilisant la présentation classique de $GL(2,\mathbf{Z})$ avec un générateur d'ordre 2, un d'ordre 4 et un d'ordre 6 ($C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et, avec nos notations, $S,(AB)$) laissent le lecteur vérifier que les relèvements $(v,u),(v^{-1},u),(v^{-1},uv)$ dans $Aut(F_2)$ de $C,S,(AB)$ vérifient modulo I les relations. Même en corrigeant (v^{-1},uv) en $(v,u^{-1}v)$, cela montre que l'extension $1\to K/I\to Aut(F_2)/I\to GL(2,\mathbf{Z})\to 1$ a une section, mais pas que $K/I=\{1\}$.

[12] *Die Isomorphismengruppe der freien Gruppen* Math. Ann. **91** (1924), p. 169-209, (traduction en anglais par J. Stillwell [**N-12**]).

[13] sans référence par Nielsen, imaginons : la conservation à conjugaison près du commutateur des générateurs par l'endomorphisme φ permet d'étendre en une application de degré 1 du tore $f : \mathbf{R}^2/\mathbf{Z}^2 =: R \to R$ sur lui-même une application $h : B \to B$ du bouquet $B = \mu \cup \lambda := \mathbf{R}{\times}\{0\}/\mathbf{Z}{\times}\{0\}\cup\{0\}{\times}\mathbf{R}/\{0\}{\times}\mathbf{Z}$ sur lui-même, identité près de $m=\overline{(\frac{1}{2},\frac{1}{2})}$ et induisant sur le groupe fondamental de B l'endomorphisme φ. On déforme $f : (R, R\backslash\{m\},\{m\}) \to (R, R\backslash\{m\},\{m\})$ en une appliction lisse transverse à B et simplifie $f^{-1}(\mu)$, puis $f^{-1}(\lambda)$ (pour $f^{-1}(\mu)$: on élimine les composantes inessentielles puis, celles qui restent (il y en a car f est de degré 1) sont, s'il y en a plus d'une, des courbes parallèles, chaque paire de composantes voisines étant séparée par deux anneaux A_1, A_2. Alors la restriction de f à A_1, celui qui ne contient pas m, est d'image disjointe de m donc de degré nul et f se déforme, près de A_1, en une application envoyant A_1 hors de $\mu\ldots$). Ainsi f se déforme en g lisse transverse à B avec $g^{-1}(\mu)$ et $g^{-1}(\lambda)$ connexes, donc $g_| : g^{-1}(B)\to B$ est un revêtement connexe, de degré $deg(g_|) = deg(g) = deg(f) = 1$, ainsi $g_|$ est un homéomorphisme, donc l'endomorphisme φ qu'il induit sur le groupe fondamental de $\pi_1(R\backslash\{m\})$ est un isomorphisme. ∎

Le point $i)$ est plutôt supposé que démontré[14] au tout début de I.

N'ayant dégagé le sous-groupe $H \subset Aut^+(F_2)$, pour l'analogue de $i)$ et $iii)$, Nielsen procède en deux temps : d'abord de I 1. à I 6. il réduit jusqu'à 1, par automorphisme intérieur et changement de «paires images» $(S(t_1), S(t_2))$ décrits dans le complément de l'AFFIRMATION 1 de l'Appendice B, la longueur des images, par l'endomorphisme surjectif S, des générateurs, puis de I 7. à I 10., examinant pas à pas le passage inverse et, utilisant la dernière partie de sa thèse[15], il établit que dans chacun des mots $S(t_i)$, $i=1,2$ les exposants de chaque générateur ont même signe et que ces mots ont une forme uniquement déterminée par l'abélianisé de S.

Cette dernière partie a été oubliée[16]et a provoqué une grande activité pour déterminer la forme explicite des mots $S(t_i)$, avec McShane et Rivin, citons [**OZ**].

