Université Sorbonne Paris Nord

Le théorème de Nielsen-Schreier, deux approches différentes

Lydia BAKIRI

Projet dirigé par Geoffroy HOREL et William TROIANI

29 août 2023

Table des matières

0 Introduction

L'objectif de ce rapport est de se familiariser avec les concepts nécessaires qui nous permettront de comprendre un théorème particulier, celui de Nielsen-Schreier :

≪ Tout sous-groupe d'un groupe libre est libre. ≫

Ces quelques mots mettent en avant une première particularité qui m'a donné envie d'en apprendre plus à ce sujet : ce théorème est très compréhensible, et paraît plus ou moins trivial. Mais il n'en est rien : afin de démontrer ce résultat, un bagage mathématique conséquent est requis. Cela a donc éveillé ma curiosité et m'a donné la volonté et la motivation d'en savoir plus sur ce domaine.

Une autre spécificité est qu'il existe différentes preuves de ce théorème, en fonction du domaine mathématique dans laquelle on veut se situer. Cela montre l'importance et la richesse de ce théorème. Il est utilisé dans la théorie des groupes, la topologie algébrique et en combinatoire. Ce dernier domaine a d'ailleurs été la source historique de sa découverte. En effet, Jakob Nielsen prouva en 1921 dans son article *Mathematisk Tidsskrift* que tout sous-groupe d'un groupe libre à un nombre fini de générateurs est libre, en introduisant notamment des transformations, dites de Nielsen, ainsi que des résultats combinatoires. Ces transformations sont utilisées dans des problèmes d'informatique théorique, comme le problème d'isomorphisme pour ne citer que lui. Otto Schreier généralisa par la suite ce résultat pour les sous-groupes à générateur infini en 1926.

Les liens entre ce théorème et la topologie algébrique furent découverts plus tard par Max Dehn, puis par Reinhold Baer and Friedrich Levi qui ont publié cette nouvelle preuve. Cette dernière est plus souvent étudiée que les autres de nos jours.

Maintenant que nous nous sommes familiarisés avec l'histoire du théorème, attaquons-nous à son contenu. Ce rapport traitera en grande partie de sa preuve dans la topologie algébrique. En effet, ce domaine est vaste, intéressant, et nous permettra de découvrir des résultats importants, comme le théorème de Van Kampen (4.2.1), ou encore le groupe fondamental du cercle qui est isomorphe à $\mathbb{Z}$ (2.2). Après avoir traité cette partie, nous allons en établir un lien avec les combinatoires, de sa découverte à ses applications.

1 Rappels

1.1 Espaces topologiques à connaître

Afin de comprendre au mieux les notions de l'algèbre topologique, nous devons nous familiariser avec certains espaces topologiques que nous allons utiliser durant tout le long de ce rapport.

Définition 1.1.1. Soit X un ensemble. Une **topologie** sur X est une famille $\mathcal{T}$ de parties de X, appelés espaces ouverts, tels que :

— $\emptyset, X \in \mathcal{T}$;

— Une intersection finie d'éléments de $\mathcal{T}$ appartient à $\mathcal{T}$;

— Une réunion quelconque d'éléments de $\mathcal{T}$ appartient à $\mathcal{T}$.

Une partie F de X est dite **fermée** si son complémentaire F^c est ouvert (i.e appartient à $\mathcal{T}$).
On appelle la paire $(X, \mathcal{T})$ un **espace topologique**. Si le contexte rend le contenu de $\mathcal{T}$ clair, nous pouvons simplement noter X.

Définition 1.1.2. Soit $(X, \mathcal{T})$ un espace topologique, et $Y \subset X$. On définit $L := \{W \cap Y | W \in \mathcal{T}\}$. L est appelé **topologie induite** sur Y.

Lemme 1.1.3. *L est une topologie sur Y.*

Définition 1.1.4. Soit $(X, \mathcal{T})$ un espace topologique, Y un ensemble quelconque, et $\pi : X \longrightarrow X/Y$ une application. On définit $\mathcal{T}_Y := \{U \subset X/Y | \pi^{-1}(U) \in \mathcal{T}\}$. $\mathcal{T}_Y$ est la **topologie quotient** de X/Y.

Lemme 1.1.5. *$\mathcal{T}_Y$ est une topologie sur X/Y.*

Définition 1.1.6. Soit $(X_i, \mathcal{T}_i)$ des espaces topologiques. On définit $\mathcal{T} := \{\bigsqcup_{i \in I} U_i | U_i \in \mathcal{T}_i\}$. $\mathcal{T}$ est la **topologie de la réunion disjointe** des (X_i).

Lemme 1.1.7. *$\mathcal{T}$ est une topologie sur $\{\bigsqcup_{i \in I} X_i\}$.*

Définition 1.1.8. Soit X un espace topologique.

— X est dit **connexe** si les seuls ouverts-fermés de X sont $\emptyset$ et X.

— Une **base de voisinage** d'un point x est une famille de parties V de X tels que tout voisinage de x contienne un élément de V.

— X est dit **localement connexe** si tout point x de X admet une base de voisinage connexe.

— X est dit **simplement connexe** si tout lacet de X est homotope à un point de X.

— X est dit **semi-localement simplement connexe** si tout point admet un voisinage U où tout lacet, contenu dans U, peut être déformée en un point dans X.

Les notions de lacet et d'homotopie seront vues par la suite.

Remarque 1.1.9. Un espace localement simplement connexe est semi-localement simplement connexe.

1.2 Définitions essentielles en topologie algébrique

Définition 1.2.1. Une **n-cellule** e^n est un ensemble appartenant au n-disque fermé D^n.

Définition 1.2.2. On appelle **CW-complexe** un espace X construit à partir des étapes suivantes :

1. On commence avec X^0, un ensemble discret composé de 0-cellules (un ensemble de points par exemple).
2. Par récurrence, on construit X^n, le **n-squelette** à partir de X^{n-1}. Pour ce faire, on considère e^n_α les n-cellules que nous utiliserons. Attachons chaque e^n_α à X^{n-1} par l'application $\phi_\alpha : S^{n-1} \to X^{n-1}$, où S^{n-1} est la sphère unité dans $\mathbb{R}$. X^n est donc l'espace quotient de $X^{n-1} \cup_\alpha D^n_\alpha$ par l'identification $x \sim \phi_\alpha(x)$, avec $x \in \partial D^n_\alpha$. Ainsi, e^n_α est l'image homéomorphique de $D^n_\alpha - \partial D^n_\alpha$ sous l'application quotient.
3. L'espace X est enfin l'union des espaces X^n construits comme expliqué ci-dessus. Cette union peut être finie ou infinie. Dans le second cas, on donne à X la topologie faible : Un ensemble $A \subset X$ est ouvert (resp. fermé) si et seulement si $A \cap X^n$ est ouvert (resp. fermé) dans X^n, pour tout n.

