

UNIVERSITE D'AIX-MARSEILLE I, II, III
U.F.R. M.I.M.

PROBLEMES DE DEHN

Memoire pour le D.E.A. de Mathématiques

Présenté par Jean-Philippe PREAUX

Sous la direction de Hamisch SHORT

Année universitaire 1994-95

Index

CHAPITRE I : Notions préliminaires	6
I.1 : Présentation de groupe	6
I.2 : Transformation de Tietze	10
I.3 : Problèmes de Dehn	15
I.4 : Machines de Turing	21
I.5 : Extensions de Britton et HNN extensions	27
CHAPITRE II : Théorèmes généraux d'insolubilité	33
II.1 : Théorème de Post	34
II.2 : Théorème de Novikov-Boone	38
II.3 : Théorèmes de plongements	51
II.3.1 : Théorème de Higman	51
II.3.2 : Théorème de Higman-Neumann-Neumann	63
II.4 : Propriété de Markov et théorème de Adjan-Rabin	66
CHAPITRE III : Problèmes de Dehn pour des groupes élémentaires	71
III.1 : Résolution des problèmes de Dehn pour les groupes libres	71
III.1.1 : Problème de la conjugaison	71
III.1.2 : Problèmes du mot généralisé	73
III.2 : Problèmes de Dehn et constructions algébriques	77
III.2.1 : Produit libre	78
III.2.2 : Produit direct	82
III.2.3 : HNN extensions et extensions de Britton	84
a) Problème du mot et problème du mot généralisé	84
b) Problème de la conjugaison	86
III.2.4 : Produit libre amalgame	90
III.2.5 : Split extension	93
III.3 : Problèmes de solubilité dans des classes algébriques	94
III.3.1 : Groupes résiduellement ,finis ,nilpotents ,libres	95
III.3.2 : Résultats d'insolubilité dans des sous-groupes de groupes élémentaires	97
CHAPITRE IV : Etude géométrique des problèmes de Dehn	100

IV.1 : Inégalité isopérimétrique et algorithmes de Dehn	100
IV.1.1 : Diagramme de Lyndon Van-Kampen	101
IV.1.2 : Inégalité isopérimétrique	102
IV.1.3 : Algorithmes de Dehn	103
IV.2 : Groupes à petites simplifications	104
IV.2.1 : Hypothèses de petites simplifications	104
IV.2.2 : Interprétation géométrique	105
IV.2.3 : Formules et inégalités pour des disques	107
IV.2.4 : Algorithmes de Dehn et inégalité isopérimétrique linéaire pour des groupes à petites simplifications	110
IV.3 : Groupes hyperboliques	111
IV.3.1 : Structure métrique dans un groupe f.e.	111
IV.3.2 : Graphe de Cayley	113
IV.3.3 : Espace hyperbolique	114
IV.3.4 : Caractérisation des groupes ayant un algorithme de Dehn ou une inégalité isopérimétrique linéaire	117
IV.4 : Quasi-isométries	122
CHAPITRE V : Insolubilité en topologie	126
Bibliographie	131

INTRODUCTION

Les groupes apparaissent souvent naturellement sous la forme de présentations (essentiellement en topologie). Etant donnée une présentation, on peut se donner les éléments du groupe comme des mots sur les générateurs. Le problème consiste alors à étudier des propriétés locales d'un groupe (i.e. portant sur les éléments) et des propriétés globales (i.e. portant sur le groupe) par le biais de sa présentation.

En 1911, Dehn formule les problèmes suivants :

Etant donné une présentation de groupe .

Problème du mot : Etablir une procédure permettant de décider pour un mot arbitraire sur les générateurs, s'il représente l'élément neutre du groupe .

Problème de la conjugaison : Etablir une procédure permettant de décider pour un couple de mot, s'ils sont conjugués .

Problème de l'isomorphisme : Etablir une procédure permettant de décider pour deux présentations, si elles représentent le même groupe .

Ces problèmes portent le nom de problèmes de Dehn. Nous considérons aussi un autre problème, le problème du mot généralisé : Etant donnée une famille de mots a_1, \dots, a_n , décider pour un mot arbitraire, s'il est dans le sous-groupe engendré par a_1, \dots, a_n (et alors, comme nous le verrons on peut donner une écriture de l'élément de groupe correspondant sur a_1, \dots, a_n).

Ces problèmes sont fondamentaux, et ce pour plusieurs raisons. Premièrement, les problèmes de topologie, se ramènent fréquemment, par le biais du groupe fondamental, à des problèmes portant sur les présentations. Alors pour une présentation du groupe fondamental, décider si un mot est trivial revient à décider si un lacet fermé est contractile ; décider si deux mots sont conjugués revient à décider si deux lacets fermés sont librement homotopes ; décider si un mot est dans le sous-groupe engendré par a_1, \dots, a_n

revient à décider si un lacet fermé se relève dans le revêtement correspondant au sous-groupe en un lacet fermé .

Si deux espaces topologiques sont homéomorphes ,alors leur groupe fondamental sont isomorphes .Ainsi le problème de l'isomorphisme nous donne un critère de démarcation

Deuxièmement ,La résolution du problème du mot (essentiellement) et des autres problèmes de Dehn permet d'établir des algorithmes de Decision pour beaucoup de propriétés .Par exemple si l'on a une solution au problème du mot ,pour une présentation donnée ,on peut décider si le groupe est abélien (alors les commutateurs des générateurs sont triviaux) ,si un groupe est fini ,on peut l'établir ;on peut aussi construire une table de multiplication pour le groupe (etc ...) .

Novikov et Rabin ,ont démontré qu'en général tous ces problèmes sont insolubles .Il existe néanmoins des groupes pour lesquels on sait résoudre ces problèmes .

Le but de notre travail est le suivant :

- (1) Etablir les théorèmes généraux d'insolubilité .
 - (2) Etablir des résultats d' insolubilité pour des groupes élémentaires
 - (3) Etablir des résultats de solubilité dans des classes de groupe (les plus larges possibles) .
 - (4) Etablir la stabilité de la résolution de ces problèmes par des constructions ,ou des relations entre présentations ,ou entre groupe .
- (Notons que même si les problèmes de dehn portent sur des présentations ,nous établirons que pour tous (excepté le problème de l'isomorphe) la possibilité de résolution est un invariant algébrique dans la classe des présentation f.e.)

Dans la première partie nous établirons les concepts élémentaires nécessaires à la suite ,en particuliers la notion de HNN extension dont l'utilisation sera omniprésente dans les chapitres II et III

Dans la deuxième partie ,nous établissons tous les résultats

d'insolubilité ,théorème de Post ,théorème de Novikov ,théorème d'Adjan-Rabin ainsi que des théorèmes de théorie des groupes (Higman ,Higman-Neuman-Neuman) qui nous seront utiles pour la suite .

Dans la troisième partie nous établissons des résultats d'insolubilité et de solubilité ,pour des groupes élémentaires ,i.e. ,définies par des propriétés algébriques élémentaires ,ou construits sur des groupes élémentaires par des chaînes de produit libre amalgamé ,split extension ,produit direct ,extension HNN .Nous étudions en particulier ,l'effet de ces constructions sur la résolution des problèmes .

Dans la quatrième partie ,nous employons la méthode géométrique pour résoudre le problème du mot dans des classes larges de groupes ,les groupes hyperboliques de M.Gromov ,et certains groupes à petite simplification .Nous analysons en particulier les notions d'algorithme de Dehn ,et d'inégalité isopérimétrique ,et caractérisons les groupes admettant un algorithme de Dehn ,ou une inégalité isopérimétrique (ce sont les groupes Hyperboliques) .Nous établissons aussi la stabilité de la propriété avoir un problème du mot soluble dans la classe des groupes finiment engendré ,par quasi isométrie .

Puisque ces problèmes naissent essentiellement en topologie ,il était naturel ,d'étudier certains effets des résultats que nous avons établi ,en topologie .C'est ce que nous faisons dans la cinquième partie .Nous construisons sur une présentation finie ,une présentations de 5 variétés à bord ,et de 4-variétés fermées sans bord ,dont le groupe fondamental est le groupe déterminé par la présentation de groupe utilisée .Nous avons alors l'insolubilité des problèmes de Dehn pour des groupe fondamentaux de 4 variétés et de 5 variétés .Nous établissons de plus une résultat de Markov :le problème de l'homéomorphisme est insoluble pour ces classes de variétés .

CHAPITRE 1 :

NOTIONS PRELIMINAIRES

I.1 PRESENTATION DE GROUPE

Soit X un ensemble dénombrable non vide .On considère X' ,copie de X .Il y a une bijection naturelle $\varphi : X \longrightarrow X'$. X' sera noté X^{-1} et pour un élément $x \in X$, $\varphi(x)$ sera noté x^{-1} , x sera éventuellement noté x^{+1} .

On appelle mot sur l'alphabet X (ou sur X) ,tout suite finie d'éléments de $X \cup X^{-1}$.On notera une telle suite $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ où $x_1, \dots, x_n \in X$ et $\varepsilon_1, \dots, \varepsilon_n \in \{-1; 1\}$. n est appelé longueur du mot .Le mot de longueur nulle est appelé le mot vide et sera noté 1 .Un mot de longueur n est dit positif si pour tout $i = 1 \dots n$, $\varepsilon_i = +1$. L'ensemble des mots sur X sera noté $\mathcal{M}(X)$. $\mathcal{M}(X)$ muni de la loi de concaténation est un monoïde ,noté $M(X)$ ayant pour élément neutre le mot vide .Soient ω et ω' ,deux mots sur un même alphabet ,on note $\omega \equiv \omega'$ si ω et ω' sont identiques .On dit qu'un mot μ est un sous-mot de ω ,si il existe deux mots (éventuellement vides) α et β tels que $\omega \equiv \alpha \mu \beta$.On dit que μ est un sous-mot initial (resp^t terminal) de ω ,si il existe un mot α tel que $\omega \equiv \mu \alpha$ (resp^t $\omega \equiv \alpha \mu$) .Deux mots ω et ω' sont dits conjugués cycliques si il existe des mots α et β (éventuellement vides) tels que $\omega \equiv \alpha \beta$,et $\omega' \equiv \beta \alpha$.

On considère les opérations suivantes sur $\mathcal{M}(X)$

(1) On note $\omega \xrightarrow{(1)} \omega'$ lorsque il existe deux mots α et β tels que $\omega \equiv \alpha x x^{-1} \beta$,ou $\omega \equiv \alpha x^{-1} x \beta$;et $\omega' \equiv \alpha \beta$ (où $x \in X$) .

(2) On note sous les même conditions $\omega' \xrightarrow{(2)} \omega$.

On note $\omega \longrightarrow \omega'$ si $\omega \xrightarrow{(1)} \omega'$,ou $\omega \xrightarrow{(2)} \omega'$.

Deux mots ω et ω' sont dits librement égaux si ω' peut être obtenu à partir de ω par une suite finie d'opérations (1) et (2) ,i.e. si il existe une suite finie de mots $(\omega_0, \dots, \omega_n)$ où $\omega_0 \equiv \omega$, $\omega_n \equiv \omega'$,et $\forall i \in \langle 0, \dots, n-1 \rangle$, $\omega_i \longrightarrow \omega_{i+1}$.Un mot est dit librement réduit

, si on ne peut pas lui appliquer l'opération (1) (c'est à dire si il ne contient pas un sous-mot de la forme $x x^{-1}$, ou $x^{-1}x$. On appelle réduction libre d'un mot une suite finie d'opérations (1) appliquée au mot, tel que le mot obtenu soit librement réduit.

Il est aisé de vérifier qu'être librement égal est une relation d'équivalence sur $M(X)$, compatible avec la loi de concaténation. Le quotient de $M(X)$ par cette relation a une structure de groupe, où l'inverse de la classe d'équivalence de $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$, est la classe d'équivalence de $x_1^{-\varepsilon_1} \dots x_n^{-\varepsilon_n}$. Ce groupe sera noté $F(X)$, et sera appelé groupe libre engendré par X (ou sur X). Dans la suite on commettra l'abus de langage consistant à identifier un mot sur X avec sa classe d'équivalence dans $F(X)$.

PROPOSITION I.1.1 : Soit $F(X)$ un groupe libre. Si ω et ω' sont deux mots librement réduits, $\omega = \omega'$ dans $F(X)$ ssi $\omega \equiv \omega'$. En particulier si ω est réduit, et $\omega = 1$ dans $F(X)$, alors $\omega \equiv 1$.

Démonstration : Remarquons que si un mot ω donné peut être librement réduit en un unique mot ω_0 , il en est de même du mot obtenu à partir de ω par une opération (1) ou (2). Pour une opération de la forme (1) le résultat est trivial. Appliquons (2) à $\omega \equiv A B$. On obtient $\omega_1 \equiv A x x^{-1} B$ (l'autre cas étant similaire), que l'on réduit librement. Une opération (1) intervenant sur un sous-mot de A ou de B , pourrait être appliquée sur ω , et donc donc d'après ce qui précède n'altère pas le résultat. On peut donc sans perte de généralités supposer que A et B sont librement réduits. On a alors un des cas suivants :

$$\begin{aligned}\omega_1 &\equiv A x x^{-1} B \xrightarrow{(1)} A B \equiv \omega \\ \omega_1 &\equiv A x x^{-1} B \equiv A' (x^{-1} x) x^{-1} B \xrightarrow{(1)} A' x^{-1} B \equiv A B \equiv \omega \\ \omega_1 &\equiv A x x^{-1} B \equiv A x (x^{-1} x) B' \xrightarrow{(1)} A x B' \equiv A B \equiv \omega\end{aligned}$$

Donc dans tout les cas, si ω peut être librement réduit en un unique élément ω_0 , il en est de même de ω_1 .

Considérons deux mots librement réduits ω et ω' , librement égaux. Il existe donc une suite de transformations de la forme (1) et (2) changeant ω en ω' . Or ω ne peut être librement réduit qu'en lui-même. Donc ω' ne peut être librement réduit qu'en ω . Or ω' est librement réduit, et donc $\omega \equiv \omega'$. ■

Remarque : Le procédé de réduction libre est déterministe ,i.e le résultat d'une réduction libre est indépendant de la façon de procéder .Pour un groupe libre ,donné par ses générateurs ,on a une solution au problème du mot ,par application de réductions libres .

Etant donné un groupe G ,et une S famille génératrice de G ,on peut se donner les éléments de G ,par des mots sur les générateurs .On dira que G est Libre sur S ,si tout mot réduit sur S ,représentant un élément l'élément neutre de G ,est vide .On vérifie aisément qu'alors G est le groupe libre sur S , $G \cong F(S)$.Un groupe est dit Libre ,si il est libre sur une de ses familles génératrices .

$|X|$ sera appelé le rang de $F(X)$.Si X est fini ,on dira que $F(X)$ est de rang fini .Un résultat important est le fait qu'un groupe libre est uniquement déterminé par son rang (à isomorphisme près).

PROPOSITION I.1.2 : Soient un groupe G et $\psi : X \rightarrow G$.Alors il existe un unique homomorphisme Ψ ,tel que le diagramme suivant commute .

$$\begin{array}{ccc} & F(X) & \\ \uparrow & \searrow \Psi & \\ X & \xrightarrow{\psi} & G \end{array}$$

Remarques Il s'agit même d'une caractérisation des groupes libres .

Les groupes libres sont des objets universels dans la catégorie des groupes .

Considérons un groupe G quelconque ,et S une famille génératrice de G .Alors d'après la proposition I.1.2 ,il existe un unique homomorphisme surjectif $\Psi : F(S) \rightarrow G$,dont la restriction à S est l'inclusion sur les générateurs de G .On a donc $G \cong F(S) / \ker \Psi$.Toute groupe est donc quotient d'un groupe libre par un sous-groupe normal .Appelons R un sous-ensemble de $F(S)$,dont la clôture normale dans $F(S)$ est $\ker \Psi$ (elle sera notée $\text{gp}_{F(S)}(R)$) .On appelle présentation de G la donnée de $\langle S / R \rangle$,où R est donné comme un ensemble de mots sur S . $F(S)$ s'appelle le sous-groupe libre sous-jacent à G

Réciproquement considérons un ensemble S ,et R un ensemble de

mots sur S . Alors il existe un groupe, unique à isomorphisme près ayant pour présentation $\langle S / R \rangle$. En effet les éléments de R sont éléments du groupe libre sur S , et $F(S) / \text{gp}_{F(S)}(R)$ définit un unique groupe.

Les éléments de S sont appelés les générateurs, et les éléments de R , les relateurs. Un relateur de la forme $\alpha \beta^{-1}$ sera éventuellement noté $\alpha = \beta$ (et alors sera appelé relation). Un élément de la forme $x x^{-1}$ ou $x^{-1}x$ ($x \in S$) sera appelé relateur trivial.

Etant donné une présentation $\langle S / R \rangle$, on note $\text{gp}(\langle S / R \rangle)$ le groupe ayant cette présentation. Un groupe admet une infinité de présentations. En effet, si $\langle S / R \rangle$ est une présentation de G , il en est de même de $\langle S \cup \{a\} / R \cup \{a\} \rangle$ si $a \notin S$. Si le contexte le permet, on confondra un groupe et une de ses présentations.

une présentation est dite finie, si S et R sont finis. Un groupe est dit finiment présenté (f.p.), si il admet une présentation finie. Un groupe est dit finiment engendré (f.e.), si il admet une famille génératrice finie (dans ce cas il admet une présentation $\langle S / R \rangle$ où S est fini).

De la même façon que pour les groupes libres, lorsque l'on se donnera un groupe par une présentation, on verra les mots sur les générateurs comme éléments du groupe, i.e., on confondra un mot avec sa classe d'équivalence. Lorsque le contexte l'exigera, on notera $\bar{\omega}$, l'élément de groupe représenté par ω . Pour un groupe G , nous noterons $=_G$ pour exprimer une égalité dans G . L'écriture $=_F$ sera réservée à la relation être librement égal.

PROPOSITION I.1.3 : Si un groupe G admet une présentation finie

$$\langle x_1, \dots, x_n / r_1, \dots, r_m \rangle$$

, ainsi qu'une présentation finiment engendrée

$$\langle a_1, \dots, a_N / R_1, \dots \rangle$$

alors tous les relateurs, sauf un nombre fini d'entre eux sont superflus, i.e.

$$\langle a_1, \dots, a_N / R_i ; i \in I \rangle$$

est une présentation de G , où $I \subset \mathbb{N}$ est fini.

Démonstration : Appelons F_1/N_1 et F_2/N_2 les quotient correspondant resp^t à la première et deuxième présentation. Il

existe un isomorphisme $\psi : F_1/N_1 \longrightarrow F_2/N_2$, qui envoie les générateurs x_1, \dots, x_n sur des mots en a_1, \dots, a_N (de longueur bornée). Les images de r_1, \dots, r_m , sont dans le sous-groupe normal engendré par R_1, \dots etc... ; c'est à dire s'écrivent comme produit de conjugués sur ces relateurs. Puisque les mots $\psi(r_1), \dots, \psi(r_m)$ sont de longueur bornée, seul un nombre fini de R_i sont utiles à leur écriture comme produit de conjugués de relateurs. De plus $\psi(r_1), \dots, \psi(r_m)$ engendrent N_2 . En effet soit un mot w en a_1, \dots, a_n , trivial. Alors $\psi^{-1}(w)$, est trivial, et s'écrit donc comme produit de conjugués de r_1, \dots, r_m . Ainsi w s'écrit comme produit de conjugués de $\psi(r_1), \dots, \psi(r_m)$. Et donc seul un nombre fini de R_i est utile à engendrer N_2 . ■

Etant donné un groupe G donné par une présentation $\langle S / R \rangle$, deux mots w et w' sont égaux dans G (i.e. sont représentants de la même classe d'équivalence), si et seulement si $w w'^{-1}$ est librement égal à un élément de $gp_{F(S)}(R)$, soit si w est librement égal à $\prod_{i=1..k} p_i r_i p_i^{-1}$, où les r_i sont des éléments de R , et les p_i sont des mots sur S . On peut donc passer de w' à w par une suite finie d'opérations de la forme suivante :

- (1) Insertion d'un sous-mot de la forme $x x^{-1}, x^{-1} x$ ($x \in S$), r_i ($r_i \in R$).
- (2) Suppression d'un sous-mot de la forme $x x^{-1}, x^{-1} x, r_i$.

De plus il est clair que si l'on applique une des opérations précédentes à un mot, on obtient un mot de la même classe d'équivalence. Ceci a donné à la théorie s'intéressant aux groupes par la donnée de présentation le nom de *combinatoire des groupes*.

I.2 TRANSFORMATIONS DE TIETZE

Notations : On note $w(a_1, \dots, a_n)$ lorsque le mot w s'écrit sur a_1, \dots, a_n . Si l'on a une correspondance $a_i \longleftrightarrow b_i$ pour $i = 1..n$, on note $w(b_i)$ le mot obtenu à partir de w , en remplaçant toutes les occurrences de a_i , par b_i , $i = 1..n$.

Soit $\langle x_1, \dots, x_n / r_1, \dots, r_m \rangle$ une présentation finie d'un groupe G . On considère les transformations suivantes, appelées transformations de Tietze.

T_1 : Ajouter à la présentation de G , un relateur r_{m+1} , qui appartient à la clôture normale de $\langle r_1, \dots, r_m \rangle$.

T_1^{-1} : Opération inverse de T_1 .

T_2 : Ajouter à la présentation de G , un générateur x_{n+1} , ainsi qu'une relation $x_{n+1} = \omega(x_1, \dots, x_n)$.

T_2^{-1} : Opération inverse de T_2 .

THEOREME I.2.1 : (Tietze)

Deux présentations finies sont des présentations du même groupe ssi on peut passer de l'une à l'autre par une suite finie de transformations de Tietze.

Démonstration : Condition suffisante

La transformation T_1 laisse le groupe libre sous-jacent et son sous-groupe normal inchangés et donc le groupe reste identique

Soient G donné par $\langle x_1, \dots, x_n / r_1, \dots, r_m \rangle$ et G' dont la présentation est obtenu à partir de celle de G par une transformation T_2 . Considérons $\varphi : \langle x_1, \dots, x_n, x_{n+1} \rangle \rightarrow \langle x_1, \dots, x_n \rangle$ dont la restriction à $\langle x_1, \dots, x_n \rangle$ est l'identité et tel que l'image de x_{n+1} soit $\omega(x_1, \dots, x_n)$ intervenant dans T_2 . Alors il existe un unique homomorphisme surjectif du groupe libre sous-jacent à G' dans G (prop. I.1.2). Les relateurs de G' sont dans $\ker \varphi$, et donc φ passe au quotient en $\tilde{\varphi} : G' \rightarrow G$, homomorphisme surjectif. De plus soit un mot ζ en $\langle x_1, \dots, x_{n+1} \rangle$ tel que $\tilde{\varphi}(\zeta) =_G 1$. Alors en utilisant $x_{n+1} = \omega(x_1, \dots, x_n)$, on a un mot ζ' en $\langle x_1, \dots, x_n \rangle$ tel que $\zeta' =_G \zeta$. L'image de ζ' par $\tilde{\varphi}$ est le même mot, qui est librement égal à un élément de la forme $p_1 r_{i_1}^{\varepsilon_1} p_1^{-1} \dots p_k r_{i_k}^{\varepsilon_k} p_k^{-1}$ où les r_i sont des relateurs de G . Or tout relateur de G est un relateur de G' et donc $\zeta =_G \zeta' =_G 1$. Ainsi $\ker \tilde{\varphi} \subseteq \text{gp}_{G'}(\langle r_1, \dots, r_{m+1} \rangle)$, et donc $\tilde{\varphi}$ est un isomorphisme de G' dans G . \square

Condition nécessaire

Supposons que G admette deux présentations finies π et π' que l'on notera $\langle a_i / r_j(a_i) \rangle$ et $\langle a'_i / r'_j(a'_i) \rangle$.