A la fin[17]de [**A**] Artin transforme sa présentation $B_3 = < a, b \,|\, aba = bab >$ en $< t, s \,|\, t^3 = s^2 >$ $(t = ba, s = bab)$ et, renvoyant à Dehn [**D**] et Schreier [**Sc**], il met tout élément $w \in B_3$ sous la forme normale $w = t^{\epsilon_0} s t_1^{\epsilon_1} \cdots s t^{\epsilon_{n-1}} s^{\epsilon_n} c^k$ avec :

$$n \in \mathbb{N}, k \in \mathbb{Z}, \epsilon_j \in \{-1, 1\} \text{ pour } 0 < j < n,\ \epsilon_0 \in \{-1, 0, 1\},\ \epsilon_n \in \{0, 1\}\ .$$

Comme $ts = babab = ca^{-1}, t^{-1}s = (ba)^{-1}bab = b$, quitte à modifier le traitement des termes extérieurs : $w = s^{\nu_1} t^{\epsilon_1} s \cdots t^{\epsilon_{n-1}} s s^{\nu_2} c^k, \nu_1, \nu_2 \in \{0, 1\}$, c'est celle de l'Appendice C, obtenue par méthode de Gauß sur les matrices 2×2 à cœfficients entiers naturels que l'on trouve à la fin de la thèse de Nielsen [**N-1**].

La détermination de la torsion de $Aut(F_2)$ est due à Meskin [**Me**]. Il laisse cependant à la lectrice une grande initiative dans la distinction entre mot réduit de l'image par un endomorphisme d'un mot réduit et image de ce mot réduit et lui demande des vérifications de “non cancellation” problématiques[18].

---

[14] à moins de savoir dès 1917 qu'un sous-groupe d'un groupe libre est libre (attribué à Schreier (1927) ou Nielsen (1921) en Danois, traduction en anglais par A.W. et W.D.Neumann [**N-8**]), on ne peut affirmer avec Nielsen que si les générateurs a, b de F_2 s'expriment en fonction de mots α, β alors l'endomorphisme envoyant a, b sur α, β est un isomorphisme (pour avoir l'inverse, il faudrait savoir que α et β n'aient pas de relation entre eux).

[15] Kurvennetze au Flächen Diss. Kiel 1913, p. 47-49 (accessible depuis 1986 : [**N-1**]).

[16] ou jugée, sans accès (avant 1986) à la thèse de Nielsen, incomplète.

[17] §9, p. 70 avec $\sigma_1, \sigma_2, a = \sigma_1\sigma_2, b = \sigma_1\sigma_2\sigma_1$ pour nos $a, b, ab =: t, s$ mais, comme nous $c = s^2$!

[18] par exemple p. 497 *If* W *ends in* B*, that is,* $W = UB$*, then* $W^S = U^S A^{-1} B^{-1}$ *and* $W^{S^2} = U^{S^2} A$ *and the* A' *do not cancel* or, sans avoir prouvé préalablement que W ne peut commencer et finir par B, si $U = BU'$ commence aussi par B, d'après la relation $B^S = A^{-1}B^{-1}$, donnée plus haut, il y a une simplification de A dans l'expression :

$$(SW)^3 = W^{S^2} W^S W (= (U^{S^2} A)(A^{-1} B^{-1} U'^S) W)$$

Références

[A] Artin E. — *Theorie der Zőpfe*, Hamb. Abh. **4**, p. 47-72, 1925.

[Ce] Cerf J. — *Topologie de certains espaces de plongements*, Bull. Soc. Math. France **89**, p. 227-280 (Thèse Sc. math. Paris 1960), 1961.

[Ch] Chang B. — *The automorphism group of the free group with two generators*, Michigan Math. J. 7, p. 79-81, 1960.

[Co] Cohn H. — *Approach to Markoff's minimal forms through modular functions*, dans Annals of Mathematics **61**, p. 1-12, 1955.

[D] Dehn M. — *Die beide Kleeblattschlingen*, Math. Ann. **75**, p. 402-413, 1914.