Exemples

— Un graphe est un CW complexe de dimension 1 : c'est un ensemble de sommets (0-cellules) recollé par des 1-cellules.

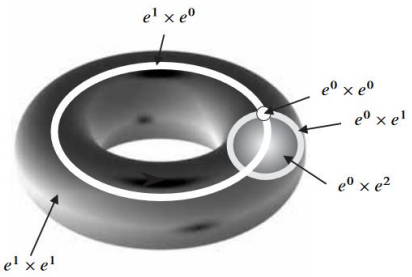
— Un polyèdre peut être vue comme un CW-complexe de dimension 2.

En raison de la structure inductive des CW-complexes, ces espaces sont particulièrement maniables car ils permettent des preuves qui influent sur la structure du n-squelette. Cet exemple de déconstruction d'un espace en ses éléments constitutifs s'inscrit dans une classe plus large d'opérations combinant des espaces pour en créer de nouveaux. Voici certaines d'entre elles.

Définition 1.2.3. Soient X et Y, deux CW-complexes, de cellules respectives e^n_α et e^n_β. Le **produit** de X et Y, noté $X \times Y$, est lui même un CW-complexe, où chaque cellule est construite à partir du produit des cellules e^n_α et e^m_β.

Exemple :

FIGURE 1 – [2, Torus]



Définition 1.2.4. Soit X un CW-complexe et A un sous-complexe de X (i.e une union de cellules de X). Le **quotient** X/A est un CW-complexe composé des cellules de $X - A$, ainsi qu'une 0-cellule représentant les cellules de A, ou l'image de A dans X/A.
Si e^n_α est une cellule de $X - A$ attaché dans X par l'application $\phi_\alpha : S^{n-1} \longrightarrow X^{n-1}$, alors elle est attaché dans X/A par la composition $S^{n-1} \longrightarrow X^{n-1} \longrightarrow X^{n-1}/A^{n-1}$.

Définition 1.2.5. Soient X et Y deux espaces topologiques, et $x_0 \in X, y_0 \in Y$. Le **bouquet** $X \vee Y$ est le quotient de l'union disjointe $X \sqcup Y$ en identifiant x_0 et y_0 en un seul point.

Remarque 1.2.6. Le bouquet d'une famille d'espaces topologiques pointés est le co-produit de cette famille dans la catégorie des espaces topologiques pointés.

Définition 1.2.7. Soient X et Y deux espaces topologiques, et $x_0 \in X, y_0 \in Y$. Le **smash-produit** $X \wedge Y$ est le quotient $X \times Y/X \vee Y$.

Définition 1.2.8. Soient X, Y, deux espaces topologiques.
Une **homotopie** est une famille d'applications $f_t : X \to Y,\ t \in I$, telle que l'application associée $F : X \times I \to Y, (x,t) \to f_t(x)$ est continue. On dit que $f_0, f_1 : X \to Y$ sont **homotopes** s'il existe une homotopie f_t les connectant, c'est à dire s'il existe une application $F : X \times I \to Y, (x,t) \to f_t(x)$ telle que $F(x,0) = f_0(x)$ et $F(0,t) = f_1(t)$. On note dans ce cas $f_0 \simeq f_1$.

Un cas particulier d'homotopie est la rétraction par déformation :

Définition 1.2.9. Soit X un espace topologique, et $A \subset X$. Une **rétraction par déformation** de X sur A est un ensemble d'applications $f_t : X \to X, t \in I$, tel que $f_0 = \mathrm{id}_X, f_1(X) = A, f_t|A = \mathrm{id}_A$, pour tout t. De plus, l'application associée $X \times I \to X, (x,t) \to f_t(x)$ doit être continue.

2 Groupe Fondamental

2.1 Définition

Afin de comprendre la notion de groupe fondamental, nous nous devons de définir certaines notions au préalable.

Définition 2.1.1. Un **chemin** dans un espace topologique X est une application continue $f : I \to X$, où I est l'intervalle $[0, 1]$.
Lorsque $f(0) = x_0 = f(1)$, ce chemin est appelé **lacet**. Le point x_0 est le **point de base** de ce lacet.

Définition 2.1.2. Une **homotopie de chemin** dans X est une famille de chemins $f_t : I \to X, 0 \leq t \leq 1$, tel que :
(1) Les extrémités $f_t(0) = x_0$ et $f_t(1) = x_1$ sont indépendants de t, c'est à dire que $f_t(0) = x_0$ et $f_t(1) = x_1$ pour tout $0 \leq t \leq 1$
(2) L'application

$$F : I \times I \longrightarrow X \tag{1}$$
$$(s, t) \longmapsto f_t(s) \tag{2}$$

est continue.

Lorsque deux chemins f_0 et f_1 sont connectés par une homotopie f_t, on dit qu'ils sont **homotopes**. On note $f_0 \simeq f_1$.

Proposition 2.1.3. *La relation d'homotopie de chemins, avec les extrémités fixées dans n'importe quel espace est une relation d'équivalence.*
La classe d'équivalence d'un chemin f sous la relation d'équivalence d'homotopie est notée [f]. Elle est appelée ***classe d'homotopie*** *de f.*

Définition 2.1.4. Soit $f : I \longrightarrow X$ un chemin. On note $\bar{f}$ le chemin défini par :

$$\bar{f} : I \longrightarrow X \tag{3}$$
$$s \mapsto f(1 - s) \tag{4}$$

Définition 2.1.5. Soient $f, g : I \longrightarrow X$ deux chemins vérifiant $f(1) = g(0)$. Leur composition est le chemin noté $f \cdot g$, et est défini par :

$$f \cdot g(s) = \begin{cases} f(2s), & 0 \leq s \leq 1/2 \\ g(2s - 1), & 1/2 \leq s \leq 1 \end{cases} \tag{5}$$

Définition 2.1.6. Le groupe fondamental de X en x_0, noté $\pi_1(X, x_0)$, est l'ensemble de toutes les classes d'homotopie $[f]$ de lacets $f : I \to X$ de point de base x_0 avec le produit défini par $[f][g] = [f \cdot g]$, $g : I \to X$ un lacet de $\pi_1(X, x_0)$.