Puisque les deux présentations représentent le même groupe il y a des mots α'_i en a_i représentant les a'_i . Alors les $r'_j(\alpha'_i)$ sont conséquences des $r_j(a_i)$ (i.e. sont dans le sous-groupe normal engendré par les $r_j(a_i)$). De même il y a des mots α_i en a'_i .

représentant les a_i , et les $r_j(\alpha_i)$ sont conséquences des $r'_j(a'_i)$.
On effectue alors les transformations de Tietze suivantes :

$$\begin{aligned}
 & \langle a_i / r_j(a_i) \rangle \\
 & \langle a_i / r_j(a_i) ; r'_j(\alpha'_i) \rangle \quad \text{par } T_1 \\
 & \langle a_i ; a'_i / r_j(a_i) ; r'_j(\alpha'_i) ; a'_i = \alpha'_i \rangle \quad \text{par } T_2 \\
 & \langle a_i ; a'_i / r_j(a_i) ; r'_j(a'_i) ; r'_j(\alpha'_i) ; a'_i = \alpha'_i \rangle \quad \text{par } T_1 \\
 & \langle a_i ; a'_i / r_j(a_i) ; r'_j(a'_i) ; a'_i = \alpha'_i \rangle \quad \text{par } T_1^{-1} \\
 & (*) \langle a_i ; a'_i / r_j(a_i) ; r'_j(a'_i) ; a'_i = \alpha'_i ; a_i = \alpha_i \rangle \quad \text{par } T_2
 \end{aligned}$$

De même on peut transformer la présentation π' en (*) par une suite finie de transformations de Tietze. Et, en considérant les transformations inverses, (*) se transforme en π' . On a alors une suite finie de transformations de Tietze :

$$\pi \longrightarrow \dots \longrightarrow (*) \longrightarrow \dots \longrightarrow \pi' \quad \text{C. Q. F. D.} \blacksquare$$

Remarques Si l'on se permet de faire intervenir dans les transformations, une infinité de générateurs ou relateurs, le théorème se généralise aux présentations quelconques. La démonstration est en tout point similaire.

Ce résultat caractérise combinatoirement des présentations (finies) d'un même groupe, tout en fournissant des opérations élémentaires permettant de changer une présentation d'un groupe, en une autre. Il ne fournit néanmoins pas de procédure effective permettant de décider si deux présentations données, définissent un même groupe. Cependant pour une présentation finie d'un groupe G , les transformations de Tietze permettent d'établir un algorithme énumérant toutes les présentations finies de G . Ainsi pour des groupes dont on connaît une présentation finie canonique, on peut énumérer toutes ses présentations finies. C'est le cas des groupes libres de rang fini (avec pour présentation $\langle x_1 \dots x_n / \rangle$), des groupes abéliens (théorème de Kronecker), des groupes finis (relateurs $x_i x_j = x_k$), du groupe trivial ($\langle a / a \rangle$), etc ...

COROLLAIRE I.2.1 : On peut construire un algorithme, qui pour une présentation finie quelconque, énumère toutes les présentations finies du même groupe.

Démonstration : Nous allons construire un tel algorithme .

Considérons les transformations élémentaires de Tietze $T_1, T_1^{-1}, T_2, T_2^{-1}$. Une telle transformation sera dite de rang k ($k \in \mathbb{N}$), lorsqu'une des conditions suivantes est satisfaite :

-Il s'agit d'une transformations T_1 ou T_1^{-1} portant sur un relateur R dérivable en k étapes , i.e obtenu à partir du mot vide par au plus k opérations consistant à insérer ou à supprimer un relateur (autre que R) de la présentation , ou un relateur trivial .

-Il s'agit d'une transformation T_2 ou T_2^{-1} , portant sur un générateur α_{n+1} et un relateur $\alpha_{n+1} = \omega(\alpha_1, \dots, \alpha_n)$, tel que le mot ω soit de longueur au plus k .

Pour une transformation T quelconque $\exists k \in \mathbb{N}$, tel que T soit de rang k . De plus T est de rang k' pour tout $k' \geq k$.

Si l'on se donne une présentation finie , alors pour $k \in \mathbb{N}$, il y a un nombre fini de transformations de rang k pour cette présentation . De plus il y a une procédure finie les déterminant toutes :

-On détermine toutes les opérations T_1 réalisables , en énumérant tous les éléments dérivables en k étapes . Il y a un nombre fini de relateurs et de générateurs et donc aussi d'opération T_1 .

-On détermine toutes les opérations T_1^{-1} , En considérant pour chaque relateur de la présentation , tous les mots dérivables en k étapes à partir des autres relateurs . Puisqu'il y a un nombre fini de générateurs et de relateurs on peut décider (après réduction libre des mots obtenus) pour chaque relateur s'il est dérivable des autres en moins de k étapes , et ainsi déterminer toutes les transformations T_1^{-1} .

-On détermine toutes les transformation T_2 , en considérant tous les mots de moins de k lettres , qui bien sûr sont en nombre fini .

-Pour déterminer les opérations T_2^{-1} , on repère les générateurs n'apparaissant que dans un unique relateur . On peut alors appliquer T_2^{-1} , uniquement lorsqu'après réduction cyclique du relateur , le générateur considéré à une unique occurrence , et le relateur est de longueur $k + 1$. De même que précédemment il n'y a qu'un nombre fini de possibilités .

L'algorithme d'énumération est le suivant :

- Etape 1 : Enumérer et appliquer à la présentation toutes les transformations de rang 1 .On obtient un ensemble fini de présentations (finies) \mathcal{P}_1
- Etape i : Enumérer toutes les transformations de rang i applicables à des éléments de \mathcal{P}_{i-1} ,et les appliquer .On obtient un ensemble fini de présentations (finies) \mathcal{P}_i .

Considérons deux présentations finies d'un même groupe , Π et Π' . Alors il y a une suite finie de présentations (f.) $(\Pi_0; \dots; \Pi_n)$ telle que $\Pi = \Pi_0$ et $\Pi' = \Pi_n$,et une suite finie de changements de Tietze $(t_1; \dots; t_n)$,tels que $\forall i \in \langle 1, \dots, n \rangle$ t_i change Π_{i-1} en Π_i . On note $(rg_1; \dots; rg_n)$ la suite finie d'entiers ,telle que rg_i est le rang de t_i .On applique l'algorithme précédent à Π_0 . Alors :

- Π_1 est obtenu à l'étape rg_1
- si $rg_2 \leq rg_1$ alors Π_2 est obtenu à l'étape $rg_1 + 1$
- sinon Π_2 est obtenu à l'étape rg_2
- etc ...

Et ainsi soit M tel que $rg_m = \max \{rg_1, \dots, rg_n\}$. Alors Π_n est obtenu exactement à la $(rg_m + n - m)^{\text{ème}}$ étape . Toute présentation finie présentant le même groupe que Π est donc énumérée au bout d'un temps fini . L'algorithme néanmoins tourne indéfiniment et l'on ne sera jamais en possession de toutes les présentations finies du même groupe . ■

COROLLAIRE I.2.2 : On peut construire un algorithme ,qui pour deux présentations finies d'un même groupe permet d'exprimer tout élément du groupe donné par un mot dans une des présentations ,comme mot dans l'autre présentation .

Démonstration : Nous allons construire un tel algorithme .

Etant données deux présentations Π et Π' finies d'un même groupe . On peut utiliser l'algorithme précédent pour énumérer toutes les présentations finies ,représentant le même groupe que Π' . Alors au bout d'un temps fini ,on obtiendra Π' . Cet algorithme permet en outre d'explicitier une suite de changements de Tietze (t_1, \dots, t_N) ainsi qu'une suite de présentations (Π_0, \dots, Π_N) ,menant

de Π à Π' (i.e. $\Pi = \Pi_0$; $\Pi' = \Pi_N$) .

Considérons un mot ω exprimé dans Π . L'algorithme suivant permet d'écrire un mot de Π en un mot représentant du même élément dans Π' .

- Soit un mot ω exprimé dans Π_i . Si t_i est une opération de la forme T_2^{-1} , de générateur α et de relateur $\alpha = m$ où m est un mot sur les générateurs autres que α , alors ω' est le mot obtenu à partir de ω en remplaçant dans ω les occurrences de α par m . Sinon $\omega' \equiv \omega$. ω' est exprimé dans Π_{i+1} , et représente le même élément du groupe que ω .

Soit un mot exprimé dans Π_0 , On réitère l'opération l'opération précédente . On fini par aboutir à un mot dans Π_N , exprimant le même élément que ω . ■

I.3 PROBLEMES DE DEHN

On considère un groupe G donné par une présentation finie Π . Les problèmes de Dehn sont les suivants .

-Problème de l'égalité Existe-t-il un algorithme permettant de décider pour tout couple de mots sur les générateurs , s'ils représentent le même élément du groupe .

-Problème du mot Existe-t-il un algorithme permettant de décider pour tout mot ω sur les générateurs , si $\bar{\omega} = 1$.

-Problème de la conjugaison Existe-t-il un algorithme permettant de décider pour tout couple de mot , s'ils représentent des éléments conjugués du groupe (i.e si pour x et y , $\exists h \in G$ tel que $h^{-1}xh = y$ dans G) .

-Problème du mot généralisé Existe-t-il un algorithme qui pour $n + 1$ mots a_1, \dots, a_n, x , décide si x est dans le sous-groupe engendré par a_1, \dots, a_n .

-Problème de l'isomorphisme Existe-t-il un algorithme permettant de décider pour tout couple de présentations finies Π et Π' , si $gp(\Pi) \cong gp(\Pi')$.

Il faut remarquer que les problèmes de Dehn portent sur une présentation d'un groupe et non sur le groupe. Nous verrons néanmoins que pour les 4 premiers, leur résolution est indépendante de la présentation f.e. choisie.

On distingue dans les problèmes de décision sur les présentations, un problème local, d'un problème global, i.e. portant sur les mots, ou sur les présentations. Le problème de l'isomorphisme est global, alors que les autres problèmes de Dehn sont locaux. Le problème de l'isomorphisme semble être un analogue global du problème de l'égalité. Dans les deux cas, deux mots ou deux présentations sont équivalentes, si l'on peut aller de l'un(e) à l'autre par une finie de transformations élémentaires. Dans les deux cas le problème de décision consiste à décider si l'on peut construire entre deux éléments un cheminement. Dans la pratique, cependant la résolution du problème de l'isomorphisme s'avère être bien plus complexe.

Ces problèmes n'ont de sens que pour des présentations que l'on peut expliciter, c'est pourquoi on les définit pour des présentations finies. Les problèmes locaux peuvent néanmoins être étendus à une classe plus large, les présentations récursives. Une présentation est dite réursive si elle admet un nombre fini de générateurs, et si l'on peut énumérer ses relateurs (la notion d'énumération sera formalisée dans le paragraphe I.4). En particulier, toute présentation finie est réursive.

Pour de telles présentations, on a des algorithmes de semi-décision (i.e. d'énumération). On a déjà vu (corollaire I.2.1) que l'on peut énumérer toutes les présentations finies d'un groupe f.p. Pour les problèmes locaux, on peut pour un groupe f.e., énumérer sous une forme canonique, tous les éléments du groupe triviaux, égaux à un même élément, conjugués d'un élément, ou s'écrivant sur des générateurs donnés. Si la présentation est réursive, alors on peut énumérer tous les changements élémentaires, et ainsi tous les mots vérifiant les propriétés respectives.

Si l'on veut cependant décider, par exemple, si un mot est trivial, un algorithme de semi-décision laissera l'utilisateur devant des indéisions. En effet pour tout élément non trivial, l'utilisateur à un temps donné ne pourra décider si l'élément

n'est pas trivial ou bien si ,tout simplement la procédure ne l'a pas encore déterminé (les procédures d'énumération sont en général infinies) .De façon générale il en est de même pour tout les autres problèmes ,un algorithme d'énumération ne résoud pas le problème : il permet d'énumérer une liste perpétuellement incomplète .Remarquons néanmoins que dans la cas d'une classe de groupe f.p. pour laquelle tout groupe admet une (unique) écriture canonique ,l'algorithme d'énumération établit au corollaire I.2.1 ,nous permet de résoudre le problème de l'isomorphisme dans cette classe .En effet étant données deux présentations ,on peut énumérer toutes les autres présentations des même groupes .On finira par aboutir à deux présentations canoniques ,et l'on pourra décider si elles représentent le même groupe .Ainsi ,c'est le cas des groupes finis ,abéliens ,libres .En pratique cette algorithme ,ainsi que tout autre algorithme ,utilisant une énumération par changements de Tietze ,n'est pas effectif .

Dans la suite ,étant donnée une présentation Π ,on note respectivement , $\mathcal{WP}(\Pi)$, $\mathcal{Eg}(\Pi)$, $\mathcal{CP}(\Pi)$, $\mathcal{SWP}(\Pi)$, $\mathcal{Isom}(\Pi)$; le problème du mot ,le problème d'égalité ,le problème de conjugaison ,le problème du mot généralisé ,et le problème de l'isomorphisme (resp^t) ,sur Π .

Etant donnés deux problèmes de décision A et B ,on dit que A est réductible à B ,et l'on note $A \leq B$,si un algorithme pour B permet d'établir un algorithme pour A ,c'est à dire si une réponse positive au problème A est nécessaire à une réponse positive au problème B .Ainsi $\mathcal{WP}(\Pi) \leq \mathcal{Eg}(\Pi)$,puisque si l'on peut décider si deux mots sont égaux ,on peut décider lorsqu'un mot est trivial .Réciproquement deux mots ω et μ sont égaux ssi $\omega \mu^{-1} = 1$,ainsi $\mathcal{Eg}(\Pi) \leq \mathcal{WP}(\Pi)$.On note $\mathcal{Eg}(\Pi) \equiv \mathcal{WP}(\Pi)$.La relation \equiv est une relation d'équivalence sur l'ensemble des problèmes de décision ,les classes d'équivalences admettent un ordre partiel \leq ,et sont appelées degrés (cette notion se formalise en théorie des fonctions récursives .Etant donnés ,deux sous-ensemble de \mathbb{N}^p ,A et B ,on écrit $A \leq B$,si χ_A est construit à partir de χ_B et des fonctions élémentaires ,grâce aux schémas de construction des fonctions récursives .On démontre que \equiv est une relation d'équivalence sur les sous-ensembles de \mathbb{N}^p , $p \in \mathbb{N}$,qu'il existe

une infinité de classes d'équivalence ,et que la relation \leq établit une structure d'ordre partiel sur les classes d'équivalence ,avec une borne maximale $0'$ degré du problème d'arrêt de la machine de Turing universelle ,et une borne minimale 0 ,classe des ensembles rékursifs) .

On ne s'intéressera plus au problème de l'égalité,sa décidabilité est dans tous les cas équivalente à celle du problème du mot ,et de plus un algorithme pour le problème du mot fournit (de façon explicite) ,un algorithme pour le problème d'égalité .On peut remarquer d'autres cas de réducibilité dans les problèmes de Dehn

$\mathcal{WP}(\Pi) \leq \mathcal{EP}(\Pi)$,ceci car pour décider si un mot est trivial ,il suffit de décider s'il est conjugué au mot vide .

$\mathcal{WP}(\Pi) \leq \mathcal{SWP}(\Pi)$,car pour décider si un mot est trivial ,il suffit de décider s'il appartient au sous-groupe engendré par le mot vide .

Ainsi ,si l'on démontre que le problème de conjugaison ,ou le problème du mot généralisé sont résolubles pour Π ,alors le problème du mot est résoluble pour Π (et par la même le problème de l'égalité) .Dualement ,si l'on montre que le problème du mot n'est pas résoluble il en est de même pour les problèmes de conjugaisons ,et du mot généralisé .

LEMME I.3.1 : Dans la classe des présentations rékursives ,les problèmes du mot généralisé ,du mot ,et de conjugaison sont des invariants algébriques ,i.e ,pour deux présentations rékursives Π_1 ,et Π_2 d'un même groupe $\mathcal{WP}(\Pi_1) \equiv \mathcal{WP}(\Pi_2)$; $\mathcal{EP}(\Pi_1) \equiv \mathcal{EP}(\Pi_2)$; $\mathcal{SWP}(\Pi_1) \equiv \mathcal{SWP}(\Pi_2)$.

Démonstration : Considérons deux présentations $\Pi_1 = \langle S_1/R_1 \rangle$ et $\Pi_2 = \langle S_2/R_2 \rangle$,d'un même groupe .Alors ,il existe un isomorphisme $\varphi : F(S_1)/gp(R_1) \longrightarrow F(S_2)/gp(R_2)$ qui envoie les générateurs de Π_1 disons a_i ,sur des mots de Π_2 disons α_i .Remarquons que générateurs sont en nombre fini .

Si il existe un algorithme résolvant \mathcal{WP} , \mathcal{EP} , \mathcal{SWP} ,pour Π_2 ,alors il existe un algorithme les résolvant dans Π_1 .Puisque les générateurs de Π_1 ,sont en nombre fini il existe un algorithme changeant un mot de Π_1 ,en un mot de Π_2 (Il suffit de se doter

d'une table de correspondance $\alpha_i \longleftrightarrow \alpha_j$, et alors puisque ces éléments représentent le même élément de groupe, et que la validité des propriétés (être trivial, conjugué d'un élément ...) ne dépend pas de la présentation, pour des mots w de Π_1 , on détermine leur écriture dans Π_2 , et puisque l'on peut alors décider de tous les problèmes dans Π_2 , on le peut aussi dans Π_1 .

De façon similaire on peut voir que si des algorithmes existent pour Π_1 , alors il en est de même pour Π_2 . ■

Les algorithmes en question ne sont pas donnés constructivement, c'est à dire que si l'on se dote d'un algorithme résolvant, par exemple, le problème du mot pour une présentation récursive d'un groupe G donné, alors on sait qu'il existe un tel algorithme pour toute présentation récursive de G , mais on ne sait en général pas l'explicitier. En fait la constructivité de cet algorithme est réductible à la constructivité d'un isomorphisme donné explicitement, c'est à dire par l'image des générateurs (et inversement).

Dans la classe des présentations finies, le corollaire I.2.2 nous permet étant données deux présentations, de construire un tel isomorphisme. On a ainsi un résultat plus fort :

LEMME I.3.2 : Si l'on dispose d'un algorithme pour résoudre le problème du mot généralisé (resp^l du mot, de la conjugaison), pour une présentation finie d'un groupe G , alors on peut construire un tel algorithme pour toute présentation finie de G .

Ainsi l'on peut parler pour un groupe G f.p. (ou rec.p.) de $WP(G)$, $EP(G)$, $GWPC(G)$. Dans la suite nous parlerons de ces problèmes pour des classes particulières de groupe f.p. Lorsque l'on donnera explicitement un algorithme, on le donnera pour une présentation finie canonique d'un groupe; un algorithme pourra alors être construit pour chaque présentation finie de ce groupe, grâce aux algorithmes donnés dans le corollaire I.2.2 et le lemme I.3.1. Ces algorithmes ne sont néanmoins pas effectifs.

Définition : On dit d'une propriété de groupe qu'elle est héréditaire dans une classe de groupe C , lorsque si un groupe de C vérifie cette propriété, il en est de même de tous ses

sous-groupes qui appartiennent à C .

LEMME I.3.3 : Avoir un problème du mot résoluble est une propriété héréditaire dans la classe des groupes récursivement présentés.

Démonstration : Etant données deux groupes H et G par une présentation récursive, tel que H est un sous-groupe de G , alors il existe une application injective qui envoie les générateurs de H , sur des mots de G . Le noyau de cette application est trivial, et ainsi un mot de H est trivial ssi son image est trivial. Si le problème du mot est résoluble dans G , alors de même que pour le lemme I.3.1, il est résoluble dans H . ■

Remarque Le problème de la conjugaison, n'est pas héréditaire dans la classe des groupes récursivement présentés, comme nous le verrons dans la suite.

Définition : On dit d'une propriété de groupe P , que c'est une poly-propriété, si pour tout groupe G , tout sous-groupe normal de G , N , si N et G/N vérifient P , alors il en est de même de G .

Hall a démontré, qu'être finiment présenté, est une poly-propriété.

Lemme I.3.5 : être finiment présenté, et avoir un problème du mot soluble est une poly-propriété.

Démonstration : Considérons un sous-groupe normal N de G . Si N et G/N sont finiment présentés, il en est de même de G (Hall). On considère le plongement naturel $\Pi : G \longrightarrow G/N$. Etant donnée une présentation finie $\langle S \mid R \rangle$ de G , on peut prendre une présentation finie (proposition I.1.3) de G/N ayant pour générateurs les images par Π des éléments de S , et une présentation finie de N où les générateurs sont des mots sur S . De plus d'après le lemme I.3.2, la résolution du problème du mot, est indépendante de la présentation. Supposons que N et G/N aient un problème du mot soluble.

Etant donné un mot ω sur S , $\omega =_G 1$ ssi $\Pi(\omega) = 1$ dans G/N , et $\bar{\omega} = 1$ dans N . Pour décider si un mot $\omega = 1$ dans G , on teste si $\Pi(\omega) = 1$ dans G/N . Si ce n'est pas le cas, alors $\omega \neq_G 1$.

Si c'est le cas ,alors $\bar{\omega} \in N$.Puisque N est f.p. ,on peut énumérer tous les éléments de N ,et leurs écritures dans G (simplement ,en énumérant tous les mots de N ,et en leur appliquant toutes les transformations utilisant des éléments de R) .Alors on finit par trouver une écriture de $\bar{\omega}$ sur les générateurs de N .On peut alors décider si $\bar{\omega} =_N 1$,et donc si $\omega =_G 1$. ■

Remarque : En particulier toute extension d'un groupe ayant un problème du mot soluble ,par un groupe ayant un problème du mot soluble ,a un problème du mot soluble .(en particulier ,pour les produits directs ,et semi-directs (ou split extension)).

Avoir un problème du mot généralisé (resp^t de la conjugaison) ,soluble n'est pas une poly-propriété (Nous établiront en III.2 ,l'existence d'une split extension de 2 groupes ayant ces problèmes soluble ,pour laquelle ils ne sont pas solubles).

I.4 MACHINES DE TURING

Pour discuter de l'existence d'algorithme ,nous avons d'abord besoin de formaliser la notion intuitive d'algorithme .C'est ce que nous nous proposons de faire dans cette partie .