[FLP] Fathi A., Laudenbach F., Poénaru V. — *Travaux de Thurston sur les surfaces. Séminaire Orsay* Astérisque 66-67, 1979.

[KT] Kassel C., Turaev V. — *Braid groups*, Appendice A, Graduate texts in Mathematics **247**, p. 311-314. 2008.

[LS] Lyndon R.C., Shupp P. — *Introduction to algebraic K-theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete **89**, Springer , 1977.

[MKS] Magnus W., Karras A., Solitar D. — *Combinatorial group theory*, Interscience publishers, 1966.

[McR] McShane G., Rivin I. — *A norm on homology of surfaces and counting simple geodesics*, Int. Math. Res. Notices. 1995 n°2, p. 61-69, 1995.

[Me] Meskin S. — *Periodic automorphisms of the two generator free group*, in Proc. Conf. Cambera 1973 L.N.M. **372**, Springer, p. 494-498, 1974.

[Mi] Milnor J. — *Introduction to algebraic K-theory*, Annals of mathematical studies **72**, P.U.P., p. 494-498 , 1971.

[N] Nielsen J. — *Die Isomorphismen der allgemeinen unendlichen Gruppe mit zwei Erzeugenden*, Math. Ann. **78**, p. 385-397, 1917.

[N-i] Nielsen J., Hansen V.L.(ed.). — **i**ième article de *Jakob Nielsen: Collected papers Volume 1 (1913-1932)*, Birkhấuser, 1986.

[OZ] Osborne R.P., Zieschang H.. — *Primitives in the free group on two generators*, Invent. Math. **63**, p. 17-24, 1981.

[Ra] Rankin R. — *Modular forms and functions*, C.U.P.,, 1977.

[Re] Reidemeister K. — *Einfűhrung in die kombinatorische Topologie* Vieweg, 2 §8 et 9, p. 42-46, 1932.

[Sc] Schreier O. — *Űber die Gruppen* $A^aB^b = 1$, Hamb. Abh. **3**, p. 167, 1925.

[Se] Serre J.-P. — *arbres, amalgames,* SL_2, Astérisque **46** , 1977.

Quatrième de couverture de la plaquette, scénario de :

$SL(2,\mathbb{Z})$, les tresses à trois brins, le tore modulaire et $Aut^+(F_2)$

The main subject of this booklet, which is written in french, is to propose an "Artin presentation" of $SL(2,\mathbb{Z})$. This presentation is obtained via the action of the two-dimensional integer special linear group on the flat sphere with three permuted conic points and a fourth fixed conic point.

This sphere is the quotient of the integer two-dimensional torus by minus one involution. Artin's presentation of B_3, braid group on three strings seen as modular group of the sphere with 3+1 marked points, gives the searched presentation.

This Artin's presentation allows an easy description of the derived group and its action on Poincaré half plane whose quotient is the modular torus.

It appears that a formulation, using Artin's braid group B_3, of Nielsen's theorem for direct automorphisms of the free group F_2 gives even more quickly this, known but not very popularized, Artin presentation of $SL(2,\mathbb{Z})$.

However the proof of this formulation of Nielsen's theorem, which seems not being explicited in the litterature, needs Artin presentation. This is the task of the second appendix (an appendix, not the core of the paper, only a flash-back).

Other appendices treat other subjects related to Nielsen's theorem such as determining torsion elements of $SL(2,\mathbb{Z})$ and the automorphism group of the free group of rank 2, a corresponding formulation of Nielsen's theorem for the full automorphism group and the treatment of semi-direct product of groups with amalgation used in the formulation of Nielsen's theorem.

During the shooting of this short movie, the "director and script", not only cited, but read old and new litterature and thought that his effort can help, avoiding some traps, a reader to enjoy such "past and present safari".

Metteur en scène et secrétaire : Alexis Marin Bozonat
courriel : alexis.charles.marin@gmail.com

Univ. Grenoble Alpes, CNRS, IF, 38100, Grenoble, France