Proposition 2.1.7. *Soit X un espace topologique, x_0, x_1, deux points appartenant à une même composante connexe par arcs de X et $h : I \longrightarrow X$ un chemin de x_0 à x_1. Alors l'application $\beta_h : \pi_1(X, x_1) \to \pi_1(X, x_0), f \longmapsto h \cdot f \cdot \bar{h}$ est un isomorphisme. Cette application β_h est appelée* ***changement de point de base.***

Preuve. Soient $f, g \in \pi_1(X, 1)$.
• $\beta_h[f \cdot g] = [h \cdot f \cdot g \cdot \bar{h}] = [h \cdot f \cdot \bar{h} \cdot h \cdot g \cdot \bar{h}] = \beta_h[f]\beta_h[g]$. β_h est donc bien un homorphisme.
•$\beta_h\beta_{\bar{h}}[f] = \beta_h[\bar{h} \cdot f \cdot h] = [h \cdot \bar{h} \cdot f \cdot h \cdot \bar{h}] = [f]$ et similairement, $\beta_{\bar{h}}\beta_h[f] = [f]$.
Ainsi, β_h est un isomorphisme d'inverse $\beta_{\bar{h}}$. □

Ainsi, nous pouvons omettre dans certains cas le point de base de ce groupe $\pi_1(X, x_0)$ qui est, à un isomorphisme près, indépendant du choix du point de base x_0. Gardons cependant en tête que cet isomorphisme dépend du choix du chemin h.

2.2 Le groupe fondamental Du cercle

Le premier groupe fondamental sur lequel nous allons travailler est celui de la sphère unitaire $S^1, \pi_1(S^1)$. Ce groupe donne un théorème important que nous allons étudier dans cette section.

Théorème 2.2.1. *Le groupe $\pi_1(S^1)$ est un groupe cyclique infini généré par la classe d'homotopie du lacet $\omega : s \mapsto (\cos 2\pi s, \sin 2\pi s)$ de base (1,0). Autrement dit, $\pi_1(S^1)$ est isomorphe à $\mathbb{Z}$.*

Remarque 2.2.2. Notons $\omega_n(s) = (\cos 2\pi ns, \sin 2\pi ns), n$. On a $[\omega]^n = [\omega_n]$. Prouver le théorème précédent revient donc à prouver que tout lacet dans S^1 de base $(1, 0)$ est homotope à ω_n pour un unique $n \in \mathbb{Z}$.
On peut comparer les chemins de S^1 avec des chemins de $\mathbb{R}$ grâce à l'application $p : \mathbb{R} \to S^1, s \mapsto (\cos 2\pi s, \sin 2\pi s)$.
Observons que le lacet $\omega_n = p\tilde{\omega}_n$, où $\tilde{\omega}_n : I \longrightarrow \mathbb{R}$ est le chemin $\tilde{\omega}_n(s) = ns$. On dit dans ce cas que $\tilde{\omega}$ est un **relèvement** de ω_n.

Quelques résultats nous seront utiles pour démontrer ce théorème :

Soit X un espace topologique.

Lemme 2.2.3. *Pour tout chemin $f : I \to X$ commençant à $x_0 \in X$, et pour tout $\tilde{x}_0 \in p^{-1}(x_0)$, il existe un unique relèvement $\tilde{f} : I \to \tilde{X}$ commençant à $\tilde{x}_0$.*

Lemme 2.2.4. *Pour tout homotopie de chemin $f_t : I \to X$ commençant à x_0 et pour tout $\tilde{x}_0 \in p^{-1}(x_0)$, il existe une unique homotopie relevée de chemins $\tilde{f}_t : I \to \tilde{X}$ commençant à $\tilde{x}_0$.*

Preuve du théorème. :
Soit $f : I \to S^1$ un lacet de point de base $x_0 = (1, 0)$, tel que f représente un élément de $\pi_1(S^1, x_0)$.

Montrons tout d'abord que $[f] = [\omega_n]$. Tout d'abord, par le Lemme 2.2.3, il existe un relèvement $\tilde{f}$ commençant à 0, et finissant à $n \in \mathbb{Z}$. En effet, $p\tilde{f}(1) = f(1) = x_0$ et $p^{-1}(x_0) = \mathbb{Z} \subset \mathbb{R}$. Il existe un autre chemin de 0 à $n : \omega_n$. Soit $H : I \to \mathbb{R}, t \mapsto (1-t)\tilde{f} + t\tilde{\omega_n}$. Cette application est continue, et on a $H(0) = \tilde{f}$ et $H(1) = \tilde{\omega_n}$. $\tilde{f}$ et $\tilde{\omega_n}$ sont donc homotope, d'homotopie H, et par composition, f et ω_n le sont aussi, d'homotopie pH.

Prouvons désormais que n est déterminé de manière unique par $[f]$. Supposons $f \simeq \omega_n$ et $f \simeq \omega_m$. Par conséquent, $\omega_n \simeq \omega_m$.
Soit f_t une homotopie de $\omega_m = f_0$ à $\omega_n = f_1$. par Lemme 2.2.4, f_t se relève en une homotopie de chemin $\tilde{f}_t$, commençant à 0. De plus, par Lemme 2.2.3, $\tilde{f}_t$ est unique, et donc $\tilde{f}_0 = \tilde{\omega_m}$ et $\tilde{f}_1 = \tilde{\omega_n}$. Comme $\tilde{f}_t$ est une homotopie de chemin, son extrémité est indépendante de t. Or, $\tilde{f}_0(1) = \tilde{\omega_m}(1) = m$ et $\tilde{f}_1(1) = \tilde{\omega_n}(1) = n$, donc $m = n$.

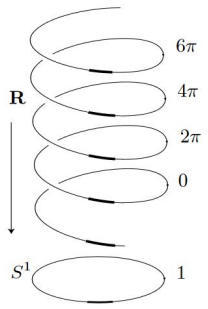
□

3 Revêtement d'un espace

3.1 Définition et exemple

Définition 3.1.1. Un **revêtement** d'un espace topologique X par un espace topologique $\tilde{X}$ est une application $p : \tilde{X} \to X$ telle que, pour tout point $x \in X$, il existe un voisinage ouvert $V \subset X$ de x tel que $p^{-1}(V)$ est une union disjointe d'ouverts, chacune homéomorphe à V par p.

Exemple : L'exemple le plus classique serait celui de l'hélice, donnée lorsque nous parlions de $\pi_1(S^1)$. Dans ce cas, $X = S^1,\ \tilde{X} = \mathbb{R},\ p : s \mapsto (\cos 2\pi s, \sin 2\pi s)$.



3.2 Relèvement des homotopies

Définition 3.2.1. Soient X, Y deux espaces topologiques, $p : \tilde{X} \to X$, un revêtement de X, et $f : Y \to X$ une application. Un **relèvement** de f est une application $\tilde{f} : Y \to \tilde{X}$ tel que $p\tilde{f} = f$. On dit que $\tilde{f}$ relève f.