Un algorithme est un procédé permettant de décider pour des éléments donnés explicitement (par une suite finie de symbole ,de telle qu'un utilisateur ,peut pour chaque élément ,l'écrire sous sa forme explicite) ,s'ils vérifient ou non une certaine propriété ,c'est à dire s'ils appartiennent à un certain sous-ensemble de l'ensemble de ces éléments .L'existence de tels algorithmes ne dépend pas de la façon d'explicitier les éléments ,mais de la propriété étudiée .On dit intuitivement qu'une propriété (resp^t un ensemble) est calculable ,si l'on peut reconnaître grâce à un procédé mécanique (ou "machine") ,si un élément la vérifie (resp^t lui appartient) ,ou non .Cette notion de calculable a été formalisée dans les années 30 ,en la notion de récursivité ,par Turing ,Godel ,Church (...) de diverses façon qui sont toutes équivalentes .La thèse de Church affirme que la récursivité est une définition rigoureuse de la calculabilité

.Elle est vérifiée par l'expérience depuis plus de 50 ans ,on n'a encore jamais trouvé un ensemble qui soit calculable (au sens intuitif du terme) ,et qui ne soit pas récursif (On ne peut démontrer la thèse de Church ,puisque ce n'est pas une assertion mathématique) .

Nous utilisons la définition de Turing ,qui n'est pas la plus maniable ,mais qui dans notre cas sera la plus pratique .La théorie des fonctions récursives aurait ,par exemple ,été plus naturelle pour définir la notion de réducibilité .

Dans la suite nous continuerons à parler informellement d'algorithme .Par exemple on établira des algorithmes ,plutôt que de démontrer que l'ensemble en question est récursif .Ce serait un travail très laborieux ,et en fait la théorie ne sert qu'à démontrer qu'un problème de décision est **récursivement insoluble** ,i.e. qu'il n'existe pas d'algorithme permettant de décider (on emploiera aussi le terme **récursivement soluble**) .C'est la raison pour laquelle ,il a fallu attendre 1930 ,pour que ces notions apparaissent ,puisque l'on pensait avant les travaux de Gödel que des algorithmes existaient toujours .

Turing utilise des "machines" formelles idéales ,et élémentaires ,permettant (en principe) d'effectuer tout ce qu'une machine peut faire .De telles machines sont appelées machines de Turing .

Dans cette partie ,parallèlement au discours formel ,nous donnerons une interprétation intuitive des notions employées.

De façon informelle ,on peut se représenter une machine de turing comme une boîte ; composée d'une tête de lecture-écriture ,parcourant par une bande de longueur illimitée .La bande est constituée d'une suite de cases , chaque case contenant un symbole ,pris sur un alphabet fini $S=\{s_0, \dots, s_n\}$ (on considèrera que le symbole s_0 représente un "blanc").(c.f. fig.1).Les actions de la machine consistent à scanner une case ;lire ou écrire sur une case scanné ;déplacer sa tête de lecture sur la bande (de façons à scanner une autre case) .

La machine possède un nombre fini d'états q_0, q_1, \dots, q_m . A chaque instant, elle se trouve dans un état donné, sa tête de lecture-écriture positionnée sur une case de la bande. Son action est alors déterminée par sa structure initiale, son état, et le symbole scanné sur la case. La machine peut alors effectuer une des actions suivantes :

- (i) Remplacer le symbole scanné s par le symbole s' , et passer à l'état q' .
- (ii) Se déplacer d'une case vers la droite et passer à l'état q' .
- (iii) Se déplacer d'une case vers la gauche et passer à l'état q' .

où $s, s' \in S$; $q' \in \{q_0, \dots, q_m\}$.

La machine se trouve initialement à l'état q_1 , sa tête étant positionnée sur la première case, à gauche, non vide. Pour effectuer le calcul d'un mot w de \mathcal{G}^* (ensemble des mots sur l'alphabet \mathcal{G}), l'utilisateur fait démarrer la machine avec w inscrit sur la bande.

Dans la suite on considère $\mathcal{G} = \{s_0, \dots, s_n\}$ et $\mathcal{Q} = \{q_0, \dots, q_n\}$.

Définitions : Un Quadruple sur l'alphabet \mathcal{G} , et l'ensemble d'états \mathcal{Q} , est un 4-uplet d'une des formes suivantes

$$q \ s \ s' \ q'$$

$$q \ s \ R \ q'$$

$$q \ s \ L \ q' \quad \text{où } q, q' \in \mathcal{Q}, \ s, s' \in \mathcal{G}$$

On appelle préfixe d'un quadruple, le 2-uplet formé de ses 2 premiers éléments (q, s) .

Définition : Une machine de Turing, est un ensemble fini de quadruples sur un alphabet et un ensemble d'états ; tel que pour tout couple de quadruples, leur préfixe sont distincts (on dit qu'il n'y a pas d'ambiguïté).

Remarque Lorsque l'on parlera d'une machine T sur un alphabet \mathcal{S} et un ensemble d'état \mathcal{Q} , on prendra \mathcal{S} et \mathcal{Q} minimum, i.e tels que tout élément de $\mathcal{S} \cup \mathcal{Q}$ ait une occurrence dans un quadruple de T .

Informellement, le quadruple $q \ s \ s'q'$; (respectivement $q \ s \ R \ q'$, $q \ s \ L \ q'$) correspond à l'instruction : "lorsque l'état est q , le symbole lu est s ; effectuer l'action (i) (respectivement (ii), (iii)). Ainsi la définition d'une machine de Turing formelle, correspond informellement à ce que nous avons appelé structure initiale de la machine i.e., les règles déterminant les actions de la machine.

Définition : Une description instantanée est un mot sur $\mathcal{S} \cup \mathcal{Q}$ ayant exactement une occurrence d'un élément de \mathcal{Q} .

Une description instantanée $\alpha \equiv s_i \dots s_k q_l s_j \dots s_n$ doit être informellement interprétée comme "description instantanée" de la machine i.e., le mot inscrit sur la bande est $s_i \dots s_n$, l'état est q_l , le symbole lu est s_j (symbole se trouvant immédiatement à droite de q_l).

Définition : Considérons une machine de Turing T , α et β deux descriptions instantanées ; on dit que $\alpha \rightarrow \beta$ est un mouvement élémentaire si il existe P et Q mots sur \mathcal{S} (éventuellement vides), tel que l'on a une des conditions suivantes :

$$(i) \quad \begin{cases} \alpha \equiv P \ q_i s_j \ Q \\ \beta \equiv P \ q_l s_k \ Q \end{cases} \quad \text{où } q_i s_j s_k q_l \in T$$

$$(ii) \quad \begin{cases} \alpha \equiv P \ q_i s_j s_k \ Q \\ \beta \equiv P \ s_j q_l s_k \ Q \end{cases} \quad \text{où } q_i s_j R q_l \in T$$

$$(iii) \quad \begin{cases} \alpha \equiv P \ q_i s_j \\ \beta \equiv P \ s_j q_l s_o \end{cases} \quad \text{où } q_i s_j R q_l \in T$$

$$(iv) \quad \begin{cases} \alpha \equiv P \ s_k q_l s_j \ Q \\ \beta \equiv P \ q_l s_k s_j \ Q \end{cases} \quad \text{où } q_i s_j L q_l \in T$$

$$(v) \quad \begin{cases} \alpha \equiv q_i s_j Q \\ \beta \equiv q_i s_o s_j Q \end{cases} \quad \text{où } q_i s_j L q_l \in T$$

Remarques On interprétera $\alpha \longrightarrow \beta$, comme une opération élémentaire de la machine .

Les cas (iii) et (v) formalisent la présence d'une bande infinie à droite et à gauche .

Etant donné qu'il n'y a jamais d'ambiguïté , $\alpha \longrightarrow \beta$ et $\alpha \longrightarrow \gamma \Rightarrow \beta = \gamma$.

Définitions : Un calcul de T est une suite finie de descriptions instantanées $\alpha_1, \dots, \alpha_n$ avec $\alpha_i \longrightarrow \alpha_{i+1}$ pour tout i de $\{1, \dots, n-1\}$, et tel que pour toute description instantanée δ , on n'a pas $\alpha_n \longrightarrow \delta$. α_1 (resp α_n) est alors appelé description initiale (resp terminale).

Soit ω un mot sur \mathcal{G} , on dit que $T(\omega)$ existe si il existe un calcul de T , avec pour description initiale , $q_1 \omega$.

Soit $e(T) = \left\{ \omega \in \mathcal{G}^* / T(\omega) \text{ existe} \right\}$. On dit que T énumère $e(T)$.

Définition : $E \subseteq \mathcal{G}^*$, est dit récursivement énumérable si il existe une machine de turing qui énumère E .

Définition : $E \subseteq \mathcal{G}^*$ est dit récursif si E et $\mathcal{G}^* \setminus E$ sont récursivement énumérables .

Si un ensemble E est récursif alors il existe un algorithme décidant pour un élément donné écrit sur \mathcal{G} s'il appartient à E . En effet il existe deux machine de Turing énumérant E , et ainsi on peut savoir pour un élément donné ω si il appartient à E ou non , simplement en énumérant E et $\mathcal{G}^* \setminus E$. Au bout d'un temps fini , ω sera listé , soit comme élément de E , soit comme élément de $\mathcal{G}^* \setminus E$

THESE DE CHURCH : La récursivité est une définition rigoureuse de la calculabilité .

On se donne une présentation finie Π de G , de famille génératrice S . Ainsi les problèmes de Dehn deviennent :

Problème du mot : $\langle \omega \in \mathcal{M}(S) / \omega =_G 1 \rangle$ est-il récursif ?

Problème de la conjugaison : $\langle \omega, v \in \mathcal{M}(S) / \exists h \in G ; h^{-1}\omega h = v \rangle$ est-il récursif ?

Problème du mot généralisé : pour chaque famille génératrice a_1, \dots, a_n , $\langle \omega \in \mathcal{M}(S) / \omega =_G \text{mot}(a_1, \dots, a_n) \rangle$ est-il récursif ?

Problème de l'isomorphisme : $\langle (\Pi, \Pi') / \text{gp}(\Pi) \cong \text{gp}(\Pi') \rangle$ est-il récursif ?

Nous avons déjà vu que l'on dispose d'un algorithme d'énumération, ce qui signifie avec la thèse de Church, que ces ensembles sont récursivement énumérables. Néanmoins pour un ensemble récursivement énumérable non récursif, on peut décider lorsqu'un élément est O.K., mais pas s'il ne l'est pas. En effet un tel ensemble est toujours infini (car sinon après énumération, on connaît tous les éléments qui ne le sont pas) tout ce que l'on peut faire c'est énumérer cet ensemble, et pour un élément qui ne sera jamais énuméré, l'utilisateur ne peut pas savoir s'il le sera un jour. De tels ensembles existent. Ce résultat est la source de tous les problèmes d'indécidabilité en Mathématiques.

Proposition I.4.1 : Il existe un ensemble récursivement énumérable, non récursif.

Pour une démonstration voir par exemple [35]

Proposition I.4.2 : L'intersection ou la réunion de deux ensembles récursivement énumérables (resp^t récursif) est r.e. (resp^t rec.).

Démonstration : La notion de r.e. et de récursif peut se formaliser par la théorie des fonctions récursives. Alors le résultat est trivial puisque :

$$\chi_{A \cap B} = \chi_A \cdot \chi_B, \text{ et } \chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B} \quad \blacksquare$$

Définition : On appelle état d'arrêt d'une machine T , tout état ayant une occurrence dans une description instantanée

terminale .

Le résultat suivant sera utile à la suite .

LEMME I.4.1 : Pour toute machine de Turing ,il existe une machine énumérant le même ensemble ,et dont tous les états d'arrêt sont q_0 .On dit alors que q_0 est l'état d'arrêt de la machine .

Démonstration : Remarquons qu'une machine de Turing s'arrête ,lorsque pour un état q est un symbole s ,il n'existe pas de quadruple ayant pour préfixe (q,s) .Pour de tels couples (q,s) contruisons une nouvelle machine d'ensemble d'état $Q \cup \{q_0\}$ et de même alphabet ,ayant même quadruples que T ,plus les quadruples $q s s q_0$,ils sont en nombre fini .De plus la machine a alors pour état d'arrêt q_0 . ■

Remarque : Pour formaliser la notion de présentation récursive ,on a besoin que R soit un ensemble de mots positifs .Mais étant donné une présentation de groupe ,on peut la transformer en une présentation ou les relateurs sont des mots positifs .Il suffit de rajouter des générateurs x_i ,et des relateurs $x_i = a_i^{-1}$,où les a_i sont les générateurs ,et changer dans les relateurs ,des occurrences de a_i^{-1} ,par x_i .

I.5 EXTENSIONS DE BRITTON ET HNN EXTENSIONS

Notations : Soient une présentation $G = \langle S \mid D \rangle$,des lettres t_1, \dots, t_n n'appartenant pas à S ,et des mots r_1, \dots, r_m ,sur $S \cup \{t_1, \dots, t_n\}$.On note $\langle S ; t_1, \dots, t_n \mid D ; r_1, \dots, r_m \rangle$,ou plus simplement $\langle G ; t_1, \dots, t_n \mid r_1, \dots, r_m \rangle$,la présentation suivante $\langle S \cup \{t_1, \dots, t_n\} \mid D \cup \{r_1, \dots, r_m\} \rangle$.Dans cette partie nous confondrons groupes et présentations de groupe .

Soient $E = \langle S \mid D \rangle$ une présentation ,et $V = \{1, \dots, n\}$ $I = \{1, \dots, m\}$.Une seconde présentation E^* ,a pour lettres stables $\{p_v ; v \in V\}$,et pour base E ,si :

$$E^* = \langle S ; p_v , v \in V \mid D ; p_{v(w)}^{-1} A_i p_{v(u)} = B_i , i \in I \rangle$$

où $v, w : I \longrightarrow V$,et A_i et B_i sont des mots sur S .

On note $p_y \simeq p_z$ ($y, z \in V$), si $p_y = p_z$, dans le groupe obtenu à en rajoutant les relateurs $s = 1$, $\forall s \in S$ à la présentation de E^* . \simeq est une relation d'équivalence sur $\langle p_v, v \in V \rangle$, qui induit une relation d'équivalence sur I . Soit $K(v) = \langle i \in I / p_i \simeq p_v \rangle$ ($v \in V$), classe d'équivalence de la relation induite sur I . $A(v)$ dénote le sous-groupe de E engendré par $\langle A(i), i \in K(v) \rangle$, $B(v)$ le sous-groupe de E engendré par $\langle B(i), i \in K(v) \rangle$. On dit que E^* (défini comme précédemment) satisfait la condition de l'isomorphisme généralisée (G.I.C), si pour tout $v \in V$, la fonction $\varphi : A(v) \longrightarrow B(v)$, telle que $\forall i \in I \quad \varphi(A(i)) = B(i)$, s'étend en un isomorphisme entre $A(v)$ et $B(v)$.

Définition : E^* est une extension de Britton de E si E^* a pour base E , pour lettres stables $\langle p_1, \dots, p_n \rangle$, et si E^* satisfait la condition de l'isomorphisme généralisé.

Remarque Dans ce cas les relateurs additionnels, sont appelés relateurs de l'extension.

Soient S et T , des mots sur S , et $y, z \in V$. On dit que $S p_y$ produit $p_z T$, si $S p_y$ peut être transformé en $p_z T$ par une suite d'opérations de la forme :

$$\begin{aligned} X A_i p_{z(i)} Y &\longrightarrow X p_{y(i)} Y \\ X A_i^{-1} p_{y(i)} Y &\longrightarrow X p_{z(i)} B_i^{-1} Y \end{aligned}$$

où X et Y sont des mots de S .

Théorème I.5.1 : (Lemme de Britton)

Soit E^* une extension de Britton de E , ayant pour lettres stables P . Alors

- (i) E est plongé dans E^* par l'inclusion sur les générateurs
- (ii) Si $w = 1$ dans E^* , alors w contient un sous-mot d'une des formes (1) $p_y^{-1} C p_z$ ou (2) $p_y C p_z^{-1}$; où $p \in P$ et C est un mot sur S (générateurs de E). Dans le cas (1) C est égal dans E à un mot $\mu(A_i) \in A(y)$, et $\mu(A_i) p_z$ produit $p_y \mu(B_i)$. Dans le cas (2), C est égal dans E à un mot $\mu(B_i) \in B(y)$, et $\mu(A_i) p_z$ produit $p_y \mu(B_i)$.

Remarque C'est le théorème fondamental de cette partie .Il est dû sous une forme simplifiée à J.L.Britton .

Démonstration : Soit $\langle a_v, v \in V \rangle$ le groupe libre engendré par les a_v . Dans cette démonstration nous noterons $\langle X \rangle_G$ le sous-groupe de G engendré par X .

On considère : $F = \langle a_v, v \in V \rangle * E$
 $G = \langle b_v, v \in V \rangle * E$

et les sous-groupes $M_v = \langle a_{y(i)}^{-1} A_i a_{z(i)} ; i \in K(v) \rangle_F$
 $N_v = \langle b_{y(i)} B_i b_{z(i)}^{-1} ; i \in K(v) \rangle_G$.

Alors $M_v = M_t$ ssi $K(v) = K(t)$. De plus $\langle M_v, M_t \rangle_F \cong M_v * M_t$ si $K(v) \neq K(t)$, et à M_v sinon ; et $\langle M_v, E \rangle_F \cong M_v * E$, et ce pour tout $v \in V$. Les considérations analogues sont valables pour N_v .

Puisque E^* vérifie G.I.C. , alors $M_v \cong N_v$, par l'isomorphisme canonique . Nous prenons $Y = \langle a_{y(i)}^{-1} A_i a_{z(i)} ; i \in I \rangle_F * E \leq F$

$$\text{et } Z = \langle b_{y(i)} B_i b_{z(i)}^{-1} ; i \in I \rangle_G * E \leq G$$

et alors $Y \cong Z$ en étendant les fonctions $E \rightarrow E$, et $M_v \rightarrow N_v \quad \forall v \in V$ (propriété des produits libres) , qui envoie $a_{y(i)}^{-1} A_i a_{z(i)}$, sur $b_{y(i)} B_i b_{z(i)}^{-1}$ pour tout i .

Considérons $\bar{E} = \langle S ; a_v, b_v, v \in V \mid D ; a_{y(i)}^{-1} A_i a_{z(i)} = b_{y(i)} B_i b_{z(i)}^{-1} ; i \in I \rangle$

Avec ce qui précède , il est clair que $\bar{E} = F_{Y=Z} * G$.
 L'application $S \rightarrow S$, et $p_v \rightarrow a_v b_v$, s'étend en un homomorphisme $E^* \rightarrow \bar{E}$, puisque les relateurs de E^* , sont envoyés sur les relateurs de \bar{E} . De plus il est injectif . Si si un mot $\omega(S, a_v, b_v)$ est trivial dans \bar{E} , il l'est aussi dans le groupe obtenu à partir de \bar{E} , en rajoutant les relations $b_v = 1 \quad \forall v \in V$. Or ce groupe est clairement isomorphe à E^* , avec $S \rightarrow S$, et $a_v \rightarrow p_v$ et si l'on compose ces deux homomorphismes on obtient l'identité . Ainsi ω^{-1} est trivial dans E^* . Ainsi puisque E se plonge dans \bar{E} , dans l'image de E^* , E est plongé dans E^* par l'inclusion sur les générateurs .

Considérons le mot ω intervenant dans le théorème . On peut prendre ω librement réduit .

$$\omega \equiv S_1 p_{v_1}^{\alpha_1} S_2 p_{v_2}^{\alpha_2} \dots S_{n-1} p_{v_n}^{\alpha_n} S_n$$

où $n \geq 1$, $\alpha_i \neq 0$, et les S_i sont des mots dans E .

Puisque $\omega = 1$ dans E^* , son image $\omega' \equiv S_1 (a_{v_1} b_{v_1})^{\alpha_1} \dots (a_{v_n} b_{v_n})^{\alpha_n}$, est égal à 1 dans \bar{E} . Or $a_i \in F \setminus Y$, $b_i \in G \setminus Z$, et les $S_i \in Y = Z$ donc le produit libre amalgamé $\bar{E} = F_{Y=Z}^* G$, ω' a une écriture unique sous forme normale. Et alors pour tout i seul un des cas suivants est possible :

(1) $\alpha_i < 0$, $\alpha_{i+1} > 0$ et $a_{v_i}^{-1} S_{i+1} a_{v_{i+1}} \in Y$.

(2) $\alpha_i > 0$, $\alpha_{i+1} < 0$ et $b_{v_i} S_{i+1} b_{v_{i+1}}^{-1} \in Z$.

Considérons le cas (1). Puisque Y est engendré par les $a_{y(i)}^{-1} A_i a_{z(i)}$, $i \in I$ et S , et que ces un produit libre, forcément $\exists v \in V$ tel que $a_{v_i}^{-1} S_{i+1} a_{v_{i+1}} \in M_v$ (puisque'il doit avoir une écriture sous forme normale de longueur 1 et que les réductions entre a_i ne peut se faire que pour des indices i du même $K(v)$). De plus $S_{i+1} = \mu(A_l)$ où $\forall l, A_l \in A(v)$. Nous avons alors :

$$a_{v_i}^{-1} S_{i+1} a_{v_{i+1}} = \prod_{j=1}^m a_{t_j}^{-1} A_{l_j}^{\varepsilon_j} a_{t_{j+1}}$$

$$\text{et} \quad \mu(A_l) = \prod_{j=1}^m A_{l_j}^{\varepsilon_j} \quad \text{avec } \varepsilon_j = \pm 1$$

et $a_{v_i} = a_{t_1}$, $a_{v_{i+1}} = a_{t_{m+1}}$, et les $a_{t_j}^{-1} A_{l_j}^{\varepsilon_j} a_{t_{j+1}}$ sont les générateurs de M_v ou leur inverse. De plus $K(v_i) = K(v_{i+1})$.

Donc ω' contient un sous-mot de la forme $b_{v_i}^{-1} a_{v_i}^{-1} \mu(A_l) a_{v_{i+1}} b_{v_{i+1}}$

où $\exists v, A_l \in A(v)$. Donc ω contient un sous-mot de la forme $p_{v_i}^{-1} \mu(A_l) p_{v_{i+1}}$.

Or dans E^* , nous avons $a_{v_i}^{-1} \mu(A_l) a_{v_{i+1}} = b_{v_i} \mu(B_l) b_{v_{i+1}}^{-1}$. De plus

$p_{v_i}^{-1} \mu(A_l) p_{v_{i+1}} = \mu(B_l)$, donc $\mu(A_l) p_{v_{i+1}}$ produit $p_{v_i} \mu(B_l)$. Ce qui

dans le cas (1), démontre la partie (1) du théorème. Dualelement, le cas (2) démontre la partie (2). ■

On note $E \leq E^*$, si E^* a pour base E , et si pour tout mot ω de E , $\omega = 1$ dans E , ssi $\omega = 1$ dans E^* .

Lemme I.5.1 : Si E^* est une extension de Britton ayant pour base E , alors $E \leq E^*$.

Démonstration : Le résultat est clair puisque (avec le théo. I.5.1) ,E est plongé naturellement dans E^* . ■

Considérons une extension de Britton ayant pour lettres stables P .Un sous-mot tel que dans le théorème I.5.1 ,est appelé un pinch .Si un mot contient un pinch ,on peut lui appliquer la réduction suivant :

$$\begin{aligned} \omega \equiv U p_y^{-1} C p_z V &= U p_y^{-1} \mu(A_i) p_z V \\ (\text{théo I.5.1 (1)}) &= U p_y^{-1} p_y \mu(B_i) V \\ &= U \mu(B_i) V \end{aligned}$$

Cette opération s'appelle extraction d'un pinch ,nous l'avons appliquée dans le cas (1) ,mais elle similaire dans l'autre cas .Une telle opération diminue le nombre d'occurrences de lettres stables dans un mot .