Proposition 3.2.2. *Soient X, Y deux espaces topologiques, $p : \tilde{X} \to X$ un revêtement de X, $f_t : Y \to X$ une homotopie et $\tilde{f}_0 : Y \to \tilde{X}$ un relèvement de f_0. Alors il existe une unique homotopie $\tilde{f}_t : Y \to \tilde{X}$ de $\tilde{f}_0$ qui relève f_t.*

Preuve. Voir [1, Chapitre 1, page 30] □

Lorsque $Y = I$, nous obtenons la propriété de relèvement des homotopies.
Lorsque $Y = \{0\}$, nous obtenons la propriété de relèvement des chemins.

Définition 3.2.3. Le lemme 2.2.3 définit **la propriété de relèvement des homotopies**.

Définition 3.2.4. Le lemme 2.2.4 définit **la propriété de relèvement des chemins**.

3.3 Correspondance entre revêtement et sous groupes de groupes fondamentaux

Proposition 3.3.1. *Soit $p : (\tilde{X}, \tilde{x}_0) \to (X, x_0)$ un revêtement. Alors l'application induite $p_* : \pi_1(\tilde{X}, \tilde{x}_0) \to \pi_1(X, x_0)$ est injective.*

Preuve. Voir [1, Chapitre 1, page 61] □

Proposition 3.3.2. *Soit X un espace topologique connexe par arc et semi-localement simplement connexe, et $x_0 \in X$. Alors pour tout sous-groupe H de $\pi_1(X, x_0)$, il existe un revêtement $p : X_H \to X$ et un point $\tilde{x}_0 \in X_H$ tel que $p_*(\pi_1(X_H, \tilde{x}_0)) = H$.*

Preuve. Voir [1, Chapitre 1, page 66] □

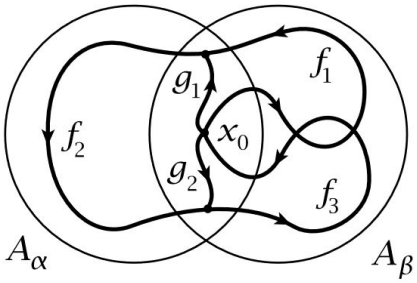
4 Théorème de Van-Kampen

Lorsque l'on travaille sur les groupes fondamentaux, Le théorème de Van-Kampen est incontournable. C'est un outil très utile dans le calcul de ces groupes. Dans le cadre de ce rapport, ce théorème nous permettra de nous rendre compte des liens entre les groupes fondamentaux et les graphes, ce qui nous donnera des résultats clés afin d'arriver à notre but.

4.1 Lacets d'un espace topologique dans des ouverts le recouvrant

Lemme Soit A_α,$\alpha \in J \subset \mathbb{N}$ une collection d'ensembles ouverts et connexes par arc d'un espace X, étant l'union de ces A_α. Si chaque intersection $A_\alpha \cap A_\beta$ est connexe par arc, alors tout lacet dans X de point de base x_0 est homotope à un produit de lacets, chacun contenu dans un seul A_α.

Preuve. Soit $f : I \longrightarrow X$ un lacet de point de base x_0, et une partition $0 = s_0 < s_1 < ... < s_m = 1$ telle que chaque intervalle $[s_{i-1}, s_i]$ appliqué à f appartient à un unique A_α. Nous pouvons la construire de la sorte :
Par la continuité de f, nous savons que tout $s \in I$ possède un voisinage ouvert V_s dans I tel que $f(V_s) = A_\alpha$. Par compacité de I, un nombre fini de ces intervalles recouvre I. Les extrémités de ces intervalles définissent la partition voulue. On notera par la suite A_i l'ensemble A_α auquel appartient $f([s_{i-1}, s_i])$, et f_i le chemin obtenu en restreignant f à $[s_{i-1}, s_i]$.
Nous savons que $A_i \cap A_{i+1}$ est connexe par arcs, nous pouvons donc choisir un chemin g_i de l'intersection précédente, partant de x_0 vers le point $f(s_i)$. Les chemins construits peuvent être schématisés de la sorte [2] :



Nous pouvons donc construire le lacet suivant :

$$(f_1 \cdot \bar{g}_1) \cdot (g_1 \cdot f_2 \cdot \bar{g}_2) \cdot (g_2 \cdot f_3 \cdot \bar{g}_3) \cdot ... \cdot (g_{m-1} \cdot f_m \cdot) \tag{6}$$

Ce lacet est homotope à f, dont chaque composante est un lacet appartenant à un unique A_i. □

4.2 Théorème de Van-Kampen

Théorème 4.2.1 (Théorème de Van Kampen)**.** *Soient A_α, un ensemble d'ouverts connexes par arcs d'un espace topologique $X = \bigcup_\alpha A_\alpha$. On suppose qu'il existe $x_0 \in X$ tel que pour tout $\alpha, x_0 \in A_\alpha$, et pour tout (α, β), $(A_\alpha \cap A_\beta)$ est connexe par arc. Alors :*
• *L'homomorphisme $\phi : *_\alpha \pi_1(A_\alpha) \to \pi_1(X)$ est surjectif.*
• *Supposons de plus que pour tout (α, β, γ), $(A_\alpha \cap A_\beta \cap A_\gamma)$ est connexe par arc. On note N le groupe normal généré par les éléments de la forme $\iota_{\alpha\beta}(\omega)\iota_{\beta\alpha}(\omega)^{-1}, \omega \in \pi_1(A_\alpha \cap A_\beta)$ (où $\iota_{\alpha\beta} : \pi_1(A_\alpha \cap A_\beta) \to \pi_1(A_\alpha)$ est l'homomorphisme induit par l'inclusion $(A_\alpha \cap A_\beta) \hookrightarrow A_\alpha$).*
Alors $\ker(\phi) = N$. *Autrement dit, ϕ induit un isomorphisme $\pi_1(X) \approx *_\alpha \pi_1(A_\alpha)/N$.*

Ebauche de preuve. La preuve du théorème de Van-Kampen est longue et complexe. C'est pourquoi nous allons en extraire un résumé qui mettra en exergue une explication intuitive de celle-ci.

Soient A_α et X, des ensembles vérifiant les hypothèses du théorème.

— Soient $L_\alpha : A_\alpha \longrightarrow X$, les applications d'inclusion de chaque A_α. ces applications induisent des applications $\pi_1(x_0, A_\alpha) \longrightarrow \pi_1(x_0, X)$. Par le lemme précédent, pour tout lacet dans X de point de base x_0, il existe un produit de lacets, chacun d'entre eux étant contenu dans un seul A_α, étant homotope à celui-ci. Autrement dit, l'homomorphisme $\phi : *_\alpha \pi_1(A_\alpha) \longrightarrow \pi_1(X)$ est surjectif.

— La deuxième partie de la preuve est bien plus complexe. Tout d'abord, soient les inclusions $\iota_{\alpha\beta} : A_\alpha \cap A_\beta \hookrightarrow A_\alpha$ (on a donc : $\iota_{\beta\alpha} : A_\alpha \cap A_\beta \hookrightarrow A_\beta$). Ces applications induisent :

$$\pi_1(\iota_{\alpha\beta}) : \pi_1(x_0, A_\alpha \cap A_\beta) \longrightarrow \pi_1(x_0, A_\alpha)$$
$$\pi_1(\iota_{\beta\alpha}) : \pi_1(x_0, A_\alpha \cap A_\beta) \longrightarrow \pi_1(x_0, A_\beta)$$

Soit $N = \{\iota_{\alpha\beta}(\omega)\iota_{\beta\alpha}(\omega)^{-1}, \omega \in \pi_1(x_0, A_\alpha \cap A_\beta)\}$. Notre but est de montrer que $N = \ker(\phi)$.
En reprennant les et notations du lemme (et de sa preuve), on introduit la notion de **factorisation** de $[f] \in \pi_1(X)$ comme étant le produit $[f_1][f_2]...[f_m]$, soit un mot dans $*_\alpha \pi_1(A_\alpha)$ dont l'image par ϕ est dans $[f]$. La première partie de la preuve nous a déjà montré que tout $[f] \in \pi_1(X)$ possède une factorisation. Le but de la seconde partie est de montrer qu'elle est unique. Deux factorisations de $[f]$ sont **équivalentes** si l'une peut se ramener à l'autre par les transformations suivantes (ou leurs inverses) :

- Si $[f_i]$ et $[f_{i+1}]$ appartiennent à un même $\pi_1(A_\alpha)$, alors on combine les termes adjacents $[f_1][f_{i+1}]$ en un seul terme $[f_i \cdot f_{i+1}]$;
- si $[f_i] \in \pi_1(A_\alpha)$ est un lacet dans $A_\alpha \cap A_\beta$, considérer $[f_i]$ comme étant dans le groupe $\pi_1(A_\beta)$.

Les deux transformations (et leurs inverses) ne changent pas l'image de ces éléments dans le groupe quotient $Q = *_\alpha \pi_1(A_\alpha)/N$: La première ne change pas l'élement, et N ne tient pas compte de la seconde transformation : Si $f_i \in A_\alpha \cap A_\beta$, alors qu'il appartienne à $\pi_1(A_\alpha)$ ou $\pi_1(A_\beta)$, son image par $\pi_1(\iota_{\alpha\beta})$ sera le même.
Ainsi, des factorisations équivalentes donnent le même élément dans Q. L'idée de la preuve est donc de montrer que toute factorisation de $[f]$ est équivalente, ce qui implique directement que l'application $Q \longrightarrow \pi_1(X)$ induise par ϕ est injective, et donc que N est le noyau de ϕ.

□

La preuve complète de ce théorème se trouve dans [1, Chapitre 1, page 44]

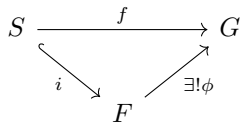
4.3 Exemple : Le bouquet

Soient X_α,$\alpha \in J \subset \mathbb{N}$ une collection d'espaces topologiques pointés et connexes par arc, et $x_\alpha \in X_\alpha$ leurs points de bases. Nous construisons le bouquet $\bigvee_\alpha X_\alpha$.
Si pour tout α, x_α est une rétraction par déformation d'un voisinage U_α simplement connexe dans A_α, alors X_α est une rétraction par déformation du voisinage $A_\alpha = X_\alpha \bigvee_{\beta\neq\alpha} U_\beta$. Donc $A_\alpha \cup A_\beta = (X_\alpha \bigvee_{\gamma\neq\alpha} U_\gamma) \cup (X_\alpha \bigvee_{\gamma\neq\beta} U_\gamma) = U_\alpha \vee U_\beta$. Ainsi, $A_\alpha \cup A_\beta$ se rétracte par déformation à un point. Ce résultat tient évidemment pour toute intersection de plus de deux A_α. On a donc $\bigcap_\alpha A_\alpha = \bigvee_\alpha U_\alpha$., dont le groupe fondamental est trivial : $A_\alpha \cap A_\beta$ est contractible, donc si $\omega \in \pi_1(x_0, A_\alpha \cap A_\beta)$, alors $\omega = e$, et donc $\iota_{\alpha\beta}(\omega)\iota_{\beta\alpha}(\omega)^{-1} = e$. Ainsi, le noyau de $\phi : *_\alpha \pi_1(A_\alpha) \to \pi_1(X)$ est trivial. Par le théorème de Van Kampen, ϕ est un isomorphisme.

5 Groupes Libres et Graphes

5.1 Définitions

Définition 5.1.1. Un groupe F est dit **libre** sur un ensemble S si $S \subset F$ et si pour tout groupe G et pour toute application $f : S \to G$, il existe un unique morphisme de groupe ϕ de F dans G prolongeant f. Nous avons donc le diagramme commutatif suivant :



Exemple : Le groupe libre le plus simple est tout simplement $(\mathbb{Z}, +)$, ayant pour base $S = \{1\}$. En effet, si f est une application de $\{1\}$ dans un groupe G, et i l'inclusion de $\{1\}$ dans (Z), nous pouvons définir $\phi(n) = f(1)^n,\ n \in \mathbb{Z}$. ϕ est bien un morphisme de groupe, et il est bien le seul vérifiant $\phi(1) = f(1)$.

Lemme 5.1.2. *Tout groupe isomorphe à un groupe libre est libre.*

Preuve. Soit G groupe isomorphe à un groupe libre F. Alors la propriété universelle de F donnée par la définition 5.1.1 est étendue par l'isomorphisme, et montre que G vérifie cette même propriété. Ainsi, G est libre. □

Définition 5.1.3. Un **graphe** est un CW-complex de dimension 1, c'est à dire un espace topologique G obtenu à partir d'un ensemble de sommets G^0 (0-cellules), en recollant une collection de 1-cellules e_α.
Nous pouvons donc voir les graphes comme l'union disjointe de G^0 et d'intervalles I_α, quotienté en identifiant les extrémités de chaque I_α à un élément de G^0

5.2 Liens entre groupes libres et graphes

Nous pouvons représenter les groupes libres comme des groupes fondamentaux de graphes. En effet :

Proposition 5.2.1. *Soit X un graphe connexe. Alors $\pi_1(X)$ est un groupe libre.*

Preuve. Soit T un arbre couvrant de X. L'application quotient $X \longrightarrow X/T$ est une équivalence d'homotopie. De plus, comme T contient tous les sommets de X, X/T est un graphe ne contenant qu'un sommet. plus précisément, X/T est un bouquet de cercles, prenant en compte les boucles du graphe X passant par les arêtes prises en comptes dans X/T. Par l'exemple d'application du théorème de Van Kampen, nous avons $*_\alpha \pi_1(X_\alpha) \approx \pi_1(\bigvee_\alpha X_\alpha)$, ce qui signifie que $\pi_1(X/T)$ est un groupe libre, ayant en tant que base les lacets données par les arêtes de X/T, qui sont les images des lacets de X par l'application quotient.