Un mot qui n'est pas égal à un mot ayant moins d'occurrences d'éléments de P ,est dit P-réduit .

Lemme I.5.2 : Un mot sur E^* ,extension de Britton ayant pour lettres stables P est P-réduit ssi ,on ne peut pas extraire un pinch .

Démonstration : La condition nécessaire est triviale ,puisque un pinch réduit le nombre d'occurrence d'éléments de P .

Prenons W ne contenant pas de pinchs ,et supposons que $W = U$ où U contient moins d'éléments de P que W .Si U n'en contient pas ,alors avec le théorème I.5.1 ,W contient un pinch ce qui est contradictoire ,sinon ,on peut considérer que U ne contient pas de pinch .Alors $W U^{-1}$,d'après le théorème I.5.1 contient un pinch ,qui est forcément à la jonction puisque W et U n'en contiennent pas .Ainsi de suite ,on retire toutes les occurrences d'éléments de P ,jusqu'à ce qu'il n'y en ait plus .Mais puisque tous les pinchs sont à la jonction ,on a retiré autant d'éléments de P dans W que dans U ,ce qui est contradictoire . ■

Définition : E^* est une HNN extension de E ,si E^* ,a pour base $E = \langle S / D \rangle$,pour lettres stables $P = \langle p_v , v \in V \rangle$,et si $E^* = \langle S ; p_v , v \in V / D ; p_{v(i)}^{-1} A_i p_{v(i)} = B_i , i \in I \rangle$,où I est fini ,V est fini A_i et B_i ,sont des mots sur S , $v : I \longrightarrow V$,et E^* satisfait C.I.G. .

Remarque Il est clair que les HNN extensions sont un cas particulier des extensions de Britton. En particulier tous les résultats démontrés pour les extensions de Britton sont valables pour les HNN extensions.

Dans ce cas $p_y \cong p_z$, si et seulement si $p_y = p_z$. La condition de l'isomorphisme généralisé s'appelle alors condition de l'isomorphisme. Le théorème I.5.1 devient le *lemme de Britton*.

Les HNN extensions sont aussi appelées extensions forte de Britton.

Lemme I.5.3 : Si E^* est une HNN extension de E , ayant pour lettres stables P , alors le sous-groupe de E^* engendré par P est libre sur P .

Démonstration : Soit F le groupe libre engendré par P . Considérons l'application $\varphi : E^* \longrightarrow F$ telle que $\varphi(p) = p$, $\varphi(s) = 1$; $\forall p \in P$, et $\forall s \in S$. Il est clair au vu des relateurs de E^* , que φ s'étend en un homomorphisme. Alors tout relateur sur P dans E^* , serait un relateur sur F , qui est libre. ■

Lemme I.5.4 : Soit E^* , HNN extension de E avec pour lettres stables, $P = \langle p_v, v \in V \rangle$. Soient deux mots U et V tels que, $U \equiv S_0 p_{v_1}^{\varepsilon_1} S_1 \dots S_{n-1} p_{v_n}^{\varepsilon_n} S_n$, et $V \equiv T_0 p_{w_1}^{\zeta_1} T_1 \dots T_{m-1} p_{w_m}^{\zeta_m} T_m$, sont deux mots P -réduits, tels que S_0, \dots, S_n et T_0, \dots, T_m sont des mots dans E ; $v_1, \dots, v_n, w_1, \dots, w_m \in V$; $\varepsilon_1, \dots, \varepsilon_n, \zeta_1, \dots, \zeta_m \in \langle -1; 1 \rangle$. Alors si $U = V$ dans E^* , $n = m$; $\forall i = 1 \dots n$, $v_i = w_i$, $\varepsilon_i = \zeta_i$, et de plus $p_{v_n}^{\varepsilon_n} S_n T_m^{-1} p_{w_m}^{-\zeta_m}$ est un pinch.

Démonstration : On a $U V^{-1} = 1$ dans E^* . Donc d'après le théorème I.5.1, il contient un pinch. Puisque U et V sont P -réduits, (lemme I.5.2), le pinch est $p_{v_n}^{\varepsilon_n} S_n T_m^{-1} p_{w_m}^{-\zeta_m}$, et donc $v_n = w_m$ et $\varepsilon_n = \zeta_m$. Le mot obtenu est encore trivial dans E^* . En appliquant le même raisonnement jusqu'à ce qu'il n'y ait plus d'occurrences d'éléments de P ; on a $n = m$ (puisque chaque extraction de pinch se fait à la jonction), $v_i = w_i$, et $\varepsilon_i = \zeta_i$. ■

CHAPITRE II :

THEOREMES GENERAUX D'INSOLUBILITE

Dans cette partie nous démontrons que tous les problèmes de Dehn ,sont en général insolubles pour des groupes finiment présentés .

Les deux premières parties sont consacrées au problème du mot . Dans la première partie nous démontrons le théorème de Post ,i.e. il existe un semi-groupe finiment présenté ayant un problème du mot récursivement insoluble . Pour établir ce résultat , nous construisant pour une machine de Turing quelconque , un semi-groupe f.p. associé , de telle façon que le problème d'arrêt de la machine de Turing , se réduise au problème du mot dans le semi-groupe . Dans la deuxième partie , nous utilisons ce résultat , pour établir l'existence d'un groupe f.p. ayant un problème du mot insoluble . Pour ce faire , nous construisons sur un semi groupe f.p. un groupe f.p. associé , et démontrons que le problème du mot du semi-groupe est réductible au problème du mot dans le groupe . La première démonstration de ce résultat est due à *P. Novikov* . Elle utilisait des arguments combinatoire . *W.W. Boone* a établi un lemme , raccourcissant considérablement la démonstration initiale . La démonstration que , nous donnons , est due essentiellement à *S. Aandera* . Il utilise le fait établi par *J.L. Britton* que ce groupe est le résultat d'une suite de HNN extensions sur le groupe cyclique infini . L'utilisation du lemme de Britton permet de remplacer l'argument combinatoire , par un argument de théorie des groupes . Sa démonstration se prolonge , en une démonstration du théorème de Higman . C'est cette démonstration que nous établissons dans la troisième partie . (ainsi que le théorème de Higman-Neumann -Neumann) . L'utilisation des théorèmes de plongements établis dans la troisième partie , est omni-présente , dans la suite de notre propos

Dans la quatrième partie nous établissons simplement , en utilisant le théorème de Novikov , le théorème de Adjan-Rabin . Sa démonstration utilise un lemme technique , simple à établir , dû à

C.F. Miller III ,qui pourrait certainement avoir beaucoup d'autres intérêts en théorie des groupes (nous l'utilisons aussi pour établir le théorème de Higman-Neumann-Neumann) .

Nous montrons que non seulement le problème de l'isomorphisme est insolubles mais qu'un grand nombre d'autres problèmes de décisions globaux sont insolubles .

Cette partie établit l'insolubilité de tous les problèmes de Dehn ,en général ,mais ne donne explicitement aucune présentation de groupe ayant un problème insoluble .

II.1 THEOREME DE POST

De façon similaire à ce que nous avons vu en I.1 ,on peut se donner un semi-groupe par la donnée d'une présentation :

$$\Gamma = \langle X \mid A_i = B_i \quad i \in I \rangle .$$

Deux mots sur X , ω et ξ , représentent le même élément de Γ s'il y a une suite finie finie d'opérations élémentaires de ω à ξ

$$\text{i.e} \quad \omega \equiv W_1 \longrightarrow W_2 \longrightarrow \dots W_k \longrightarrow W_{k+1} \dots \longrightarrow W_n \equiv \xi$$

où l'on écrit $W_k \longrightarrow W_{k+1}$ si il existe P et Q , mots sur S (éventuellement vides); tel que l'on a une des conditions suivantes :

$$\begin{array}{l} W_k \equiv P A_i Q \quad \text{et} \quad W_{k+1} \equiv P B_i Q \\ \text{ou} \quad W_k \equiv P B_i Q \quad \text{et} \quad W_{k+1} \equiv P A_i Q \quad ; \quad i \in I . \end{array}$$

Le problème du mot se généralise aux semi-groupes .C'est par contre faux pour le problème de la conjugaison .

Le problème du mot est "plus simple" pour un semi-groupe que pour un groupe . Nous allons néanmoins démontrer qu'il existe un semi-groupe finiment présenté ,pour lequel le problème du mot est récursivement insoluble .Intuitivement ,la méthode va consister à construire un semi-groupe "simulant" une machine de turing ; i.e on va établir des analogies entre opérations élémentaires du semi-groupe et mouvements élémentaires de la machine ,de sorte que le problème d'arrêt de la machine se réduise au problème du mot du semi-groupe.Dans la suite nous préciseront plus clairement ces analogies .

On considère une machine de Turing T , sur un alphabet $\mathcal{G} = \{s_0, \dots, s_n\}$ et un ensemble d'états $\mathcal{Q} = \{q_0, \dots, q_m\}$. On lui "associe" un semi-groupe $\Gamma(T)$ par la donnée d'une présentation :

Générateurs : $s_0, \dots, s_n, q_0, \dots, q_m, q, h$.

Relateurs : (i) $\left\{ \begin{array}{l} q_i s_j = q_l s_k \end{array} \right.$ pour $q_i s_j s_k q_l \in T$

$\forall s_k \in \mathcal{G}$ (ii) $\left\{ \begin{array}{l} q_i s_j s_k = s_j q_l s_k \\ q_i s_j h = s_j q_l s_0 h \end{array} \right.$ pour $q_i s_j R q_l \in T$

$\forall s_k \in \mathcal{G}$ (iii) $\left\{ \begin{array}{l} s_k q_i s_j = q_l s_k s_j \\ h q_i s_j = h q_l s_0 s_j \end{array} \right.$ pour $q_i s_j L q_l \in T$

$\forall s_k \in \mathcal{G}$ (iv) $\left\{ \begin{array}{l} q_0 s_k = q_0 \\ s_k q_0 h = q_0 h \end{array} \right.$

(v) $\left\{ \begin{array}{l} h q_0 h = q \end{array} \right.$

Intuitivement Les relateurs (i), (ii), (iii) reproduisent les actions de T . La lettre h représente les extrémités des mots sur la bande. Par abus de langage on emploiera la terminologie de "description instantanée" pour des mots de $\Gamma(T)$. Un mot de la forme $h \omega h$ où ω est une description instantanée est alors analogue de la description instantanée ω pour T . Les relations (iv) et (v) établissent q comme analogue de l'état d'arrêt de T .

Definition : On dit qu'un mot de $\Gamma(T)$ est *h-spécial* si il est de la forme $h P h$ où P est une description instantanée.

Lemme II.1.1 : Soit T une machine de turing ,et $\Gamma(T)$ son semi-groupe associé .Considérons U et V ,deux mots de $\Gamma(T)$.

(i) Si $U \not\equiv q$,et $V \not\equiv q$,et $U \longrightarrow V$ est une opération élémentaire ,alors U est h-spécial ssi V est h-spécial .

(ii) Si $U \equiv h \alpha h$ et U est h-spécial ,et $V \not\equiv q$ et $U \longrightarrow V$ est une opération élémentaire utilisant un

relateur de la forme (i) , (ii) , ou (iii) , alors $V \equiv h \beta h$ et soit $\alpha \rightarrow \beta$, soit $\beta \rightarrow \alpha$ est un mouvement élémentaire de T .

Démonstration : (i) la seule relation qui transforme un mot h-spécial, en un mot qui n'est pas h-spécial est $h q_0 h = q$.

Avec U et V $\neq q$ le résultat est clair . \square

(ii) Avec ces hypothèses , (i) \Rightarrow V est h-spécial soit que $V \equiv h \beta h$, où β est une description instantanée

On peut alors considérer que $\alpha \equiv P A_i Q$ et $\beta \equiv P B_i Q$ où soit $h A_i = B_i$, soit $A_i = B_i h$, soit $A_i = B_i$ est un relateur , et donc on passe de α à β par un relateur de la forme , (i) (ii) ou (iii) . Donc puisque les relateurs de cette forme correspondent à des quadruples de T , il aisé d'établir que soit $\alpha \rightarrow \beta$, soit $\beta \rightarrow \alpha$ est un mouvement élémentaire de T \blacksquare

Le lemme suivant établit ce que nous entendions par " $\Gamma(T)$ simule la machine T " .

Lemme II.1.2 : Soit T une machine de turing avec pour état d'arrêt q_0 . Soit E l'ensemble énuméré par T ; et ω un mot sur l'alphabet de T .

$$\omega \in E \iff h q_1 \omega h = q \text{ dans } \Gamma(T) .$$

Démonstration : (\Leftarrow) Supposons que $h q_1 \omega h = q$. Alors il existe une suite d'opérations élémentaires :

$$h q_1 \omega h \equiv W_1 \longrightarrow \dots \longrightarrow W_n \equiv q .$$

Remarquons que si W_i est h-spécial et $W_i \longrightarrow W_{i+1}$ est une opération élémentaire ; alors si W_i n'a pas d'occurrence de q_0 , $W_{i+1} \neq q$. En effet , W_i est h-spécial , et pour "tuer" les h il faut utiliser le relateur (v) , ce qui n'est possible qu'avec une occurrence de q_0 .

Un des éléments de la suite , a donc une occurrence de q_0 . Prenons W_k , le premier élément ayant une occurrence de q_0 ($k \geq 2$) . Posons $\forall i \in \{1, \dots, k-1\}$, $W_i \equiv h \alpha_i$. Aucun α_i n'ayant d'occurrence de q_0 , les relateurs utilisés sont d'une des formes (i) , (ii) ou (iii) . Alors , avec le lemme II.1.1 (ii) , soit $\alpha_i \rightarrow \alpha_{i+1}$ soit $\alpha_{i+1} \rightarrow \alpha_i$, est un déplacement élémentaire . Le problème consiste à

démontrer que le sens de déplacement est de gauche à droite (alors qu'une opération élémentaire est symétrique, un déplacement élémentaire ne l'est pas). q_0 est l'état d'arrêt de la machine, d'où $\alpha_{k-1} \rightarrow \alpha_k$ est un déplacement élémentaire.

Si $k = 2$, alors $\alpha_1 \rightarrow \alpha_2$ est un calcul de T ; dans ce cas on a bien $\omega \in E$.

Si $k \geq 2$, alors soit $\alpha_1 \rightarrow \alpha_2 \dots \rightarrow \alpha_k$ est une suite de déplacements élémentaires, et dans ce cas un calcul de ω dans T (i.e. $\omega \in T$); soit il existe i tel que $\alpha_{i-1} \leftarrow \alpha_i \rightarrow \alpha_{i+1}$. Etant donné qu'une machine de Turing n'a jamais d'ambiguïté quand à son déplacement, on a nécessairement $\alpha_{i-1} = \alpha_{i+1}$, on peut alors raccourcir la suite, tout en gardant les mêmes hypothèses. En procédant par induction, on peut donc se ramener à la suite $\alpha_1 \rightarrow \dots \rightarrow \alpha_k$, et donc $\omega \in E$. \square

(\Rightarrow) Si $\omega \in E$, alors on a dans T une suite de déplacements élémentaires :

$$q_1 \omega \rightarrow \dots \rightarrow X q_0 Y$$

où X et Y sont des mots sur l'alphabet de T . Alors on a la suite d'opérations élémentaires dans $\Gamma(T)$:

$$h q_1 \omega h \rightarrow \dots \rightarrow h X q_0 Y h \quad (1)$$

En utilisant la relation $q_0 s_b = q_0$ on peut construire la suite

$$h X q_0 Y h \rightarrow \dots \rightarrow h X q_0 h \quad (2)$$

, avec la relation $s_b q_0 h = q_0 h$, on peut construire la suite

$$h X q_0 h \rightarrow h q_0 h \quad (3)$$

; et ce, car X et Y sont des mots sur $\mathcal{Q} = \{s_1, \dots, s_n\}$. Finalement avec (1), (2), (3) et le relateur (v) on construit la suite d'opérations élémentaires :

$$h q_1 \omega h \rightarrow \dots \rightarrow h X q_0 Y h \rightarrow \dots \rightarrow h X q_0 h \rightarrow h q_0 h \rightarrow q$$

, et donc $h q_1 \omega h = q$ dans $\Gamma(T)$. \blacksquare

Théorème I.1.1 : (Post)

Il existe un semi-groupe finiment présenté, Γ ayant un problème du mot insoluble récursivement insoluble.

$$\Gamma = \Gamma(T^*) = \langle q, h, s_0, \dots, s_n, q_0, \dots, q_m \mid R(T^*) \rangle$$

Il n'existe pas d'algorithme permettant de décider pour un mot h -spécial hwh , si $hwh = q$.

Démonstration : Il existe un ensemble E , récursivement énumérable, non récursif. Soit T^* la machine de Turing qui l'énumère. On construit $\Gamma(T^*)$ comme précédemment. Soit W l'ensemble des mots sur \mathcal{G} , \tilde{W} l'ensemble des mots de Γ .

Considérons l'ensemble $V = \{v \in \tilde{W} \mid v \equiv h q_1 \alpha h \text{ où } \alpha \in W\}$

V est clairement récursif (Théorie des fonctions récursives).

Si Γ a un problème du mot résoluble, alors $U = \{u \in \tilde{W} \mid u = q\}$ est récursif.

Considérons $\tilde{E} = \{h q_1 \alpha h \mid \alpha \in E\}$. \tilde{E} est récursif ssi E est récursif. Or $\tilde{E} = U \cap V$ est donc récursif puisque intersection d'ensembles récursifs, ce qui contredit l'hypothèse ■

Nous avons démontré que le problème du mot dans le problème d'arrêt de T est réductible au problème du mot de $\Gamma(T)$. W.W. Boone démontre dans [4], que la réciproque est vraie, et il établit ainsi le résultat :

Théorème I.1.2 : (Boone)

Pour tout degré D d'insolubilité, il existe un semi-groupe f.p., ayant un problème du mot de degré D .

II.2 THEOREME DE NOVIKOV-BOONE

Dans cette partie, nous allons démontrer le théorème suivant.

Théorème II.2.1 : (Novikov-Boone)

Il existe un groupe finiment présenté, ayant un problème du mot insoluble.

Il est clair que puisque le problème du mot est réductible au problème de la conjugaison, et au problème du mot généralisé, on a le corollaire suivant du théorème de Novikov-Boone :

Corollaire I.2.1.1 : Il existe un groupe f.p. ayant un problème du mot, un problème de la conjugaison, un

problème du mot généralisé ,récursivement insolubles

Nous n'aurons plus besoin de faire référence aux machines de Turing . Le résultat qui nous sera utile est le corollaire suivant du théorème de Post .

Proposition II.2.1 : Il existe un semi-groupe finiment présenté

$$\Gamma = \langle q, q_1, \dots, q_N, s_1, \dots, s_M \mid F_i q_{v(i)} G_i = H_i q_{v(i)} K_i \rangle$$

; où $I \ni i$ est fini ; $q_{v(i)}, q_{v(i)} \in \langle q, q_1, \dots, q_N \rangle$; et F_i, G_i, H_i, K_i sont des mots sur $\langle s_1, \dots, s_M \rangle$; ayant un problème du mot récursivement insoluble .

Démonstration : Considérons le semi-groupe $\Gamma(T^*)$, du théorème de Post . Renumerotons $\langle q_0, \dots, q_m \rangle$ en $\langle q_1, \dots, q_N \rangle$; $\langle s_0, \dots, s_n \rangle$ en $\langle s_1, \dots, s_{M-1} \rangle$ et posons $s_M \equiv h$. On a alors la présentation donnée ci-dessus . Le theo. I.1.1 nous permet de conclure ■

Notations :

Soit $X \equiv s_1^{\zeta_1} \dots s_m^{\zeta_m}$ un mot sur $\langle s_1, \dots, s_M \rangle$. Dans ce paragraphe on notera \bar{X} le mot $\bar{X} \equiv s_1^{-\zeta_1} \dots s_m^{-\zeta_m}$.

Soient X et Y des mots sur $\langle s_1, \dots, s_M \rangle$, on note :

$$(X q_j Y)^* \equiv \bar{X} q_j Y$$

où $q_j \in \langle q, q_1, \dots, q_N \rangle$.

Un mot Σ est dit spécial , si $\Sigma \equiv \bar{X} q_j Y$, où X et Y sont des mots positifs sur $\langle s_1, \dots, s_M \rangle$.

Nous allons construire sur Γ (i.e en faisant référence à la présentation de Γ) , un groupe de présentation finie . Nous verrons que ce groupe est le résultat d'une chaîne de Britton sur le groupe cyclique infini , et qu'il a un problème du mot récursivement insoluble .

On considère le groupe finiment présenté , $G = G(T)$:

Générateurs : $q, q_1, \dots, q_N, s_1, \dots, s_M, r_i (i \in I), x, t, k$

Relateurs :

$$\begin{aligned} x s_b &= s_b x^2 & \Delta_1 & \Delta_2 & \Delta_3 \\ r_i s_b &= s_b x r_i x \end{aligned}$$

$$r_i^{-1} \bar{F}_i q_{i_1} G_i r_i = \bar{H}_i q_{i_2} K_i$$

$$t r_i = r_i t$$

$$t x = x t$$

$$k r_i = r_i k$$

$$k x = x k$$

$$k (q^{-1} t q) = (q^{-1} t q) k$$

$$\text{où } s_b \in \langle s_1, \dots, s_M \rangle \text{ et } i_1 = v(i), i_2 = w(i)$$

Lemme II.2.1 : (Boone)

Si Σ est un mot spécial alors $k(\Sigma^{-1} t \Sigma) = (\Sigma^{-1} t \Sigma) k$
dans G ssi $\Sigma^* = q$ dans Γ .

Le lemme de Boone nous permet de conclure : si l'on a un algorithme pour résoudre le problème du mot dans G , alors $\forall \Sigma$ mot spécial sur $\langle s_1, \dots, s_M \rangle$, on peut décider si $\Sigma^* = q$ dans Γ , (i.e $\forall X$ et Y mots positifs sur $\langle s_1, \dots, s_M \rangle$, $\forall q_j \in \langle q, q_1, \dots, q_m \rangle$, on peut décider si $X q_j Y = q$ dans Γ); ce qui contredit le théorème de Post.

L'objectif de cette partie est de démontrer ce résultat. Cette démonstration sera effectuée en plusieurs étapes. Commençons par démontrer la condition suffisante.

Démonstration de la condition suffisante du lemme de Boone :

Nous commençons par établir quelques propriétés de G . Soit V un mot positif sur $\langle s_1, \dots, s_M \rangle$. Alors $\forall i \in I$, $r_i V = V R$ dans G où R est un mot (positif) sur $\langle x, r_i (i \in I) \rangle$.

Nous prouvons ce résultat, par induction sur la longueur m de $V \equiv s_{\alpha_1} \dots s_{\alpha_m}$.

Si $m = 0$ alors la propriété est vraie, avec $R = r_i$.

Supposons que la propriété soit vraie pour $m > 0$.

On a alors $r_i V = V R$ pour tout $i \in I$ et tout mot V , de longueur m sur $\langle s_1, \dots, s_M \rangle$.