□

6 Le théorème de Nielsen-Schreier en Topologie Algébrique

6.1 Revêtement et graphe

Lemme 6.1.1. *Soit $\tilde{G}$ un revêtement d'un graphe G. Alors $\tilde{G}$ est lui aussi un graphe. De plus, les sommets et arêtes de $\tilde{G}$ sont des relèvements des sommets et arêtes (respectivement) de G.*

Preuve. Soit $p : \tilde{G} \to G$ un revêtement du graphe G. Nous allons prouver le lemme précédent en construisant les composantes du graphe $\tilde{G}$ à partir du graphe G.
L'ensemble discret des sommets se définit simplement par $= \tilde{G^0} = p^{-1}(G^0)$.
En effet, (G^0) est discret et chacun de ses points induit une union disjointe d'ouverts chacune homéomorphe à ce point. Ainsi, $\tilde{G^0}$ est bien discret
Quant aux arêtes, considérons l'ensemble des applications $f_\alpha : I_\alpha \to G$ compte tenu que G peut s'écrire, par définition, sous forme d'espace quotient de $X_0 \bigcup_\alpha I_\alpha$.
Par la propriété de relèvement des chemins, nous obtenons pour chaque f_α un unique relèvement $\tilde{f_\alpha}$, passant par chaque point de $p^{-1}(x), x \in e_\alpha$. Il nous reste à montrer que ces relèvements sont des 1-cellules. Ces relèvements définissent les arêtes de $\tilde{X}$. □

6.2 Le théorème de Nielsen-Schreier, une preuve topologique

Théorème 6.2.1 (Théorème de Nielsen-Schreier)**.** *Tout sous groupe d'un groupe libre est libre.*

Preuve. Soit F un groupe libre. Par le théorème de Van Kampen, on sait qu'il existe un graphe X tel que $\pi_1(X) \approx F$ (voir preuve proposition 5.2.1). Ce graphe X peut être par exemple un bouquet de p cercles, où p est l'ordre de F.
Soit maintenant G un sous-groupe de F. par la proposition 3.3.2, il existe un revêtement $p : \tilde{X} \to X$, avec $p_*(\pi_1(\tilde{X})) = G$. Or, d'après la proposition 3.3.1, p_* est injective, d'où $\pi_1(\tilde{X}) \approx G$.
D'après le lemme précédent, $\tilde{X}$ est un graphe, et par la proposition 5.2.1, nous savons que son groupe fondamental est aussi libre. Ainsi, le sous-groupe $G \approx \pi_1(\tilde{X})$ est libre.

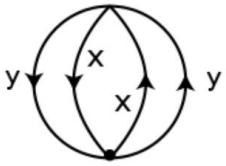
□

6.3 Exemple et application

Exemple

Soit F un groupe libre de base $\{x, y\}$, et G le sous groupe composé des mots de longueur pair. Le bouquet de 2 cercles X est un graphe dont le groupe fondamental est isomorphe à F.

En suivant la preuve, il existe un revêtement $\tilde{X}$ de ce graphe :



Nous savons aussi que $\pi_1(\tilde{X}) \approx G$. Notons aussi que le revêtement $\tilde{X}$ est homotope au bouquet de 3 cercles. Nous savons donc que la base de G est composé de 3 générateurs.

Un travail plus approfondi est nécessaire afin de relier les relèvements des chemins le long des applications de revêtements aux générateurs de groupes libres, mais cette information est implicite dans [1, chapitre 1, page 57]. En supposant que cela soit vrai, nous obtenons la présentation suivante du sous-groupe : H = $\{x^2, y^2, xy\}$.

Application

Soit F un groupe libre, et x, y des éléments de F commutant entre eux. On veut montrer l'existence un élément z de F tel que x et y sont tous deux des puissances de z.

D'après le théorème de Nielsen-Schreier, le sous-groupe $\langle x, y\rangle$ de F est libre. Il est aussi abélien, car x et y commutent entre eux. Cette commutativité exclut la possibilité que $\langle x, y\rangle$ soit de rang 2. Ce groupe est donc cyclique et on peut trouver un élément z tel que $\langle x, y\rangle = \langle z\rangle$. Autrement dit, x et y sont tous deux puissances de z.

7 Nielsen-Schreier en combinatoire

7.1 Notations

Définition 7.1.1. Soit G un groupe et $A \subset G$. On note $\langle A \rangle$ le sous-groupe de G généré par A, c'est à dire :

$$\langle A \rangle = \{a_{i_1}^{\pm 1}, a_{i_2}^{\pm 1}, ..., a_{i_n}^{\pm 1} | a_{i_1} \in etA, n \in \mathbb{N}\} \tag{7}$$

on dit aussi que A est une **base** pour $\langle A \rangle$

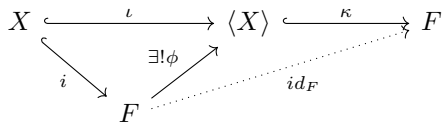
Définition 7.1.2. Soit X un ensemble. un mot w de X est une séquence finie d'éléments que l'on note $w = y_1, y_2, ..., y_n \in X$. Le nombre n est appelé **longueur** du mot w, et on le note $|w|$.
w est dit **réduit** s'il ne contient aucun sous-mot de la forme yy^{-1} pour tout $y \in X^{\pm 1}$.
Le mot vide ϵ a pour longueur $|\epsilon| = 0$ et est réduit.

A partir des ces définitions et notations, nous pouvons donner une autre définition d'un groupe libre, qui est évidemment équivalente à la définition donnée antérieurement.

Définition 7.1.3. Un groupe G est dit **libre** s'il existe un ensemble X générant G tel que tout mot réduit non vide de X définit un élément non trivial de G.

Lemme 7.1.4. *Si F est libre sur X, alors X génère F.*

Preuve. Soit $\langle X \rangle$ le groupe engendré par X. On note $\iota : X \hookrightarrow \langle X \rangle$ et $\kappa : F \hookrightarrow \langle X \rangle$ deux inclusions (par définition, $\langle X \rangle \subset F$). Par l'aspect libre de F, on a le diagramme commutatif suivant :



Par unicité, $\kappa \circ \phi = id_F$. Alors, $F = Im(id_F) = Im(\kappa \circ \phi) = Im(\phi) \subset \langle X \rangle$.
Ainsi, $\langle X \rangle = F$. □

Lemme 7.1.5. *L'application ϕ du lemme précédent est bijective.*

Preuve. ϕ est surjectif si pour tout $x \in \langle X \rangle$ il existe un ensemble $f \in F$ tel que $\phi(f) = x$.

Soit $x \in \langle X \rangle$. On sait que $\phi\kappa(x) = \mathrm{id}(x) = x$. Ainsi, nous pouvons prendre $f = \kappa(x)$, et on a bien $\phi(f) = x$. ϕ est donc bien surjectif.

Il nous reste maintenant à montrer que $\phi\kappa = \mathrm{id}_{\langle X \rangle}$. On sait que $\kappa\phi \mid_{\langle X \rangle} = \mathrm{id}_{\langle X \rangle}$. Ainsi, pour tout $x \in \langle X \rangle$, on a :

$$\kappa\phi \mid_{\langle X \rangle} (x) = x = \kappa(x) \tag{8}$$

κ est injectif, donc : $\phi \mid_{\langle X \rangle} = \mathrm{id}_{\langle X \rangle}$. Autrement dit, ϕ est injectif, et donc bijective. □

Définition 7.1.6. On note $F(X)$ le groupe libre de base X. La construction de ce groupe peut être trouvé dans le livre *Presentation of groups*[2].

Lemme 7.1.7. *Tout groupe isomorphe à un groupe libre est libre.*

Preuve. Soit G groupe isomorphe à un groupe libre F. Alors la propriété universelle de F donnée par la définition 5.1.1 est étendue par l'isomorphisme, et montre que G vérifie cette même propriété. Ainsi, G est libre. □

Proposition 7.1.8. *Soit F un groupe, et $X \in F$. F libre sur X si et seulement si ces deux conditions sont vérifiées :*

(i) X génère F

(ii) Aucun mot réduit de $X^{\pm}$ de longueur positive n'est égal à e.

Preuve. Soit $\iota : X \hookrightarrow F$. Il existe donc un unique homomorphisme $\phi : F(X) \longrightarrow F$ tel que $\phi \circ \iota = i$, avec i l'inclusion de X dans $F(X)$. D'après la preuve vue précédemment, les conditions (i) et (ii) sont équivalents au fait que ϕ est respectivement surjectif et injectif.
De plus, dire que F est libre est équivalent à dire que ϕ a un inverse, et donc est un isomorphisme. En effet, la première implication vient du fait que l'unique morphisme ψ donnant la commutativité du diagramme dans le cas où F est libre est l'inverse de ϕ. L'implication inverse vient du fait que tout groupe isomorphe à un groupe libre est libre, ce qui correspond au lemme 7.1.7.
Nous avons donc établi les équivalences nécessaires :

$$F \text{ libre sur } X \Leftrightarrow \phi \text{ est une bijection} \Leftrightarrow \text{(i) et (ii) sont vérifiés.} \tag{9}$$

□

7.2 Transformations de Nielsen

La première preuve historique du théorème de Nielsen-Schreier repose sur la transformation d'un sous-groupe donné X d'un groupe libre F, en lui imposant certaines opérations, appelées **transformations de Nielsen**. En faisant subir à X une certaine séquence de transformations, nous le réduisons en un ensemble Y, dit **Nielsen-réduit**. De là s'en suit des propositions qui mèneront tout d'abord à la preuve de notre théorème dans le cas fini, puis dans le cas général.

Définition 7.2.1. Soit $F = F_n$ un groupe fini de rang $n \geq 2$, un ensemble $X = \{x_1, x_2, ...\}$ de générateurs libres et $Y = \{y_1, y_2, ...\}$ un ensemble fini d'éléments de F. Nous pouvons appliquer les transformations élémentaires suivantes à Y :

(T1) y_i est remplacé par $y_i y_j$ pour un certain $j \neq i$;

(T2) y_i est remplacé par y_i^{-1} ;

(T3) On interchange y_j et y_i ;

(T4) Si $y_i = e$, on supprime y_i.

Ces transformations sont appelées **transformations de Nielsen**.

Définition 7.2.2. Soit $F = F_n$ un groupe fini de rang $n \geq 2$, et $Y = \{y_1, y2, ..., y_n\}$ un ensemble fini d'éléments de F. Alors il existe une suite de transformations de Nielsen sur Y qui renvoie un ensemble $U = \{u_1, u_2, ..., u_m\}$ vérifiant :
Pour tout triplets v_1, v_2, v_3 de la forme $u_i^{\pm 1}$, on a :

i) $v_1 \neq 1$;

ii) $v_1 v_2 \neq 1 \Longrightarrow |v_1 v_2| \geq |v_1|, |v_2|$;

iii) $v_1 v_2 \neq 1$ et $v_2 v_3 \neq 1 \Longrightarrow |v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

Un tel ensemble U est appelé un ensemble **Nielsen-réduit**, ou **N-réduit**.

Il existe un algorithme prenant en argument un ensemble $U = (u_1, u_2, ..., u_m)$ et renvoyant sa Nielsen-réduction. L'algorithme utilise la fonction ρ, qui renvoie le mot réduit d'un mot donné en argument. Voici son déroulé :

Algorithm 1 Nielsen-Réduction

(1)
$U = \{u_1, ..., u_m\}$
for all i **do**
  $v \leftarrow \rho(u_i)$:
  if $v = e$ **then**
    delete u_i
  else
    $u_i \leftarrow \min\{v, v^{-1}\}$
  end if
end for

(2)
$B \leftarrow true$
while B **do**
  $B \leftarrow false$
  for all i, j **do**
    for $\epsilon, \eta = \pm 1$ **do**
      $v \leftarrow \rho(u_i^{\epsilon}, u_i^{\eta})$
      if $i \neq j$ and $|v| < |u_i|$ **then**
        $B \leftarrow true$
        if $v = e$ **then**
          delete u_i
        else
          $u_i \leftarrow \min\{v, v^{-1}\}$
        end if
      end if
    end for
  end for
end while

(3)
Chercher le plus petit $u_j = pq^{-1}$ tel qu'il existe un $u_k = qc^{-1}$ ou cq^{-1}, $j \neq k$.
if il n'y a pas de tel u_j **then**
  goto (4)
else
  $u_k \leftarrow \min\{pc^{-1}, cp^{-1}\}$
  goto (2)
end if

(4)
Return $V = \{ui \mid u_i \text{ is not deleted}\}$.

Cet algorithme n'est pas efficace, dans la mesure où sa complexité est assez grande. Ainsi, dans les cas simples, nous pouvons utiliser notre intuition pour réduire l'ensemble étudié. Pour en savoir plus, voir [6, p.64].