Prenons $s_{\alpha_{m+1}} \in \langle s_1, \dots, s_M \rangle$, et $V' \equiv V s_{\alpha_{m+1}}$

Alors $r_i V' \equiv r_i V s_{\alpha_{m+1}} = V R s_{\alpha_{m+1}}$

En utilisant les relations $x s_b = s_b x^2$ et $r_i s_b = s_b x r_i x$, R étant

un mot sur x et r_i , on a $V R s_{\alpha m+1} = V s_{\alpha m+1} R'$
 $= V' R'$

; où R' est un mot (positif) sur $\langle x, r_i (i \in I) \rangle \dots$ C.Q.F.D.

En considérant $U \equiv s_{\alpha m+1} \dots s_1$ on a $\bar{U} = V^{-1}$, et alors, on a

$$\bar{U} r_i^{-1} = V^{-1} r_i^{-1} = (r_i V)^{-1} = (V R)^{-1} = R^{-1} V^{-1} = R^{-1} \bar{U}$$

i.e $\forall U$ mot positif sur S , $\forall i \in I$, $\exists L$ mot sur x, r_i ($i \in I$), tel que $\bar{U} r_i^{-1} = L \bar{U}$ dans G .

Ces considérations seront utiles dans la suite de la démonstration

Supposons que $\Sigma^* = q$ dans Γ où Σ est un mot spécial
on a dans Γ , la suite d'opérations élémentaires :

$$\Sigma^* \equiv W_1 \longrightarrow \dots W_j \longrightarrow W_{j+1} \dots \longrightarrow W_n \equiv q$$

avec $W_j \equiv U F_i q_{i1} G_i V$ et $W_{j+1} \equiv U H_i q_{i2} K_i V$ (ou inversement), où U et V sont des mots positifs sur $\langle s_1, \dots, s_M \rangle$.

Dans G nous avons les égalités suivantes :

$$\bar{U} (\bar{H}_i q_{i2} K_i) V = \bar{U} (r_i^{-1} \bar{F}_i q_{i1} G_i r_i) V = L \bar{U} \bar{F}_i q_{i1} G_i V R$$

où L et R sont des mots sur $\langle x, r_i (i \in I) \rangle$.

On a donc $\forall j \in \langle 1, \dots, n-1 \rangle$, $W_j^* = L W_{j+1}^* R$ ou $W_{j+1}^* = L W_j^* R$ dans G .

Donc $\forall j \in \langle 1, \dots, n-1 \rangle$, $\exists L_j$ et R_j mots sur $x, r_i (i \in I)$, tel que, $W_j^* = L_j W_{j+1}^* R_j$ dans G .

En posant $L = L_1 L_2 \dots L_{n-1}$, et $R = R_{n-1} \dots R_2 R_1$, on a dans G , l'égalité :

$$W_1^* = L W_n^* R$$

où L et R sont des mots sur $\langle x, r_i (i \in I) \rangle$.

Or $W_1^* \equiv (\Sigma^*)^* \equiv \Sigma$, et $W_n^* \equiv q^* \equiv q$, donc dans G , on l'égalité :

$$\Sigma = L q R$$

Donc si Σ est spécial, et $\Sigma^* = q$ dans Γ , alors $\Sigma = L q R$ dans G

Avant de poursuivre, remarquons que les relations, $k r_i = r_i k$, $k x = x k$; et $t r_i = r_i t$, $t x = x t$, assurent que k et t commutent avec les mots sur $\langle x, r_i (i \in I) \rangle$.

$$\begin{aligned} \text{Avec tout ce qui précède } (\Sigma^{-1} t \Sigma) k &\equiv R^{-1} q^{-1} L^{-1} t L q R k \\ &= R^{-1} q^{-1} L^{-1} L t q k R \\ &= R^{-1} (q^{-1} t q) k R \\ &= R^{-1} k (q^{-1} t q) R \end{aligned}$$

$$\begin{aligned}
&= k R^{-1} q^{-1} L^{-1} L t R \\
&= k R^{-1} q^{-1} L^{-1} t L q R \\
&= k (\Sigma^{-1} t \Sigma) \quad \blacksquare
\end{aligned}$$

Nous allons maintenant démontrer la condition nécessaire du lemme de Boone. Nous allons pour cela procéder en plusieurs étapes.

Considérons les groupes suivants :

$$\begin{aligned}
G_0 &= \langle x \rangle \\
G_1 &= \langle G_0 ; s_1, \dots, s_M \mid \text{relations } \Delta_1 \rangle \\
G_2 &= \langle G_1 ; q, q_1, \dots, q_N, r_i (i \in I) \mid \text{relations } \Delta_2 \rangle \\
G_3 &= \langle G_2 ; t \mid \text{relations } \Delta_3 \rangle
\end{aligned}$$

Dans la suite nous noterons $\langle u_1, u_2, \dots \rangle_i$, au lieu de $\langle u_1, u_2, \dots \rangle_{G_i}$, pour désigner le sous-groupe de G_i ($i = 0, 1, \dots, 3$), engendré par u_1, u_2, \dots .

Lemme II.2.2 : (i) G_1 est une HNN extension de G_0 ayant pour lettres stables $\langle s_1, \dots, s_M \rangle$.

(ii) $G_1 * \langle q, q_1, \dots, q_N \rangle$ est une HNN extension de G_1 ayant pour lettres stables $\langle q, q_1, \dots, q_N \rangle$.

(iii) G_2 est une HNN extension de $G_1 * \langle q, q_1, \dots, q_N \rangle$ ayant pour lettres stables $\langle r_i (i \in I) \rangle$.

(iv) G_3 est une HNN extension de G_2 ayant pour lettre stable $\langle t \rangle$.

(v) G est une HNN extension de G_3 ayant pour lettre stable $\langle k \rangle$.

Démonstration : (i) G_1 a pour base G_0 , pour lettres stables $\langle s_1, \dots, s_M \rangle$. Les relateurs de l'extension sont $\forall b \in \langle 1, \dots, M \rangle$ $s_b^{-1} x s_b = x^2$. Il faut vérifier qu'il existe un isomorphisme Ψ tel que $\Psi : \langle x \rangle_0 \rightarrow \langle x^2 \rangle_0$ et $\Psi(x) = x^2$.

Or G_0 est libre, donc ces deux sous-groupes sont cycliques infinis, et il existe donc un tel isomorphisme. \square

(ii) Le résultat est trivial en considérant les relateurs de l'extension $q_a^{-1} q_a = 1$ où $q_a \in \langle q, q_1, \dots, q_N \rangle$. \square

(iii) G_2 a pour base $G_1 * \langle q, q_1, \dots, q_N \rangle$, et pour lettres stables $\langle r_i (i \in I) \rangle$. Il faut vérifier que les sous-groupes de $G_1 * \langle q, q_1, \dots, q_N \rangle$, $A(i)$ engendré par les éléments $(\bar{F}_i q_{i1} G_i, s_b x)$, et $B(i)$ engendré par les éléments $(\bar{H}_i q_{i2} K_i, s_b x^{-1})$ ($b = 1..m$), sont isomorphes $\forall i \in I$, et que cet isomorphisme envoie les générateurs respectifs de $A(i)$, sur les générateurs respectifs de $B(i)$. Or ces sous-groupes sont libres sur leurs générateurs. En effet considérons une application de $F(q_{i1}, s_1, \dots, s_M, x)$ dans $F(q_{i1}, s_1, \dots, s_M)$, qui envoie q_{i1} sur q_{i1} , s_i sur s_i , et x sur 1. Au vu des relateurs, cette application s'étend sur $A(i)$, et l'image d'un mot non vide est un mot non vide. Donc l'application est injective, de plus elle est surjective, donc $A(i)$ est un groupe libre de rang $M + 2$, et est donc libre sur ses générateurs. Il en est de même de $B(i)$. On a donc un isomorphisme de $A(i)$ dans $B(i)$, qui envoie $s_1 x$ sur $s_1 x^{-1}$ etc... \square

(iv) G_3 a pour base G_2 et pour lettre stable $\langle t \rangle$. Avec pour relations de l'extension $t^{-1} r_i t = r_i$ et $t^{-1} x t = x$, A et B sont tout deux engendrés par $\langle x, r_i (i \in I) \rangle$ on vérifie donc la condition de l'isomorphisme (considérer l'identité). \square

(v) G a pour base G_3 , pour lettre stable k . Les relateurs de l'extension sont : $k^{-1} r_i k = r_i$, $k^{-1} x k = x$, $k^{-1} (q^{-1} t q) k = q^{-1} t q$, et on a donc comme précédemment la condition de l'isomorphisme. \blacksquare

Lemme II.2.3 : Soit Σ un mot spécial vérifiant les hypothèses du lemme de Boone.

$$\text{i.e. } k (\Sigma^{-1} t \Sigma) = (\Sigma^{-1} t \Sigma) k \quad \text{dans } G.$$

Alors il existe L_1 et L_2 , mots sur $\langle x, r_i (i \in I) \rangle$ tel que $L_1 \Sigma L_2 = q$ dans G_2 .

Démonstration : On a $k \Sigma^{-1} t \Sigma k^{-1} \Sigma^{-1} t^{-1} \Sigma = 1$ dans G , HNN extension de G_3 avec pour lettre stable $\langle k \rangle$, et donc contient un pinch. Σ n'a pas d'occurrences de k , donc le pinch est $k \Sigma^{-1} t \Sigma k^{-1}$. D'après le théorème I.5.1, $\Sigma^{-1} t \Sigma = C$ dans G_3 , où C est un mot sur $x, r_i (i \in I)$. $q^{-1} t q$ (le théorème I.5.1, nous dit que l'élément de G_3 représenté par $\Sigma^{-1} t \Sigma$ est dans le sous-groupe de

G_9 engendré par $x, r_i (i \in I), q^{-1}tq$.

On a alors $\Sigma^{-1}t \Sigma C^{-1} = 1$ dans G_9 et peut donc s'écrire :

$$W \equiv \Sigma^{-1}t \Sigma R_0 (q^{-1}t^{e_1}q) R_1 (q^{-1}t^{e_2}q) R_2 \dots (q^{-1}t^{e_m}q) R_m = 1$$

, dans G_9 où les R_i sont des mots sur $\langle x, r_i (i \in I) \rangle$ (event.^l vides) ; et $e_j = \pm 1$.

Nous pouvons prendre m minimal, ce qui revient à considérer une écriture minimale de C sur ses générateurs.

G_9 est une HNN extension de G_2 avec pour lettre stable $\langle t \rangle$. W contient donc un pinch $t^e B t^{-e}$, où \tilde{B} représentant de B dans G_2 est dans le sous-groupe engendré par $x, r_i (i \in I)$.

Si ce pinch est $t \Sigma R_0 q^{-1}t^{e_1}$, alors $e_1 = -1$ et $B \equiv \Sigma R_0 q^{-1}$. On a $\tilde{B} = \Sigma R_0 q^{-1}$ dans G_9 et donc aussi dans G_2 puisque $\Sigma R_0 q^{-1}$ est un mot dans G_2 , et que $G_2 \leq G_9$. On a donc $\tilde{B}^{-1} \Sigma R_0 = q$ dans G_2 . \tilde{B} et R_0 sont des mots sur $\langle x, r_i (i \in I) \rangle$, et donc en posant $L_1 \equiv \tilde{B}^{-1}$ et $L_2 \equiv R_0$ on a le résultat désiré.

Si le pinch est $t^{e_i} q R_i q^{-1}t^{e_{i+1}}$, alors $B \equiv q R_i q^{-1}$ et on a $e_i = -e_{i+1}$. Et alors dans G_9 , on a les égalités :

$$\begin{aligned} q^{-1}t^{e_i} q R_i q^{-1}t^{e_{i+1}} q &\equiv q^{-1}t^{e_i} q R_i q^{-1}t^{-e_i} q \\ &\equiv q^{-1}t^{e_i} B t^{-e_i} q \\ &= q^{-1}t^{e_i} \tilde{B} t^{-e_i} q \\ &= q^{-1} \tilde{B} q \\ &= q^{-1} B q \\ &= q^{-1} q R_i q^{-1} q \\ &= R_i \end{aligned}$$

car \tilde{B} est un mot sur $\langle x, r_i (i \in I) \rangle$, et t commute avec x et r_i . Ceci contredit le fait que m soit minimal (ce genre d'argument, sera fréquemment employé dans les paragraphes II.2 et II.3 ■

Considérons un mot spécial Σ , vérifiant les hypothèses du lemme. Alors si $\Sigma \equiv \bar{X} q_j Y$, et $L_1 \bar{X} q_j Y L_2 = q$ dans G_2 . On notera dans la suite $L_1 \bar{X} q_j = q L_2^{-1} Y^{-1}$.

Lemme II.2.4 : Si L_1 et L_2 sont librement réduits, alors les mots $L_1 \bar{X} q_j$ et $q L_2^{-1} Y^{-1}$ sont r_i -réduits (dans G_2) , pour tout $i \in I$.

Démonstration : On doit démontrer que les mots $L_1 \bar{X} q_j$, et $q L_2^{-1} Y^{-1}$ (pris comme éléments de G_2) ne contiennent pas de pinch $r_i^e C r_i^{-e}$, où C est un mot sur $\langle x, s_1, \dots, s_M, q, \dots, q_N \rangle$. Nous le démontrerons (par l'absurde) pour $L_1 \bar{X} q_j$, le cas de $q L_2^{-1} Y^{-1}$ étant similaire .

Supposons donc que L_1 soit librement réduit , et que $L_1 \bar{X} q_j$ contiennent un pinch $r_i^e C r_i^{-e}$. Les mots \bar{X} et q_j n'ayant pas d'occurrence de r_i , Le pinch est donc un sous mot de L_1 , où C est un mot sur x, s_b, q, q_p . Or L_1 est un mot sur $\langle x, r_i (i \in I) \rangle$, et donc $C \equiv x^m$. Pour démontrer que ce n'est pas un pinch , il faut démontrer que le représentant de x^m dans $G_1 * \langle q, q_1, \dots, q_N \rangle$ n'est pas dans le sous groupe engendré par $(\bar{F}_{i_1} q_{i_1} G_{i_1} ; s_1 x, \dots, s_M x)$, ou par $(\bar{H}_{i_2} q_{i_2} G_{i_2} ; s_1 x^{-1}, \dots, s_M x^{-1})$ (nous effectuerons la démonstration dans le premier cas , le deuxième étant similaire) .

Supposons donc que $x^m = V$ dans $G_1 * \langle q, q_1, \dots, q_N \rangle$.

où $V = {}_F W_0 (\bar{F}_{i_1} q_{i_1} G_{i_1})^{e_1} W_1 (\bar{F}_{i_2} q_{i_2} G_{i_2})^{e_2} \dots W_{n-1} (\bar{F}_{i_n} q_{i_n} G_{i_n})^{e_n}$

où les W_p sont des mots sur $\langle s_1 x, \dots, s_M x \rangle$ (éventuellement vides) , et $e = \pm 1$, et où V est réduit comme élément du produit libre .

Or x^m n'a pas d'occurrence de q_{i_1} , donc de $\bar{F}_{i_1} q_{i_1} G_{i_1}$, donc par unicité de l'écriture sous forme normale $x^m = W_0$ dans $G_1 * \langle q, \dots, q_N \rangle$. Ecrivons alors que $W_0 = (s_{b_1} x)^{f_1} \dots (s_{b_k} x)^{f_k}$, où $f_j = \pm 1$. On a alors $x^{-m} W_0 = 1$ dans $G_1 * \langle q, q_1, \dots, q_N \rangle$, et donc dans G_1 . Or G_1 est une HNN extension de $\langle x \rangle$, avec pour lettres stables $\langle s_1, \dots, s_M \rangle$. Donc si W_0 est non vide , d'après le théorème I.5.1 , $x^{-m} W_0$ contient un pinch $s_b^e x^\varepsilon s_b^{-e}$, avec $e = \pm 1$, $\varepsilon = \pm 1$. Si $e = 1$ alors d'après le théo. I.5.1 , $x^\varepsilon \in \langle x^2 \rangle$, ce qui est impossible avec $\varepsilon = \pm 1$. Donc $e = -1$ et le pinch est de la forme $s_b^{-1} x^\varepsilon s_b$. Or W_0 se trouve dans le sous-groupe libre de G_1 , engendré par $\langle s_1 x, \dots, s_M x \rangle$, au vu des générateurs , il ne peut contenir un tel sous-mot .

Donc W_0 est vide , et donc $x^{-m} = 1$ dans $\langle x / \rangle$, ce qui n'est possible qu'avec $m = 0$, et donc L_1 contient un sous-mot de la forme $r_i^e r_i^{-e}$, ce qui contredit le fait que L_1 soit librement réduit . ■

Remarquons que $L_1 \bar{X} q_j = q L_2^{-1} Y^{-1}$ dans G_2 , et de plus, sont r_i -réduits $\forall i \in I$. Donc d'après le lemme I.5.4, ils ont les même occurrences de $r_i \forall i \in I$. De plus ces occurrences se trouvent dans L_1 et L_2 .

Lemme II.2.5 : Soient L_1 et L_2 des mots sur $\langle x, r_i (i \in I) \rangle$, qui sont r_i -réduits $\forall i \in I$. Si X et Y sont des mots librement réduits sur $\langle s_1, \dots, s_M \rangle$, et si $L_1 \bar{X} q_j Y L_2 = q$ dans G_2 , alors X et Y sont des mots positifs et $(\bar{X} q_j Y)^* = q$ dans Γ .

Démonstration : Nous allons procéder par induction sur le nombre N d'occurrences de $r_i (i \in I)$, dans L_1 (qui, avec la remarque précédente, est la même dans L_2).

Si $N = 0$, $L_1 \bar{X} q_j Y L_2 = q$ dans G_2 , nous donne $x^m \bar{X} q_j Y x^n = q$ dans G_2 , où l'on n'a aucune occurrence de $r_i (i \in I)$.

Avec $G_1^* \langle q, q_1, \dots, q_N \rangle \leq G_2$, on a donc :

$$x^m \bar{X} q_j Y x^n = q \text{ dans } G_1^* \langle q, q_1, \dots, q_N \rangle.$$

Par unicité de l'écriture sous forme normale, on a donc, $q_j \equiv q$, et dans G_1 , $x^m \bar{X} = Y x^n = 1$ ce qui est possible dans G_1 , uniquement si $m = n = 0$, et \bar{X} et Y sont tout deux vides. En effet, G_1 est une HNN extension de $\langle x \rangle$ avec pour lettres stables $\langle s_1, \dots, s_M \rangle$; et si \bar{X} (respectivement Y) est non vide, d'après le théorème I.5.1 $x^m \bar{X}$ (respectivement $Y x^n$), contient un pinch $s_b^e C s_b^{-e}$, où C est un mot sur $\langle x \rangle$. Or les seules occurrences de s_b étant dans \bar{X} (resp^t Y), le pinch est un sous-mot de \bar{X} (resp^t Y). Or \bar{X} (resp^t Y) n'a pas d'occurrence de $\langle x \rangle$, et donc C est vide, ce qui contredit le fait que X (resp^t Y), soit réduit. Donc \bar{X} et Y sont tout deux vides et l'équation s'écrit alors $q = q$ dans $G_1^* \langle q, q_1, \dots, q_N \rangle$. On a donc bien X et Y positifs, et $(\bar{X} q_j Y)^* = q$ dans Γ .

Supposons $N > 0$. $L_1 \bar{X} q_j Y L_2 = q$ dans G_2 , où q ne contient pas r_i et est donc r_i -réduit. D'après le lemme I.5.2, $L_1 \bar{X} q_j Y L_2$ contient donc un pinch. Or L_1 et L_2 sont r_i -réduits $\forall i \in I (\Leftrightarrow$ ne contiennent pas de pinch). Nous pouvons alors écrire :

$$L_1 \bar{X} q_j Y L_2 \equiv L_3 (r_i^e x^m \bar{X} q_j Y x^n r_i^{-e}) L_4 = q \text{ dans } G_2$$

où L_3 et L_4 sont des mots r_i -réduits ($\forall i \in I$) sur $\langle x, r_i (i \in I) \rangle$, et le mot entre parenthèses, est un pinch.

D'après le théorème I.5.1, $x^m \bar{X} q_j Y x^n$ est dans le sous-groupe

$$A(i) = \langle \bar{F}_i q_{i1} G_i, s_1 x, \dots, s_n x \rangle \quad \text{si } e = -1$$

$$B(i) = \langle \bar{H}_i q_{i2} K_i, s_1 x^{-1}, \dots, s_n x^{-1} \rangle \quad \text{si } e = 1$$

Or c'est un élément du produit libre $G_1 * \langle q, q_1, \dots, q_N \rangle$, et donc $j = i_1$ si $e = -1$, $j = i_2$ si $e = 1$.

Dans la suite, nous ne considérerons que le cas où $e = -1$, la démonstration dans l'autre cas étant similaire.

On peut donc écrire :

$$W \equiv x^m \bar{X} q_j Y x^n U_0 (\bar{F}_i q_{i1} G_i)^{\alpha_1} U_1 \dots (\bar{F}_i q_{i1} G_i)^{\alpha_t} U_t = 1$$

dans $G_1 * \langle q, q_1, \dots, q_N \rangle$, où U_p ($p \in \langle 0, \dots, t \rangle$) est un mot réduit sur $\langle s_1 x, \dots, s_M x \rangle$ (éventuellement vide), et $\alpha_k = \pm 1$, ($k \in \langle 1, \dots, t \rangle$).

On peut prendre t minimal.

$G_1 * \langle q, q_1, \dots, q_N \rangle$ est une HNN extension de G_1 , avec pour lettres stables $\langle q, q_1, \dots, q_N \rangle$. q_j a une occurrence dans W , donc d'après le lemme de Britton W contient un pinch (en particulier $t \geq 1$).

Supposons que ce pinch porte sur la première occurrence de lettre stable, q_j . Alors $\alpha_1 = -1$, et $Y x^n U_0 G_i^{-1} = 1$ dans G_1 .

Nous allons démontrer qu'un pinch ne peut pas apparaître ailleurs dans W .

Supposons qu'un pinch apparaisse dans un sous-mot de W , de la forme :

$$(\bar{F}_i q_{i1} G_i)^{\alpha_p} U_p (\bar{F}_i q_{i1} G_i)^{\alpha_{p+1}}$$

Si $\alpha_p = 1$, alors $\alpha_{p+1} = -1$, et $G_i U_p G_i^{-1} = 1$ dans G_1 .

Si $\alpha_p = -1$, alors $\alpha_{p+1} = 1$, et $\bar{F}_i^{-1} U_p \bar{F}_i = 1$ dans G_1 .

Nous affirmons que dans les deux cas on a alors $U_p \equiv 1$. En effet G_1 est une HNN extension de $\langle x \rangle$, avec pour lettres stables $\langle s_1, \dots, s_M \rangle$. G_i et \bar{F}_i sont des mots sur $\langle s_1, \dots, s_M \rangle$ (qu'on peut prendre librements réduits), et donc d'après le théorème I.5.1, on a un pinch $s_b^{\epsilon} C s_b^{-\epsilon}$, où C est un sous-mot de U_p sur $\langle x \rangle$. Soit $C = x^m$. Mais U_p est un élément du groupe libre $\langle s_1 x, \dots, s_M x \rangle$ et ne peut donc contenir un tel sous mot que si $|m| \leq 1$. Et alors, soit U_p contient $s_b^{\epsilon} x^{\zeta} s_b^{-\epsilon}$, soit $U_p \equiv x^{\zeta}$, soit $U_p \equiv 1$ ($\epsilon, \zeta = \pm 1$). Au vu des générateurs, seul le

dernier cas est possible .

On peut alors réduire librement :

$$(\bar{F}_i q_{i1} G_i)^\alpha U_p (\bar{F}_i q_{i1} G_i)^{\alpha_{p+1}} \equiv (\bar{F}_i q_{i1} G_i)^\alpha (\bar{F}_i q_{i1} G_i)^{-\alpha} \equiv 1$$

Ce qui contredit le fait que t soit minimum .

Donc (lemme I.5.4) $t = 1$ et $\alpha = -1$.

$$W \equiv x^m \bar{X} q_j Y x^n U_0 G_i^{-1} q_j^{-1} \bar{F}_i^{-1} U_1 = 1 \quad \text{dans } G_1 * \langle q, \dots, q_N \rangle$$

$$\text{et } Y x^n U_0 G_i^{-1} = 1 \quad \text{dans } G_1$$

Et donc

$$x^m \bar{X} \bar{F}_i^{-1} U_1 = 1 \quad \text{dans } G_1$$

Ce qui nous donne après conjugaison cyclique :

$$x^n U_0 G_i^{-1} Y = 1 \quad \text{dans } G_1$$

$$\text{et } \bar{X} \bar{F}_i^{-1} U_1 x^m = 1 \quad \text{dans } G_1$$

U_0 et U_1 étant réduits , ils ne contiennent aucun sous-mot de la forme $s_b^{-1} s_b$ ou $s_b s_b^{-1}$. Nous éliminons tout les sous-mots de cette forme , dans $x^n U_0 G_i^{-1} Y$. Nous affirmons alors que la première lettre de $G_i^{-1} Y$ est positive (et donc G_i^{-1} disparaît , puisque G_i est un mot positif) . En effet supposons que G_i^{-1} commence par s_b^{-1} . Alors puisque $x^n U_0 G_i^{-1} Y = 1$ dans G_1 , et a une occurrence de s_b et que G_1 est une HNN extension de $\langle x \rangle$ avec pour lettres stables $\langle s_1, \dots, s_M \rangle$, d'après le théorème I.5.1 , il contient un pinch . Or puisque $G_i^{-1} Y$ est un mot librement réduit sur $\langle s_1, \dots, s_M \rangle$, il ne contient pas de pinch . De même U_0 ne contient pas de pinch (cf plus haut) , le pinch est donc $s_b C s_b^{-1}$ (avec C non vide) , où $s_b C$ est un mot terminal de U_0 , et s_b^{-1} est la première lettre de G_i^{-1} . Rappelons nous que U_0 est un mot sur la famille libre de générateurs $\langle s_1 x, \dots, s_M x \rangle$. On a donc forcément (C n'ayant pas d'occurrence de s_b) , $s_b C \equiv s_b x$. Or d'après le théorème I.5.1 , C est un élément de $\langle x^2 \rangle$, soit $x \in \langle x^2 \rangle$, ce qui est impossible .

De façon similaire on peut montrer qu'après avoir éliminé les sous-mots $s_b^{-1} s_b$ et $s_b s_b^{-1}$ de $\bar{X} \bar{F}_i^{-1} U_1 x^m$, la dernière lettre de \bar{F}_i^{-1} est négative (et donc \bar{F}_i^{-1} disparaît après réductions) .

On a $U_0 G_i^{-1} Y x^n = 1$ dans G_1 (conjugaison cyclique) . Ainsi $U_0^{-1} = (G_i^{-1} Y) x^n$ dans G_1 , où $G_i^{-1} Y \equiv Y_1$ est un mot positif sur $\langle s_1, \dots, s_M \rangle$.

Considérons $V_0^{-1} \equiv r_i^{-1} U_0^{-1} r_i$. Puisque U_0 est un mot sur

$\langle s_1 x, \dots, s_M x \rangle$, et que $r_i^{-1}(s_b x) r_i = s_b x^{-1}$, alors V_0^{-1} est un mot sur $\langle s_1 x^{-1}, \dots, s_M x^{-1} \rangle$. Nous pouvons considérer U_0^{-1} et V_0^{-1} , comme des éléments de G_1 .

Nous affirmons qu'il existe ψ automorphisme de G_1 qui fixe s_b $\forall b \in \{1, \dots, M\}$, et qui envoie x sur x^{-1} . En effet considérons

$$\phi : \langle s_1, \dots, s_M, x \rangle \longrightarrow \langle s_1, \dots, s_M, x^{-1} \rangle$$

tel que $\phi(s_b) = s_b$ et $\phi(x) = x^{-1}$.

Alors $\exists ! \psi$ homomorphisme, tel que le diagramme suivant commute

$$\begin{array}{ccc} \langle s_1, \dots, s_M, x \rangle & & \\ \downarrow \iota & \searrow \psi & \\ \langle s_1, \dots, s_M, x \rangle & \xrightarrow{\phi} & G_1 \end{array}$$

où ι est l'inclusion.

De plus ψ est surjective, car $\phi(\langle s_1, \dots, s_M, x \rangle) = \langle s_1, \dots, s_M, x^{-1} \rangle$ est une famille génératrice de G_1 .

De plus $\phi(\Delta_1) = 1$, car $x s_b = s_b x^2 \Rightarrow x^{-1} x s_b x^{-2} = x^{-1} s_b x^2 x^{-2} \Rightarrow s_b x^{-2} = x^{-1} s_b$. On a donc l'endomorphisme induit $\bar{\psi} : G_1 \longrightarrow G_1$, et de plus $\bar{\psi} \bar{\psi}^{-1} = \text{Id}$, c'est donc un automorphisme.

Nous avons donc $V_0^{-1} = \psi(U_0^{-1})$, et donc $V_0^{-1} = Y_1 x^{-n}$ dans G_1 . Un argument similaire montre que $V_1^{-1} = x^{-m} \bar{X}_1$, où $\bar{X}_1 \equiv \bar{X} \bar{F}_1^{-1}$ est un mot négatif, et $V_1^{-1} = r_i^{-1} U_1^{-1} r_i$.

Abordons l'étape de récurrence de notre induction.

$$\begin{aligned} \text{Nous avons dans } G_2 \quad q &= L_1 \bar{X} q_j Y L_2 \equiv L_9 r_i^{-1} (x^m \bar{X}) q_j (Y x^n) r_i L_4 \\ &= L_9 r_i^{-1} (U_1^{-1} \bar{F}_1) q_j (G_1 U_0^{-1}) r_i L_4 \\ &= L_9 V_1^{-1} r_i^{-1} (\bar{F}_1 q_j G_1) r_i V_0^{-1} L_4 \\ &= L_9 V_1^{-1} (r_i^{-1} \bar{F}_1 q_j G_1 r_i) V_0^{-1} L_4 \\ &= L_9 V_1^{-1} (\bar{H}_1 q_{i_2} K_i) V_0^{-1} L_4 \\ &= (L_9 x^{-m} \bar{X}_1) \bar{H}_1 q_{i_2} K_i (Y_1 x^{-n} L_4) \end{aligned}$$

On a donc $(L_9 x^{-m}) \bar{X}_1 \bar{H}_1 q_{i_2} K_i Y_1 (x^{-n} L_4) = q$ dans G_2 .

Considérons donc que $L_1 \bar{X} q_j Y L_2$, vérifie les hypothèses, et que L_1 et L_2 ont N occurrence de r_i ($i \in I$).

Remarquons que $L_9 x^{-m}$ et $x^{-n} L_4$ ont alors $N - 1$ occurrences de r_i et sont r_i -réduits. K_i est positif. De plus $Y_1 \equiv G_1^{-1} Y$, et puisque G_1^{-1} disparaît, Y_1 est un sous-mot de Y , et est donc librement réduit.

.Donc la seule réduction possible dans $K_i Y_1$, est à la "jonction", ce qui est impossible puisqu'on a vu que la première lettre de Y_1 est positive. (Le même raisonnement montre que $\bar{X}_1 \bar{H}_i$, est réduit).

On peut donc appliquer l'hypothèse d'induction ; $K_i Y_1$ et $X_1 H_i$ sont donc des mots positifs, et $(\bar{X}_1 \bar{H}_i q_{i_2} K_i Y_1)^* \equiv X_1 H_i q_{i_2} K_i Y_1 = q$ dans Γ (équation (*)). Or $X \equiv X_1 F_i$ et $Y \equiv G_i Y_1$, et sont donc positifs en tant que sous-mots de mots positifs.

Or $X q_j Y \equiv X_1 F_i q_{i_1} G_i Y_1 = X_1 H_i q_{i_2} K_i Y_1$ dans Γ

ce qui avec (*) nous donne le résultat souhaité $X q_j Y = q$ dans Γ ■

Nous pouvons maintenant achever la démonstration du lemme de Boone.

Démonstration de la condition nécessaire du lemme de Boone

Prenons $\Sigma = \bar{X} q_j Y$ (on peut prendre X et Y librement réduits) mot spécial tel que $k(\Sigma^{-1} t \Sigma) = (\Sigma^{-1} t \Sigma) k$ dans G . Alors (lemme II.2.3), $\exists L_1$ et L_2 , mots sur $\langle x, r_i (i \in I) \rangle$ tel que $L_1 \Sigma L_2 = q$ dans G_2 . On peut supposer que L_1 et L_2 sont librement réduits, et alors (lemme II.2.4), ils sont r_i -réduits $\forall i \in I$. On a donc d'après le lemme II.2.5, $\Sigma^* = q$ dans Γ ■

Nous avons démontré que le problème du mot de $\Gamma(T)$ est réductible au problème du mot de $G(T)$. W.W. Boone, dans [5], démontre en utilisant des extensions HNN, la réciproque (très technique). En combinant ce résultat avec le théorème I.1.2, il établit le résultat :

Théorème I.2.2 : (Boone)

Pour tout degré d'insolubilité D il existe un groupe f.p. ayant un problème du mot de degré D .

En se servant de ce résultat, Collins démontre le théorème plus général :

Théorème I.2.3 : (Collins)

Pour tout degrés d'insolubilité D_1 et D_2 , $D_1 \leq D_2$ ssi il existe un groupe f.p. ayant un problème du mot de degré D_1 , et un problème de la conjugaison

de degré D_2 .

Pour une démonstration simple voir [26] .Remarquons que cette démonstration utilise la construction que nous effectuons en III.2

II.3 THEOREMES DE PLONGEMENTS

II.3.1 Théorème de Higman

Le but de ce paragraphe est de démontrer le théorème suivant

Théorème II.3.1 : (Higman)

Un groupe finiment engendré est le sous-groupe
d'un groupe finiment présenté ssi il admet une
présentation récursive .

Ce résultat est quelque peu surprenant ,en ceci qu'il établit un lien étroit entre la théorie de la récursivité et la théorie des groupes .Il permet de démontrer simplement le théorème de Novikov-Boone .En effet il est aisé de trouver un groupe récursivement présenté ayant un problème du mot récursivement insoluble .

Considérons $I \subset \mathbb{N}$,récursivement énumérable ,non récursif .Un tel ensemble existe (proposition I.4.1) .Considérons alors le groupe récursivement présenté :

$$K = \langle a, b, c, d \mid a^i b a^{-i} = c^i d c^{-i}, i \in I \rangle .$$

Il est clair que K est le produit libre amalgamé de $\langle a, b \mid \rangle$,et de $\langle c, d \mid \rangle$ sur les sous-groupes respectifs engendrés par les membres de gauche (resp^t de droite) des relations de K .Alors $a^i b a^{-i} c^i d^{-1} c^{-i} =_K 1$ si et seulement si $i \in I$,et donc K a un problème du mot récursivement insoluble .Or avec le théorème de Higman , K se plonge dans un groupe finiment présenté G ,et puisque le problème du mot est héréditaire , G est un groupe f.p. ayant un problème du mot récursivement insoluble .

Remarquons que le sens (\Rightarrow) est trivial :

PROPOSITION II.3.1 : Tout sous-groupe finiment engendré d'un groupe f.p. ,est récursivement présenté .

Démonstration : Considérons un sous-groupe finiment engendré d'un groupe f.p. . Remarquons que l'ensemble des mots s'écrivant sur ces générateurs est récursivement énumérable . Or l'ensemble des éléments triviaux du groupe f.p. est récursivement énumérable . L'ensemble des éléments triviaux du sous-groupe est donc l'intersection de ces deux ensembles , qui est alors (prop I.4.2) récursivement énumérable . On a donc une présentation récursive du sous-groupe . ■

Considérons un groupe récursivement présenté R .

$$R = \langle u_1, \dots, u_m \mid \omega = 1, \omega \in E \rangle$$

i.e , E est un ensemble récursivement énumérable , de mots positifs sur $\langle u_1, \dots, u_m \rangle$.

Considérons alors , la machine de Turing T , qui énumère E . T a pour alphabet $\langle s_0, \dots, s_M \rangle$, où $\langle u_1, \dots, u_m \rangle \subseteq \langle s_0, \dots, s_M \rangle$. Nous pouvons prendre T , avec pour état d'arrêt q_0 (lemme I.4.1) .

Nous avons vu que nous pouvons construire sur T un semi-groupe finiment présenté $\Gamma(T)$, tel que pour tout mot ω sur $\langle s_1, \dots, s_M \rangle$, $\omega \in E \iff h q_1 \omega h = q$ dans $\Gamma(T)$.

Dans le paragraphe II.2 , nous avons réécrit sur un nouvel alphabet (en posant $s_M = h$, et en renumérotant $\langle q_i \rangle$ et $\langle s_j \rangle$) , la présentation de $\Gamma(T)$ (par commodité d'écriture), et avons nommé Γ , le semi-groupe ainsi (finiment) présenté. Nous avons construit sur Γ , un groupe finiment présenté G , tel que (lemme de Boone) , pour tout mot spécial Σ ,

$$k (\Sigma^{-1} t \Sigma) = (\Sigma^{-1} t \Sigma) k \text{ dans } G \iff \Sigma^* = q \text{ dans } \Gamma$$

Dans cette partie , nous considérerons la présentation de G , construite sur la présentation de $\Gamma(T)$ (où T est la machine décrite ci-dessus) . Il nous suffit pour cela de changer dans l'ancienne présentation s_M en h , et de prendre pour $\langle s_i \rangle$ et $\langle q_j \rangle$, respectivement l'alphabet , et l'ensemble d'états de la machine $\langle s_0, \dots, s_M \rangle$ et $\langle q_1, \dots, q_N \rangle$ (nous omettons de changer les indices M et N , par rapport à l'ancienne présentation. Nous procéderons de la même façon pour G_1, G_2, G_3 .

Considérons le mot spécial $\Sigma \equiv h^{-1} q_1 \omega h$, où ω est un mot positif sur $\langle s_0, \dots, s_M \rangle$. D'après ce qui précède , Les assertions suivantes sont équivalentes .

$$\omega \in E$$

$$\Sigma^* \equiv h q_1 \omega h = q \quad \text{dans } \Gamma(T)$$

$$k(\Sigma^{-1}t\Sigma) = (\Sigma^{-1}t\Sigma)k \quad \text{dans } G$$

$$(*) \quad k(h^{-1}\omega^{-1}q_1^{-1}h t h^{-1}q_1\omega h) = (h^{-1}\omega^{-1}q_1^{-1}h t h^{-1}q_1\omega h) \quad \text{dans } G$$

L'équation (*) est obtenu à partir de la précédente, en remplaçant Σ par $h^{-1}q_1\omega h$. Afin d'en simplifier l'écriture nous introduisons

$$k_o \equiv h k^{-1}h \quad \text{et} \quad t_o \equiv q_1^{-1}h t h^{-1}q_1.$$

Considérons alors :

$$G'_3 = \langle G_2, t_o / t_o^{-1}(q_1^{-1}h r_i h^{-1}q_1)t_o = q_1^{-1}h r_i h^{-1}q_1, \\ t_o^{-1}(q_1^{-1}h x h^{-1}q_1)t_o = q_1^{-1}h x h^{-1}q_1 \rangle$$

En remplaçant t_o par $q_1^{-1}h t h^{-1}q_1$, on remarque que G'_3 est une autre présentation de G_3 .

De même:

$$G' = \langle G'_3, k_o / k_o^{-1}(h r_i h^{-1})k_o = h r_i h^{-1}, k_o^{-1}(h x h^{-1})k_o = h x h^{-1}, \\ k_o(h q_1^{-1}h^{-1}q_1 t_o q_1^{-1}h q h^{-1})k_o = h q_1^{-1}h^{-1}q_1 t_o q_1^{-1}h q h^{-1} \rangle$$

est une autre présentation de G .

Lemme II.3.1 : G' est une HNN extension de G'_3 ayant pour lettre stable $\langle k_o \rangle$. G'_3 est une HNN extension de G_2 , ayant pour lettre stable $\langle t_o \rangle$.

Démonstration : k_o a pour sous-mot k , qui n'est pas sur l'alphabet de G' . Les relateurs invoquant k_o , sont donc uniquement ceux donnés dans la présentation. On vérifie aisément la condition de l'isomorphe (les sous-groupes en question sont engendrés par les même générateurs).

Le même raisonnement est valable pour G'_3 . ■

Lemme II.3.2 : Soit ω un mot positif sur $\langle s_o, \dots, s_M \rangle$.

$$\text{Alors } \omega \in E \iff k_o(\omega^{-1}t\omega) = (\omega^{-1}t\omega)k_o \text{ dans } G'$$

Démonstration : Le deuxième membre de l'équivalence n'est rien d'autre que l'équation (*) réécrite en utilisant k_o et t_o . ■

Nous définissons le produit libre

$$G_4 = G' * R$$

Nous considérons une présentation de G_4 donnée par la réunion des générateurs et des relateurs de G' et R . L'union doit être disjointe, nous considérons donc :

$$\langle a_1, \dots, a_m \rangle \subseteq \langle s_0, \dots, s_M \rangle \quad \text{avec} \quad a_i \leftrightarrow u_i$$

E peut alors être considéré comme un ensemble de mots positifs sur $\langle a_1, \dots, a_m \rangle$.

Nous définissons :

$$G_5 = \langle G_4 ; b_1, \dots, b_m \mid b_i^{-1} u_j b_i = u_j ; b_i^{-1} a_j b_i = a_j ; \\ b_i^{-1} k_0 b_i = k_0 u^{-1} \\ \text{pour tout } i, j = 1, \dots, m \rangle$$

$$G_6 = \langle G_5 ; d \mid d^{-1} k_0 d = k_0 ; d^{-1} a_i b_i d = a_i ; i = 1, \dots, m \rangle$$

$$G_7 = \langle G_6 ; \sigma \mid \sigma^{-1} t_0 \sigma = t_0 d ; \sigma^{-1} k_0 \sigma = k_0 \\ \sigma^{-1} a_i \sigma = a_i ; i = 1, \dots, m \rangle$$

La démonstration du théorème de Higman va alors consister à :

1°) - Montrer que l'on a une chaîne de Britton

$$R \subseteq G_4 \leq G_5 \leq G_6 \leq G_7$$

2°) - Montrer que G_7 a une présentation finie.

Notation : Dans cette partie nous noterons $\langle x_1, x_2, \dots \rangle_i$, pour désigner le sous-groupe de G_i engendré par x_1, x_2, \dots ($i = 4 \dots 7$)

Nous avons besoin du lemme suivant.

Lemme II.3.3 : Les sous-groupes de G_4 , $\langle a_1, \dots, a_m, k_0 \rangle_4$ et $\langle a_1, \dots, a_m, t_0 \rangle_4$ sont librement engendrés par leurs générateurs

Démonstration : Nous démontrerons le résultat dans le premier cas, le deuxième étant similaire. Avec nos nouvelles notations ; G_1 est une HNN extension de $\langle x \rangle$ ayant pour lettres stables $\langle s_0; \dots; s_n \rangle$. Donc d'après le lemme I.5.3 le sous-groupe de G_1

engendré par s_0, \dots, s_n est libre. Or :

$$G_1 \leq G_1 * \langle q, \dots, q_n \rangle \leq G_2 \leq G'_g \leq G'$$

Donc puisque $G_4 = G' * R$ et que $\langle a_1; \dots; a_m \rangle \subseteq \langle s_0; \dots; s_m \rangle \subset G'$
 $\langle a_1; \dots; a_m \rangle_4$ est libre sur ses générateurs.

Prenons un mot W sur a_1, \dots, a_m, k_0 .

$$W \equiv C_0 k_0^{e_1} C_1 \dots k_0^{e_n} C_n = 1 \quad \text{dans } G_4.$$

Où les C_i sont des mots sur $\langle a_1, \dots, a_m \rangle$.

Or puisque W n'invoque que des lettres de G' ; $W = 1$ dans G' .

G' est une HNN extension de G'_g ayant lettre stable k_0 ; donc si

$n \geq 1$ W contient un pinch $k_0^{e_i} C_i k_0^{e_{i+1}}$ où C_i est égal dans G'_g à un mot sur $h r_i h^{-1}$; $h x h^{-1}$; et $h q_i^{-1} h^{-1} q_i t_{01} q_i^{-1} h q_i h^{-1}$.

Or les relations de G' assurent que k_0 commutent avec ces éléments, et donc on peut remplacer le pinch dans W ; par C_i . Après avoir réitéré ce procédé on arrive à :

$$W' \equiv C_0 \dots C_n = 1 \text{ dans } G' \text{ et donc dans } F(a_1; \dots; a_m); \text{ donc } W' \equiv 1.$$

Si l'on prend $C_0 \dots C_n$ réduits; alors ceci est contradictoire.

Donc $\langle a_1, \dots, a_m, k_0 \rangle_4$ est libre sur ses générateurs. ■

Lemme II.3.4 : G_5 est une HNN extension de G_4 ayant pour lettres stables $\langle b_1, \dots, b_n \rangle$.

Démonstration : Il est clair que G_5 a pour base G_4 , et pour lettre stable $\langle b_1, \dots, b_m \rangle$.

Il nous reste à vérifier la condition de l'isomorphisme, i.e. $\forall i$, il existe un isomorphisme $\Psi_i : A(i) \longrightarrow B(i)$

$$\text{avec } \forall i \quad A(i) = \langle u_1, \dots, u_m, a_1, \dots, a_m, k_0 \rangle.$$

$$B(i) = \langle u_1, \dots, u_m, a_1, \dots, a_m, k_0 u_i^{-1} \rangle_4.$$

tel que $\Psi_i(u_p) = u_p$, $\Psi_i(a_p) = a_p$, $\Psi_i(k_0) = k_0 u_i^{-1}$, pour tout $p = 1 \dots m$, et pour tout $i = 1 \dots n$.

Remarquons que $k_0 = k_0 u_i^{-1} u_i \in B(i)$ donc $A(i) = B(i)$.

Nous avons $G_4 = G' * R$. On peut donc écrire (lemme 4.1.2 de [23])

$$A(i) = B(i) = \langle u_1, \dots, u_m \rangle_4 * \langle a_1, \dots, a_m, k_0 \rangle_4.$$

D'après le lemme II.3.2, $\langle a_1, \dots, a_m, k_0 \rangle_4$ est libre.