Définition 7.2.3. On dit que deux ensembles sont **Nielsen-équivalents** si l'un peut être obtenu par une séquence de transformation de Nielsen sur l'autre.

Proposition 7.2.4. *Soit $F = F_n$ un groupe fini de rang $n \geq 2$, et $Y, \tilde{Y}$ deux ensembles finis d'éléments de F. Si Y et $\tilde{Y}$ sont Nielsen-équivalents, alors ils génèrent le même sous groupe.*

Preuve. Il suffit de prouver que pour toute transformation élémentaire de Nielsen τ, $\langle Y \rangle = \langle Y_\tau \rangle$, où Y_τ est l'ensemble donné par la transformation τ sur Y. □

Corollaire 7.2.5. *Soit V un ensemble N-réduit d'un groupe libre F. Alors F est libre sur V.*

Lemme 7.2.6. *Soit F un groupe libre, et U un ensemble dans F. Alors il existe une séquence de transformations de Nielsen qui, appliqué U, donne un ensemble V N-réduit.*

Preuve du théorème : voir [3, Chapitre 3, page 29]

Théorème 7.2.7 (Théorème de Nielsen-Schreier dans le cas fini)**.** *Tout sous-groupe généré par un ensemble fini d'un groupe libre est libre.*

preuve. Soit F un groupe libre, et H un sous-groupe généré par un ensemble U. Par le lemme 7.2.6, il existe une séquence de transformations de Nielsen T donnant un ensemble V N-réduit, avec $V = UT$. Par la proposition 7.2.4, le groupe généré par V est le même que celui généré par U, soit H. Enfin, la proposition 7.1.8 nous dit que $\langle V \rangle = H$ est libre. □

Remarque 7.2.8. Nous pouvons en fait élargir ce théorème dans le cas général. En effet, comme nous l'avons vu dans la section précédente, le théorème de Nielsen-Schreier reste vrai pour un sous-groupe arbitraire d'un groupe libre. Ainsi, la preuve donnée peut être étendue dans ce cas, mais nous l'omettrons dans le cadre de ce rapport. Le lecteur intéressé peut consulter [3, Chapitre 3.3, page 33]

7.3 Exemple

Reprenons l'ensemble de la section 6.3. Le groupe $H \subset F(\{x, y\})$ est l'ensemble des mots de longueur pair de F, libre d'après le théorème de Nielsen-Schreier. Un générateur évident serait donc $U = (u_1, ..., u_6) = (x^2, xy, xy^{-1}, yx, y^2, y^{-1}x)$. Cependant, U n'est pas libre : $xyy^{-1} = x^2 \in U$. Essayons donc de le Nielsen-réduire. Nous pouvons utiliser l'algorithme 1, ou nous pouvons essayer de le déduire intuitivement :

$(y^{-1}x) \longrightarrow_{\mathrm{T2}} (x^{-1}y)$
$(x^2) \longrightarrow_{\mathrm{T1}} (x^2x^{-1}y) \equiv (xy) \longrightarrow_{\mathrm{T1}} (y^{-1}x^{-1}) \longrightarrow_{\mathrm{T1}} (y^{-1}x^{-1}xy) \equiv e$ (T4)
$(xy) \longrightarrow_{\mathrm{T1}} (xyx^{-1}y^{-1}) \equiv (x^2)$
$(xy^{-1}) \longrightarrow_{\mathrm{T2}} (yx^{-1}) \longrightarrow_{\mathrm{T1}} (yx^{-1}x^2) \equiv (yx) \longrightarrow_{\mathrm{T2}} (x^{-1}y^{-1}) \longrightarrow_{\mathrm{T1}} (x^{-1}y^{-1}yx) \equiv e$ (T4)
$(y^2 \longrightarrow_{\mathrm{T1}} (y^2y^{-1}x) \equiv (yx) \longrightarrow_{\mathrm{T2}} (x^{-1}y^{-1}) \longrightarrow_{\mathrm{T1}} (x^{-1}y^{-1}yx) \equiv e$ (T4)

Ainsi, nous obtenons l'ensemble suivant : $V = \{x^2, yx, y^{-1}x\}$. Ce dernier vérifie bien les conditions d'un ensemble Nielsen-réduit. Il est donc la base du groupe libre H. Une autre méthode pour Nielsen-réduire cet ensemble se trouve dans [3, Chapitre 3, page 32].

7.4 Comparaison des deux méthodes

Le théorème de Nielsen-Schreier met en exergue les liens entre les différents domaines mathématiques. Sa découverte historique est purement combinatoire, mais l'utilisation des groupes fondamentaux a permi de rattacher la topologie des graphes aux groupes libres, menant ainsi à la découverte de la preuve topologique. Nous pouvons donc comparer ces deux approches.

Une chose à remarquer est que la méthode topologique est plus intuitive dans le cas général, elle découle directement de théorèmes et propriétés qui se visualisent facilement. Cependant, la méthode combinatoire possède un avantage dans sa richesse d'information dans le cas fini : à partir d'un générateur quelconque du sous-groupe à étudier, nous pouvons directement, à partir de l'algorithme, lui trouver une base, alors que la méthode topologique demande plus d'intuition et de travail pour le même résultat.

8 Conclusion et conséquences du théorème

Par son application dans différents domaines mathématiques, le théorème de Nielsen-Schreier ouvrent sur d'autres résultats. Nous pouvons en citer des purement mathématiques, comme le *théorème fondamental des groupes cycliques*, ou encore la *conjecture de Hanna Neumann*.

Ce théorème a également des applications en cryptographie. En effet, en raison de la menace imposante de systèmes informatiques de plus en plus puissants, des alternatives basées sur la théorie des groupes à la cryptographie RSA ou Diffie-Hellman pour la distribution secrète ont été envisagées. Parmi elles, un des protocoles de partage de secret tient son origine de la preuve combinatoire du théorème de Nielsen-Schreier. En raison de la nature constructive et algorithmique de la preuve originale, une telle utilisation est naturelle. Une étude approfondie des méthodes cryptographiques qui utilisent les transformations de Nielsen est donnée dans [5].

Références

[1] A. Hatcher, *Algebraic Topology* (2001)

[2] R. Brown, *Nonabelian Algebraic Topology*, UWB Math Preprint (2008)

[3] D. L. Johnson, *Presentation of Groups*, Cambridge University Press (1997)

[4] M. Audin, *Topologie : Revêtements et groupe fondamental*, Université Louis Pasteur (2000)

[5] Anja I. S. Moldenhauer, *Cryptographic protocols based on inner product spaces and group theory with a special focus on the use of Nielsen transformations*, Universität Hamburg (2016)

[6] J. Avenhaus and K. Madlener, *The Nielsen Reduction and P-complete problems in free groups*, Universität Keiserslautern (1984)