On a donc $\forall i$ l'homomorphisme

$$\psi_i : \langle a_1, \dots, a_m, k_0 \rangle \longrightarrow A(i)$$

tel que $\psi_i(a_p) = a_p$; $\psi_i(k_o) = k_o u_i^{-1}$

On peut donc construire par propriété des produits libres :

$$\tilde{\psi}_i : A(i) \longrightarrow A(i)$$

tel que $\tilde{\psi}_i(u_p) = u_p$; $\tilde{\psi}_i(a_p) = a_p$; $\tilde{\psi}_i(k_o) = k_o u_i^{-1}$

de la même façon :

$$\phi_i : \langle a_i, \dots, a_m, k_o \rangle \longrightarrow A(i)$$

avec $\phi : (a_p) = a_p$; et $\phi : (k_o) = k_o u$

et on peut construire $\tilde{\phi}_i : A(i) \longrightarrow A(i)$ tel que $\tilde{\phi}_i(a_p) = a_p$

; $\tilde{\phi}_i(k_o u_i^{-1}) = k_o$; $\tilde{\phi}_i(u_p) = u_p$

Et alors $\tilde{\phi}_i \circ \tilde{\psi}_i = \tilde{\psi}_i \circ \tilde{\phi}_i = \text{Id}_{A(i)}$ et on a donc l'isomorphisme souhaité .

Lemme II.3.5 : G_o est une HNN extension de G_5 , ayant pour lettre stable $\langle d \rangle$.

Démonstration : Nous devons vérifier qu'il existe un isomorphisme

$$\psi : \langle k_o, a_1 b_1, \dots, a_m b_m \rangle_5 \longrightarrow \langle k_o, a_1, \dots, a_m \rangle_5$$

tel que

$$\psi(k_o) = k_o$$

$$\psi(a_i b_i) = a_i \text{ pour tout } i = 1 \dots m$$

prenons $G_5 = F_N$ quotient associé à la présentation .

définissons l'homomorphisme $\phi : F \longrightarrow G_4$ tel que $\phi(u_i) = 1$

$$\phi(b_i) = 1$$

et ϕ envoie les autres générateurs sur eux-même .

Il est clair que $N \subseteq \ker \phi$, et on peut donc considérer

l'homomorphisme $\tilde{\phi} : G_5 \longrightarrow G_4$, quotient de ϕ . $\tilde{\phi}$ envoie $\langle k_o, a_i b_i \rangle_5$

sur $\langle k_o, a_1 b_1, \dots, a_m b_m \rangle_4$ qui est libre (lemme II.3.3) . Il en est

donc de même pour $\langle k_o, a_1 b_1, \dots, a_m b_m \rangle_5$ et de plus ils ont même rang.

On a donc un isomorphisme $\Psi : \langle k_o, a_i, \dots, a_m \rangle_5 \longrightarrow \langle k_o, a_1 b_1, \dots, a_m b_m \rangle_5$

tel que $\Psi(k_o) = k_o$

$$\Psi(a_p) = a_p b_p$$

Il suffit alors de considérer $\psi = \Psi^{-1}$

Le lemme suivant va nous être utile pour démontrer que G_7 est une HNN extension de G_o .

Lemme II.3.6 : Le sous-groupe A de G' , engendré par $k_o, t_o, a_1,$

\dots, a_n admet pour présentation :

$$A = \langle k_0, t_0, a_1, \dots, a_n \mid k_0^{-1} \omega^{-1} t_0 \omega k_0 = \omega^{-1} t_0 \omega, \omega \in E \rangle$$

où l'on a réécrit les mots de E , sur l'alphabet $\{a_1, \dots, a_m\}$. (On se rappelle que $u_i \longleftrightarrow a_i$)

Démonstration : D'après le lemme II.3.2, la proposition :

(**) $k_0^{-1} \omega^{-1} t_0 \omega k_0 = \omega^{-1} t_0 \omega$ est vrai pour tout $\omega \in E$ (ω est un mot positif sur a_1, \dots, a_n), donc est vraie dans A .

Nous allons montrer qu'aucune autre relation n'est utile pour décrire A .

Il est aisé de vérifier que la relation (**) implique

$$t_0^\varepsilon \omega k_0^\eta = \omega k_0^\eta \omega^{-1} t_0^\varepsilon \omega \text{ pour } \varepsilon = \pm 1, \eta = \pm 1 \text{ et pour tout } \omega \in E.$$

Nous pouvons alors considérer les opérations élémentaires dans A

$$\text{de la forme } U \equiv U_1 t_0^\varepsilon \omega k_0^\eta U_2 \longrightarrow U_1 \omega k_0^\eta \omega^{-1} t_0^\varepsilon \omega U_2$$

Celles ne changent pas l'élément du groupe représenté par U .

Nous considérons aussi les opérations élémentaires :

$$U \equiv U_1 Y Y^{-1} U_2 \longrightarrow U_1 U_2$$

pour $Y = k_0, t_0, a_1, \dots, a_m$

Ces opérations baissent le nombre d'occurrence de t_0^ε précédant un k_0^η .

Considérons $U = 1$ dans A . Nous allons montrer que U peut être réduit au mot vide par une suite d'opérations élémentaires, comme nous venons de les définir, et donc que U est une conséquence des relateurs pré-cités. Ainsi la présentation donnée ci-dessus sera bien une présentation de A .

On lui applique les opérations élémentaires décrites ci-dessus. U est librement réduit et ne contient plus de sous-mots de la forme $t_0^\varepsilon \omega k_0^\eta$ où $\omega \in E$. Nous allons démontrer qu'alors U est le mot vide. Si U ne contient pas t_0 , alors $U = 1$ dans $\langle a_1, \dots, a_m, k_0 \rangle$, qui est un groupe libre (lemme II.3.3) et alors, U étant librement réduit $U \equiv 1$. Ce qui nous permet de conclure.

On a le même résultat si U n'invoque pas k_0 ($\langle a_1, \dots, a_m, t_0 \rangle$ est libre).

Nous avons donc démontré que U est vide s'il n'invoque pas soit k_0 , soit t_0 .

Supposons que U invoque k_0 et t_0 (et n'est donc pas vide).

G' est une HNN extension de G'_3 , ayant pour lettre stable $\langle k_0 \rangle$.
 $U = 1$ dans G' et invoque k_0 .

D'après le théorème I.5.1, U contient un pinch $k_0^e V k_0^{-e}$ où $V = D$ dans G'_3 et D est un mot sur $hr_i h^{-1}, h x h^{-1}$, et $h q_1^{-1} h^{-1} q_1 t_0 q_1^{-1} h q h^{-1}$.

Afin de simplifier les notations posons $\Delta = h q_1^{-1} h^{-1} q_1$ et donc D est un mot sur $hr_i h^{-1} h x h^{-1}$ et $\Delta t_0 \Delta^{-1}$.

Nous prenons $D = V$, de telle façon que D ait le nombre minimal d'occurrence de t_0 . G'_3 est une HNN extension de G_2 avec pour lettre stable $\langle t_0 \rangle$.

Nous affirmons que V et D sont tout deux t_0 -réduit dans G'_3 .

Supposons que D ne soit pas t_0 -réduit, il contient alors un pinch et peut donc s'écrire :

$D \equiv D_1 \Delta t_0^f \Delta^{-1} D_2 \Delta t_0^{-f} \Delta^{-1} D_3$, où D_2 n'invoque pas t_0 .

Avec le lemme de Britton $\Delta^{-1} D_2 \Delta = N$ dans G_2 où N est un mot sur $q_1^{-1} h r_i h^{-1} q_1$ et $q_1^{-1} h x h^{-1} q_1$ de plus dans G'_3 t_0 commute avec N (au vu des relations de l'extension). Et alors $D = D_1 \Delta N \Delta^{-1} D_3$ ce qui contredit le fait que le nombre d'occurrence de t_0 dans D est minimal. Donc D est t_0 réduit.

V est librement réduit puisque c'est un sous-mot de U et que U est librement réduit. Montrons que V est t_0 réduit.

Dans le cas contraire, il contient un pinch $t_0^g C t_0^{-g}$, où $C = N$ dans G_2 , où N est un mot sur $q_1^{-1} h r_i h^{-1} q_1$ et $q_1^{-1} h x h^{-1} q_1$, et donc commute avec t_0 dans G'_3 (donc C aussi). De plus C n'invoque pas t_0 , et n'invoque pas k_0 (puisque C est un sous-mot de V , qui n'invoque pas k_0). Alors C est un mot sur a_1, \dots, a_m .

Or $\langle t_0, a_1, \dots, a_m \rangle_4$ est un groupe libre donc $\langle t_0, a_1, \dots, a_m \rangle_3$ aussi.

Donc C commute avec t_0 , ssi $C \equiv 1$ ce qui contredit le fait que C soit librement réduit en tant que sous-mot de V .

Nous allons maintenant démontrer que D invoque t_0 .

Etant donné que $V = D$ dans G'_3 , et que V et D sont tout deux t_0 réduits, alors d'après le lemme I.5.4, V et D ont le même nombre d'occurrence de t_0 .

Supposons que D ne contiennent pas t_0 . Donc V ne contient pas t_0 .

Alors V est un mot sur a_1, \dots, a_m et D est un mot sur $hr_i h^{-1}, h x h^{-1}$.

Nous pouvons prendre D avec un nombre d'occurrence de r_i minimal (considérer l'écriture de D sur $hr_i h^{-1}, h x h^{-1}$, contenant le moins d'occurrence de r_i). $V = D$ dans G_2 , HNN extension de $G_1 * \langle q, q_1, \dots, q_n \rangle$ avec pour lettres stables $\langle r_i, i \in I \rangle$. Visiblement

, V est r_i -réduit, puisqu'il n'a pas d'occurrence de r_i . Démontrons que D est aussi r_i -réduit. Supposons donc que D contienne un pinch. $D \equiv D_1 h r_i^l h^{-1} D_2 h r_i^{-l} h^{-1} D_3$, où D_1, D_2, D_3 sont des mots sur $h \times h^{-1}, h r_i h^{-1}$ et D_2 n'invoque pas r_i . Donc $D_2 \equiv h x^n h^{-1}$ $n \in \mathbb{N}$ et le pinch est donc de la forme $r_i^l x^n r_i^{-l}$.

D'après le théorème I.5.1, x^n est égal dans $G_1 * \langle q, q_1, \dots, q_n \rangle$ à un mot sur $\bar{F}_i q_{i1} G_i, S_1 x, \dots, S_m x$ ou sur $\bar{H}_i q_{i2} F_i, S_1 x^{-1}, \dots, S_m x^{-1}$.

Mais nous avons déjà vu (démonstration du lemme II.2.4), que ceci n'est possible que si $n = 0$. Et alors, on peut réduire l'écriture de D , soit $D \equiv D_1 D_3$ dans G_2 . Ce qui contredit le fait que l'écriture de D contient un minimum de r_i .

Donc D et V sont tout deux r_i -réduits $\forall i \in I$. De plus $D = V$ dans G_2 donc d'après le lemme I.5.4, D et V ont même occurrences de r_i . V ne contenant pas r_i , D ne contient pas non plus r_i .

et alors $V = D$ dans G_1 , et $V = h x^n h^{-1}$ dans G_1 .

Supposons que V contienne a_j .

G_1 est une HNN extension de $\langle x \rangle$ avec pour lettres stables $\langle s_1, \dots, s_m \rangle$, et puisque $\langle a_1, \dots, a_m \rangle \subseteq \langle s_1, \dots, s_m \rangle$, alors $V h x^{-n} h^{-1}$ contient un pinch $a_j^d C a_j^{-d}$, où C est un mot sur x . Mais le pinch est alors un sous-mot de V . Or V ne contient pas x . On a donc $C \equiv 1$, ce qui contredit le fait que V soit librement réduit.

Or V est un mot sur a_1, \dots, a_m, t_0 . Supposons que D ne contienne pas t_0 . Alors V ne contient pas t_0 et d'après ce qui précède $V \equiv 1$. Or $h_0^\alpha V h_0^{-\alpha}$ est un sous-mot de U , et ceci contredit donc le fait que U soit librement réduit.

On a donc prouvé que D contient t_0 . Et donc D contient un sous-mot $h q^{-1} h^{-1} q_1 t_0 q_1^{-1} h q h^{-1}$.

On écrit $D \equiv D_1 (h q^{-1} h^{-1} q_1 t_0 q_1^{-1} h q h^{-1})^\alpha T$, où $\alpha = \pm 1$, et le mot entre parenthèses contient la dernière occurrence de t_0 dans D , i.e. D_1 est un mot sur $h x h^{-1}, h r_i h^{-1}, h q^{-1} h^{-1} q_1 t_0 q_1^{-1} h q h^{-1}$ et T est un mot sur $h x h^{-1}, h r_i h^{-1}$.

Puisque D contient t_0 , nous savons aussi que U contient t_0 (cf plus haut). Nous pouvons alors écrire :

$V \equiv V_0 t_0^{\varepsilon_1} \dots V_{r-1} t_0^{\varepsilon_r} V_r$ où chaque V_j est un mot sur a_1, \dots, a_m .

Nous avons vu que V et D sont tout deux t_0 -réduits. On peut donc appliquer le lemme I.5.4 et alors $t_0^{\varepsilon_r} V_r T^{-1} h q^{-1} h^{-1} q_1 t_0^{-\alpha}$ est un pinch, et $V_r T^{-1} h q^{-1} h^{-1} q_1 = K$ dans G_2 , où K est un mot sur

$q_1^{-1} h r_i h^{-1} q_1$ et $q_1^{-1} h x h^{-1} q_1$, T est un mot sur $h x h^{-1}$ et $h r_i h^{-1}$.
Donc nous pouvons écrire $T^{-1} = h L_1 h^{-1}$ dans G_2 , où L_1 est un mot sur x et r_i .

K est un mot sur $q_1^{-1} h r_i h^{-1} q_1$ et $q_1^{-1} h x h^{-1} q_1$, donc on peut écrire

$K = q_1^{-1} h L_2 h^{-1} q_1$, où L_2 est un mot sur x et r_i .

On a donc $V_r h L_1 h^{-1} h q_1^{-1} h^{-1} q_1 = q_1^{-1} h L_2 h^{-1} q_1$ dans G_2

$$\text{soit } V_r h L_1 q_1^{-1} = q_1^{-1} h L_2$$

$$\text{soit } L_2^{-1} h^{-1} q_1 V_r h L_1 = q \text{ dans } G_2.$$

Remarquons que $V_r h$ est librement réduit puisque V_r est un mot librement réduit sur a_1, \dots, a_m et $h \notin \langle a_1, \dots, a_m \rangle$. Avec ces hypothèses on peut appliquer le lemme II.2.5 et donc $V_r h$ est un mot positif (donc en particulier V_r) et $h q_1 V_r h = q$ dans $\Gamma(T)$.

Et donc, $V_r \in E$.

En écrivant $V \equiv V' t_o^{\varepsilon_r} V_r$, et avec $U \equiv k_o^{\varepsilon} V k_o^{-\varepsilon}$.

U contient un sous-mot de la forme $t_o^{\varepsilon_r} V_r k_o^{-\varepsilon}$ où $V_r \in E$, ce qui contredit nos hypothèses. Donc U ne contient pas à la fois k_o et t_o , et donc (comme nous l'avons vu précédemment) $U \equiv 1$.

Donc le relateur $k_o^{-1} \omega^{-1} t_o \omega k_o = \omega^{-1} t_o \omega$, suffit à décrire A . ■

Lemme II.3.7 : G_7 est une HNN extension de G_6 , ayant pour lettres stables $\langle \sigma \rangle$.

démonstration : Il est clair que G_7 a pour base G_6 et pour lettre stable $\langle \sigma \rangle$.

Nous devons vérifier la condition de l'isomorphisme, i.e., vérifier qu'il existe un isomorphisme.

$$\psi : \langle k_o, t_o, a_1, \dots, a_m \rangle_{\sigma} \longrightarrow \langle k_o, t_o d, a_1, \dots, a_m \rangle_{\sigma}.$$

$$\text{avec } \psi(k_o) = k_o$$

$$\psi(t_o) = t_o d$$

$$\psi(a_p) = a_p$$

Puisque $G' \leq G_5 \leq G_6$, on a $\langle k_o, t_o, a_1, \dots, a_m \rangle_{\sigma} = \langle k_o, t_o, a_1, \dots, a_m \rangle_4 = A$, dont nous avons donné une présentation au lemme II.3.6.

Dans la suite nous appellerons B , $\langle k_o, t_o d, a_1, \dots, a_m \rangle_{\sigma}$. Pour montrer que $A \longrightarrow B$ est un homomorphisme il nous faut montrer que l'image des relateurs de A est triviale dans G_6 i.e., il nous faut montrer

que si $\omega \in E$, $k_o^{-1} \omega^{-1} t_o d \omega k_o = \omega^{-1} t_o d \omega$ dans B .

Nous le montrerons dans G_6 . Ce sera à fortiori vrai dans B .

Nous utiliserons la notation suivante :

Soit ω un mot sur a_1, \dots, a_m .

ω_b est obtenu à partir de ω , en changeant tous les a_i en b_i .

ω_u est obtenu à partir de ω , en changeant tous les a_i en u_i .

Remarquons que si $\omega \in E$, $\omega_u = 1$ dans G_6 puisque alors ω_u est un relateur de R et $R \leq G_4 \leq G_5 \leq G_6$.

Considérons $\omega \in E$. On a dans G_6

$$\begin{aligned} k_o^{-1} \omega^{-1} t_o d \omega k_o &= k_o^{-1} \omega^{-1} t_o (d \omega d^{-1}) d k_o \\ &= k_o^{-1} \omega^{-1} t_o \omega \omega_b d k_o \end{aligned}$$

En effet, puisque $da_i d^{-1} = a_i b_i$, $d \omega d^{-1} = da_{v(1)} d^{-1} da_{v(2)} d^{-1} \dots$

$$da_{v(l)} d^{-1}$$

$$= a_{v(1)} b_{v(1)} \dots a_{v(l)} b_{v(l)}$$

$$= \omega \omega_b$$

et a_i et b_i commutent dans $G_5 \leq G_6$.

De plus dans G_5 (donc dans G_6) b_i et u_j commutent pour tout i, j

$= 1 \dots n$, et $k_o^{-1} b_i k_o = b_i u_i$, k_o et d commutent dans G_6 .

$$\begin{aligned} \text{Et alors } k_o^{-1} \omega^{-1} t_o \omega \omega_b d k_o &= k_o^{-1} \omega^{-1} t_o \omega \omega_b k_o d \\ &= k_o^{-1} \omega^{-1} t_o \omega k_o (k_o^{-1} \omega_b k_o) d \\ &= k_o^{-1} \omega^{-1} t_o \omega k_o \omega_b \omega_u d \\ &= (k_o^{-1} \omega^{-1} t_o \omega k_o) \omega_b d \\ &= \omega^{-1} t_o \omega \omega_b d \end{aligned}$$

Relation (**).

$$\text{Or } \omega^{-1} t_o d \omega = \omega^{-1} t_o (d \omega d^{-1}) d$$

$$= \omega^{-1} t_o \omega \omega_b d$$

et on a donc montré que :

$$k_o^{-1} \omega^{-1} t_o d \omega k_o = \omega^{-1} t_o d \omega \text{ dans } G_6.$$

Donc : $\varphi : A \longrightarrow B$ est un homomorphisme.

Nous construisons maintenant $\psi : G_6 \longrightarrow G_6$ dont la restriction à B , est l'inverse de φ .

Définissons ψ par $\psi(d) = \psi(b_i) = \psi(u_i) = 1$

et $\psi|_{G'} = \text{Id}_{G'}$ est bien défini,

et au vu des relateurs de G_6 (regarder les présentations de G_5 et G_6), ψ est bien défini (si r est un relateur de G_6 , $\psi(r) = 1$ dans G_6).

$$\begin{aligned} \text{Et l'on a } \psi|_B \circ \varphi &= \text{Id}_A \\ \varphi \circ \psi|_B &= \text{Id}_B. \end{aligned}$$

C. Q. F. D. ■

Nous avons donc , avec tout ce qui précède , vérifié que nous avons la chaîne de Britton .

$$R \subseteq G_4 \leq G_5 \leq G_6 \leq G_7$$

Donc R est plongé dans G_7 . Remarquons que G_7 est finement engendré . Nous allons maintenant démontrer que G_7 est finement présenté .

Lemme II.3.8 : G_7 est finement présenté .

démonstration : Rappelons nous que nous avons pris pour présentation de G_4 , la réunion des générateurs et relateurs de G' et R .

Si dans G_4 , on élimine les relateurs de la forme $\omega_u = 1$, où $\omega \in E$ (i.e. les relations de R) , alors il ne reste qu'un nombre fini de relateurs .

Au vu de la construction de G_6 , la même conclusion est vraie dans G_6 .

Nous affirmons que les relateurs de G_6 de la forme $\omega_u = 1$ ($\omega \in E$) , peuvent être obtenus grâce aux relateurs restant .

Si $\omega \in E$ alors $k_o^{-1}(\omega^{-1}t_o\omega)k_o = (\omega^{-1}t_o\omega)$ dans G' . (égalité (**)) de la démonstration précédente , en prenant $\omega_b d \equiv 1$)

Donc l'égalité est vraie dans G_6 et ne nécessite l'utilisation que des relateurs restant , pour être établie .

Alors $\sigma^{-1}(k_o^{-1}\omega^{-1}t_o\omega k_o)\sigma = \sigma^{-1}\omega^{-1}t_o\omega\sigma$
puisque σ commute avec les a_i et k_o

$$k_o^{-1}\omega^{-1}\sigma^{-1}t_o\sigma\omega k_o = \omega^{-1}\sigma^{-1}t_o\sigma\omega$$

De plus $k_o^{-1}\omega^{-1}t_o d \omega k_o = \omega^{-1}t_o d \omega$ (cf la démonstration du lemme précédent) .

Ce qui nous donne :

$$k_o^{-1}\omega^{-1}t_o(\omega k_o k_o^{-1}\omega^{-1})d\omega k_o = \omega^{-1}t_o(\omega\omega^{-1})d\omega , \text{ qui peut}$$

s'écrire $(k_o^{-1}\omega^{-1}t_o\omega k_o)k_o^{-1}\omega^{-1}d\omega k_o = (\omega^{-1}t_o\omega)\omega^{-1}d\omega$.

Or les termes entre parenthèses sont égaux .

$$\text{Et donc } k_o^{-1}\omega^{-1}d\omega k_o = \omega^{-1}d\omega . \quad (1)$$

Comme nous l'avons déjà vu , les relations $d^{-1}a_i b_i d = a_i$ et $a_i b_j =$

$b_j a_i$, nous donnent :

$$\begin{aligned} d\omega d^{-1} &= \omega \omega_b, \text{ qui peut s'écrire } \omega = d^{-1} \omega \omega_b d \\ \text{et alors } \omega^{-1} d\omega &= \omega^{-1} d d^{-1} \omega \omega_b d \\ &= \omega_b d \end{aligned} \quad (2)$$

On substitue (2) dans (1) .

$$k_o^{-1} \omega_b d k_o = \omega_b d$$

or k_o et d commutent

$$\text{donc } k_o^{-1} \omega_b k_o = \omega_b \quad (3)$$

Avec les relations $k_o^{-1} b_i k_o = b_i u_i$ et $b_i u_j = u_j b_i$ appliquées à (3)

, on a $\omega_b \omega_u = \omega_b$ soit $\omega_u = 1$ dans G_σ . ■

Le théorème de Higman ,est donc établi .

II.3.2 Théorème de Higman-Neumann-Neumann

Dans ce paragraphe ,nous allons établir le théorème de Higman-Neumann-Neumann .Nous combinerons alors ce résultat avec le théorème de Higman ou le théorème de Novikov-Boone pour en déduire des résultats utiles à la suite .

Nous utiliserons pour la démonstration du théorème de H.N.N. ,le lemme suivant ,qui nous sera aussi utile ,dans le paragraphe suivant .

Lemme II.3.9 : Soit K un groupe donné par une présentation sur un ensemble fini ou dénombrable de générateurs

$$K = \langle x_1, x_2, \dots \mid R_1 = 1, R_2 = 1, \dots \rangle$$

Considérons $\omega \in K$, on construit L_ω , le groupe obtenu à partir de la présentation de K , en ajoutant trois générateurs a ; b ; c ,et les relateurs suivant :

$$(1) \quad a^{-1} b a = c^{-1} b^{-1} c b c$$

$$(2) \quad a^{-2} b^{-1} a b a^2 = c^{-2} b^{-1} c b c^2$$

$$(3) \quad a^{-3} [\omega, b] a^3 = c^{-3} b c^3$$

$$(4) \quad a^{-(3+i)} x_i b a^{3+i} = c^{-(3+i)} b c^{3+i} \text{ pour } i = 1, 2, \dots$$

où $[\omega, b] = \omega^{-1} b \omega b^{-1}$.On a alors :

- (i) Si $\omega \neq_K 1$, alors K est plongé dans L_ω , par l'inclusion sur les générateurs.
- (ii) La clôture normale de ω dans L_ω est L_ω . En particulier si $\omega =_K 1$ alors $L_\omega \cong 1$.
- (iii) L_ω est engendré par les 2 éléments b et ca^{-1} .
- (iv) Si la présentation de K est finie, alors la présentation de L_ω est aussi finie.

Démonstration : (i) Prenons $\omega \neq_K 1$. On considère le groupe libre $\langle b, c \rangle$, et son sous-groupe C , engendré par les membres de droite des égalités (i) à (iv).

Ce sous-groupe est librement engendré sur les générateurs, puisque si on effectue un produit de puissances de générateurs de C , Les réductions entre les mots n'auront lieu qu'au extrémités et laisseront des sous-mots médians inchangés (c'est une base de Nielsen).

De façon similaire, on considère $K * \langle a, c \rangle$, et le sous-groupe A engendré par les membres de gauche des inégalités. Avec $\omega \neq_K 1$, comme précédent, A est librement engendré par ces générateurs. Il existe donc un isomorphisme $A \rightarrow C$ qui envoie les membres de gauche, sur les membres de droite correspondants. L_ω est alors le produit libre amalgamé $(K * \langle a, b \rangle)_{A=C} * \langle b, c \rangle$.

Ainsi si $\omega \neq_K 1$ alors K est plongé dans L_ω par l'inclusion sur les générateurs. \square

Remarquons que si l'on considère le groupe L n'ayant pour relations que (1) et (4), alors le même raisonnement montre que K est plongé dans L (avec ω quelconque), par l'inclusion sur les générateurs.

(ii) Appelons N_ω , la clôture normale de ω dans L_ω . $[\omega, b] = \omega^{-1}(b \omega b^{-1})$, et donc $[\omega, b] \in N_\omega$. Alors avec le relateur (3) $b = c^3 a^{-3} [\omega, b] a^3 c^{-3}$, et donc $b \in N_\omega$. Avec le relateur (1), $c = b c a^{-1} b a c^{-1} b^{-1}$, et donc $c \in N_\omega$. De même on peut voir aisément avec la relation (2) que $a \in N_\omega$. Les relations de la forme (4) peuvent alors être utilisées, pour exprimer x_i ($i = 1, 2, \dots$), en fonction de a, b , et c , et donc $x_i \in N_\omega$, $i = 1, 2, \dots$. Donc $N_\omega = L_\omega$. \square

(iii) Appelons L , le sous-groupe de L_ω , engendré

par b et ca^{-1} . Avec la relation (1), $c = b (ca^{-1})b (ca^{-1})^{-1} b^{-1}$, donc $c \in L$ et puisque $ca^{-1} \in L$, $a \in L$. De plus la relation (4) nous permet d'exprimer x_i , pour $i = 1, 2, \dots$, en fonction de a, b, c , donc $x_i \in L$ pour $i = 1, 2, \dots$. Finalement on a donc $L = L_\omega$. \square

(iv) Il est clair que si la présentation de K est finie, alors il y a un nombre fini de générateurs x_i , et donc de relations de la forme (1), (2), (3), (4). La présentation donnée de L_ω , est alors finie. \blacksquare

Remarques Remarquons que les relations (2) et (3) n'ont pas été utilisées dans la démonstration de (iii). La conclusion (iii) est donc toujours valide sous des hypothèses simplifiées, obtenues en ne considérant pas les relations (2) ou (et) (3). De même si l'on considère les mêmes hypothèses, avec un groupe L , et uniquement les relations (1) et (4), alors K est plongé naturellement dans L (i.e. par l'inclusion sur les générateurs). C'est avec des hypothèses simplifiées que nous utiliserons, dans ce paragraphe le lemme II.3.9.

Un groupe dénombrable, i.e ayant un nombre dénombrable d'éléments, admet un ensemble dénombrable de générateurs.

THEOREME II.3.2 : (Higman, Neumann, Neumann)

Tout groupe dénombrable G peut être plongé dans un groupe H ayant deux générateurs. De plus si G admet N relations, H peut être choisi avec N relations.

Démonstration : Considérons un groupe dénombrable G , et construisons comme dans le lemme précédent, un groupe L avec uniquement les relations (1) et (4). Avec le lemme II.3.9, et les remarques précédentes, G est plongé dans L , et L admet deux générateurs b et ca^{-1} .

De plus supposons que G ait N relations. La relation (1) permet d'exprimer c en fonction de b et ca^{-1} , et donc on peut avec des changements de Tietze, la supprimer.

On a avec la relation (iv), $x_i = (ca^{-1})^{-(3+i)} b (ca^{-1})^{3+i} b^{-1}$, et on peut donc réécrire les relateurs de G sur b et ca^{-1} , et ensuite

supprimer la relation (iv) . Le groupe L peut donc s'écrire avec deux générateurs et N relations . ■

Corollaire II.3.1.1 : Il existe un groupe f.p. , ayant deux générateurs , ayant un problème du mot récursivement insoluble .

Démonstration : Le théorème de Novikov établit l'existence d'un groupe finiment présenté ayant un problème du mot insoluble . Avec le théorème de H.N.N. , ce groupe peut être plongé dans un groupe finiment présenté ayant deux générateurs . Puisque le problème du mot est héréditaire , le résultat est établi .

Corollaire II.3.2.1 : Tout groupe récursivement présenté peut se plonger dans un groupe f.p. , ayant deux générateurs .

Démonstration : Soit un groupe récursivement présenté , alors avec le théorème de Higman , on peut le plonger dans un groupe f.p. . Avec le théorème de H.N.N. , ce groupe f.p. peut être plongé dans un groupe f.p. admettant deux générateurs . ■

II.4 PROPRIÉTÉ DE MARKOV ET THEOREME DE ADJAN-RABIN

Definition : Soit P une propriété sur les groupes finiment présentés . Nous disons que P est une propriété de Markov si il existe 2 groupes finiment présentés G_+ et G_- tels que :

- (i) G_+ vérifie la propriété P
- (ii) Si G_- est plongé dans un groupe H , alors H ne vérifie pas la propriété P .

Remarque: Il est clair que G_- ne vérifie pas la propriété P , puisqu'il se plonge dans lui-même .

Exemples: Etre fini est une propriété de Markov . On peut prendre $G_+ = \langle a \mid a^5 = 1 \rangle$ et $G_- = \langle b \rangle$. Tout groupe contenant G_- (i.e. le groupe cyclique infini) comme sous-groupe est infini .

Etre hyperbolique est une propriété de Markov , il suffit de prendre $G_+ = \langle a \rangle$, et $G_- = \mathbb{Z} \times \mathbb{Z}$. En effet tout groupe

libre de rang fini est hyperbolique ,et si G est hyperbolique alors G ne contient pas $\mathbb{Z} \times \mathbb{Z}$ comme sous groupe (c.f. cours de D.E.A 94/95 de H.Short).

Définitions : On dit d'une propriété P sur les groupes finiment présentés qu'elle est héréditaire si ,lorsque $G \in P$ et H est plongé dans G , $H \in P$ (où H et P sont f.p.) .

On dit d'une propriété qu'elle est non triviale si $P \neq \emptyset$ et si elle n'est pas vérifiée par tous les groupes finiment présentés .

Lemme II.4.1 : Si P est une propriété sur les groupes finiment présentés ,héréditaire et non triviale ,alors P est une propriété de Markov .

Démonstration : Puisque P est non triviale ,il existe un groupe f.p. vérifiant P ; appelons le G_+ .De même il existe un groupe G_- f.p. ne vérifiant pas P .

Supposons que G_- soit plongé dans Γ , où Γ est un groupe f.p. $\Gamma \notin P$ car si $\Gamma \in P$,puisque P est héréditaire ,alors $G_- \in P$. P est donc une propriété de Markov . ■

Ce résultat nous donne un moyen simple de trouver "beaucoup" de propriétés de MARKOV . Par exemple :

- Etre trivial
- Etre libre
- Etre abélien
- Etre fini
- Etre sans torsion
- Avoir un centre trivial
- Etre cyclique infini (respectivement fini)
- Etre nilpotent
- Etre solvable
- Etre automatique
- Avoir un problème du mot récursivement soluble .

Le but de cette partie est de démontrer les théorèmes suivants :

Théorème II.4.1 : (Adjan-Rabin)

Soit P une propriété de Markov sur les groupes finiment présentés. Il existe une classe récursive de présentations finies de groupe $\langle \Pi_\omega / \omega \in U \rangle$, indexées sur un groupe U , où U a un problème du mot récursivement insoluble telle que $gp(\Pi_\omega) \in P$ ssi $\omega =_U 1$.

Définition : On dit d'une propriété P sur les groupes finiment présentés, qu'elle est récursivement reconnaissable, si l'ensemble des présentations finies $\langle \Pi / gp(\Pi) \in P \rangle$ est récursif. Dans le cas contraire, on dit que P est récursivement irreconnaissable.

Théorème II.4.2 : (Adjan-Rabin)

Toute propriété de Markov sur les groupes f.p. est récursivement irreconnaissable.

Théorème II.4.3 : (Adjan-Rabin)

Le problème de l'isomorphisme pour les groupes finiment présentés est récursivement insoluble.

Les théorèmes II.4.2 et II.4.3 sont corollaires du théorème II.4.1. Nous allons donner une preuve du théorème II.4.1, en utilisant le lemme II.3.9.

Démonstration du théorème II.4.1 :

Soient une propriété de Markov P , et les groupes G_- et G_+ correspondant. On considère un groupe U finiment présenté ayant un problème du mot insoluble.

Soit $K = U * G_-$, puisque U a un problème du mot insoluble, il en est de même de K . U et G_- sont naturellement plongés dans K . Soit un mot de U , et son représentant w dans K . On construit alors L_w , comme dans le lemme II.3.9. Remarquons qu'étant donné une présentation finie, on peut reconnaître si c'est une présentation de la forme II.3.9 i.e. l'ensemble des présentations ainsi construites est récursif. On forme alors $L_w * G_+$, dont une présentation finie Π_w s'obtient naturellement par les présentations finies de L_w et de G_+ (et ainsi l'ensemble de telle présentations est récursif).

Si $w \neq 1$ dans H , alors avec le lemme II.3.9, G_- est plongé dans $L_w * G_+$, et alors $L_w * G_+$ ne vérifie pas P . Par contre si

$\omega = 1$ dans U , alors $L_\omega \cong 1$, et donc $L_\omega * G_+ \cong G_+$, et vérifie donc P . Ainsi on peut construire une classe récursive de présentations $\langle \Pi_\omega / \omega \in H \rangle$, tel que $\text{gp}(\Pi_\omega) \in P$ ssi $\omega = 1$ dans U . ■

Démonstration du théorème II.4.2 :

Soit P une propriété de Markov. Supposons que P soit récursivement reconnaissable i.e. $\langle \Pi / \text{gp}(\Pi) \in P \rangle$ est récursif. On forme, comme dans le théorème II.4.1, une famille récursive de présentations finies $\langle \Pi_\omega / \omega \in U \rangle$, telle que $\text{gp}(\Pi_\omega) \in P$ ssi $\omega =_U 1$. Alors leur intersection $I = \langle \Pi_\omega / \omega \in U \text{ et } \text{gp}(\Pi_\omega) \in P \rangle$ est récursive. Ainsi on peut décider pour tout mot ω sur U , si $\omega =_U 1$, en construisant sur ω la présentation Π_ω du lemme II.3.9 (ce qui est effectivement réalisable), et en décidant si $\Pi_\omega \in I$. Ceci contredit le fait que U ait un problème du mot récursivement insoluble. ■

Démonstration du théorème II.4.3 :

Supposons que $\langle \langle \Pi, \Pi' \rangle / \text{gp}(\Pi) \cong \text{gp}(\Pi') \rangle$ est récursif (où Π et Π' sont des présentations finies de groupe). L'ensemble $\langle \langle \Pi, \langle a/a \rangle \rangle \rangle$ est récursif puisque $\langle \Pi \rangle$ est récursif, et alors, en formant l'intersection $\langle \Pi / \text{gp}(\Pi) \cong 1 \rangle$ est récursif, ce qui contredit le théorème II.4.2, puisque être trivial est une propriété de Markov pour les groupes f.p. ■

Ainsi même pour des propriétés aussi simple qu'être trivial, le on ne peut reconnaître les présentations finies de groupe vérifiant ces propriétés. W. W. Boone démontre dans [6] un théorème plus fort :

Théorème II.4.4 : (Boone)

Soit U un groupe f.p. ayant un problème du mot de degré D . Il existe une classe récursive de présentations finies $\langle \Pi_\omega / \omega \in U \rangle$, telle que $\Pi_\omega \cong 1$ ssi $\omega =_U 1$.

Avec le théorème II.4.2, on ne peut pas décider pour une présentation finie donnée, si le problème du mot y est résoluble. Remarquons que dans le cas des propriétés être trivial, être fini, être abélien, être libre, on peut néanmoins énumérer toutes les

présentations finies les vérifiant .En effet on connaît des présentations canoniques des groupes vérifiant ces propriétés ,et on peut donc utiliser l'algorithme du corollaire I.2.1.1 ,pour énumérer toutes les présentations finies de tels groupes .Qu'en est il pour les groupes f.p. ayant un problème du mot soluble ? .

Théorème II.4.5 : (Boone,Rogers)

Pour les groupes finiment présentés , la propriété d'avoir un problème du mot soluble est Σ_3^0 -complète .En particulier ,on ne peut pas énumérer tous les groupes f.p. ayant un problème du mot récursivement soluble .

Pour une démonstration de ce résultat ,voir [7] .Pour la notion de Σ_3^0 -complet ,voir [34] .

CHAPITRE III :

PROBLEMES DE DEHN POUR DES GROUPES ELEMENTAIRES

Dans le chapitre précédent nous avons établi l'existence de groupes f.p. ayant des problèmes de Dehn insolubles ,mais nous n'avons explicité aucune présentation d'un tel groupe .Dans ce chapitre nous nous intéressons à ces problèmes dans des groupes élémentaires ,i.e. définis par des propriétés algébriques élémentaires ,ou construits à partir d'un groupe libre par une chaîne de constructions élémentaires .Même si nous démontrons des résultats de solubilité ,le but principal de ce chapitre ,est d'établir des problèmes d'insolubilités dans de tels groupes .

I.1 RESOLUTION DES PROBLEMES DE DEHN POUR LES GROUPES LIBRES

Nous avons déjà vu que le problème du mot est soluble pour les groupes libres ,par application de réductions libres .De plus le problème de l'isomorphisme est soluble puisque tout groupe libre admet une présentation canonique $\langle F(X) \rangle$ où $|X| = \text{rang } F$.On peut donc étant données 2 présentations de groupes libres ,énumérer toutes leurs présentations ,par changements de Tietze ,jusqu'à ce que l'on obtienne leur présentations canoniques ,et alors $F(X) \cong F(Y)$ ssi $|X| = |Y|$.

Dans cette partie nous démontrons que les autres problèmes de Dehn ,sont résolubles pour les groupes libres (de rang quelconque)

III.1.1 Problème de la conjugaison

Définition : Un mot sur X ,est dit cycliquement réduit ,si il est réduit ,et si il n'est pas de la forme $x^{-1}\mu x$,avec $x \in X \cup X^{-1}$.

Remarquons que si un mot est cycliquement réduit ,il en est de même de tous ses conjugués cycliques .

Lemme III.1.1: Soit w un mot cycliquement réduit sur un alphabet S

. Un mot réduit ω' sur S est un conjugué de ω dans $F(S)$ ssi , un conjugué cyclique de ω est un conjugué cyclique ,cycliquement réduit de ω' .

Démonstration : (\Rightarrow) Supposons que $\omega' = h^{-1}\omega h$ dans $F(S)$,où h est un mot réduit sur S . Alors puisque ω et h sont réduits ,les seules réductions possibles dans $h^{-1}\omega h$,sont à la liaison entre h^{-1} et ω ,ou entre ω et h . Soit il existe a et b mots réduits (évent. vides)sur S tels que $h \equiv a h' \equiv b h''$; et $\omega \equiv a \omega_0 b^{-1}$. Sans perte de généralité ,on peut supposer que b soit un sous-mot initial de a . Et alors $\omega \equiv b \omega_1 b^{-1}$,et donc puisque ω est cycliquement réduit , b est le mot vide . Une réduction dans $h^{-1}\omega h$,ne peut donc intervenir (sans perte de généralité) ,qu'entre h^{-1} et ω ,soit $h \equiv a h'$, $\omega \equiv a \omega_0$ (et ω_0 ne contient pas un segment terminal de a^{-1} ,comme sous-mot terminal) .
Donc $h^{-1}\omega h \equiv (a h')^{-1} a \omega_0 (a h') \equiv h'^{-1} \omega_0 a h' \equiv \omega'$ (prop I.1.1).
Or $\omega_0 a$ est cycliquement réduit ,et donc la réduction cyclique d'un conjugué cyclique de ω' ,est un conjugué cyclique de ω . \square

(\Leftarrow) Considérons $\omega \equiv A B$,et supposons que $B A$ soit la réduction cyclique d'un conjugué cyclique de ω' . Alors puisque ω est cycliquement réduit , $B A$ est cycliquement réduit (prop vv),et puisque ω' est réduit on a un des cas suivants :

1^{er} cas : $\omega' \equiv X^{-1} B A X$,où X est un mot (éventuellement vide) sur S . Alors $\omega' = X^{-1} B (A B) B^{-1} X = (B^{-1} X)^{-1} \omega (B^{-1} X)$.

2^{ème} cas : $B A$ est un conjugué cyclique de ω' . Soit (par exemple) , $B \equiv B_1 B_2$,et $\omega' \equiv B_2 A B_1$,et donc $\omega' = B_2 A B_1 B_2^{-1}$
$$= B_2 \omega B_2^{-1}$$

Tout autre cas serait contradictoire avec le fait que ω' soit réduit . \blacksquare

LEMME III.1.2: ω est conjugué de ω' ,ssi la réduction cyclique de ω est conjugué de ω' .

Démonstration : Soit ω_0 la réduction cyclique de ω ,i.e $\omega \equiv X^{-1} \omega_0 X$,où X est un mot sur S ,et ω_0 est cycliquement réduit .

(\Rightarrow) Soit $\omega' = h^{-1}\omega h = h^{-1} X^{-1} \omega_0 X h = (X h)^{-1} \omega_0 X h$ \square

(\Leftarrow) Soit $\omega' = h^{-1} \omega_0 h = h^{-1} X X^{-1} \omega_0 X X^{-1} h = (X^{-1} h)^{-1} \omega_0 X^{-1} h$ \blacksquare

PROPOSITION III.1.1 : Le problème de la conjugaison pour les groupes libres est récursivement résoluble .

Démonstration : Considérons un groupe libre ,donné par sa présentation canonique (pas de relateurs) . Soient deux mots ω et ω' exprimés sur les générateurs . On réduit cycliquement ω ,et l'on détermine tous les conjugués cycliques de ω' ,et de la réduction cyclique de ω (ils sont en nombre fini). On peut alors réduire cycliquement ceux de ω' ,et avec les lemmes III.1.1 et III.1.2 ,on peut décider si ω et ω' sont conjugués . ■

III.1.2 Problème du mot généralisé

Le problème du mot généralisé dans un groupe libre ,se résoud grâce à la notion de base de Nielsen .

Notation : Soit $F(X)$ un groupe libre et $W = \langle w_1, \dots, w_n \rangle$ un ensemble fini de mots réduits sur X ; qui engendre un sous-groupe G de $F(X)$. Tout élément de G , peut se donner comme un mot réduit sur W , ω . On note $\omega(X)$ le mot ω vu comme un mot sur X . Il est clair que ω et $\omega(X)$ représentent le même élément du groupe . On note $\text{lgr}_X(\omega) = \text{lgr}(\omega(X))$.

D'après le théorème de Nielsen-Schreier , G est un groupe libre . Néanmoins G n'est pas forcément engendré librement par W (considérer le sous-groupe de F_2 , engendré par $\langle x_1, x_1^{-1}x_2^{-1}, x_2 \rangle$) .

Définition : Soit W un ensemble de mots réduits sur X , qui engendre un sous-groupe G de $F(X)$. On dit que W est une base de Nielsen de G , si les conditions suivantes sont vérifiées :

(1) Si ω est un mot réduit sur W , $\omega \equiv W_{i(1)}^{\epsilon_1} \dots W_{i(k)}^{\epsilon_k}$, alors la réduction de $\omega(X)$ (dans X) laisse au moins une lettre de chaque W_i ayant une occurrence dans ω ; inchangée (i.e. , on n'a pas $W_i^{\epsilon_i}(X) W_j^{\epsilon_j}(X) W_k^{\epsilon_k}(X) = W_i^{\epsilon_i} W_j^{\epsilon_j} W_k^{\epsilon_k}$, où $W_i^{\epsilon_i} W_j^{\epsilon_j} W_k^{\epsilon_k}$ est un sous-mot de ω , et $W_i^{\epsilon_i}$ (resp^t $W_k^{\epsilon_k}$) est un sous-mot initial (resp^t terminal) de $W_i^{\epsilon_i}(X)$ (resp^t de $W_k^{\epsilon_k}(X)$) .

(2) $\text{lgr}_X(\omega) \geq \text{lgr}_X(W_i)$, pour tout i tel que W_i ait une occurrence dans ω .

Remarque : Si W est une base de Nielsen de G , alors G est librement engendré par W . En effet pour tout mot non vide, réduit $w(W)$, la réduction de $w(X)$ est non vide grâce à (1), et donc $\bar{w} \neq 1$.

Proposition III.1.2 : Soient $F = F(X)$ un groupe libre, et W une famille finie de mots réduits non vides sur X , qui engendrent un sous-groupe G de F . Alors on peut construire une base de Nielsen de G .

Démonstration : Etant donné un ensemble fini W de mots sur X , on peut effectivement le symétriser (i.e considérer le plus petit ensemble \tilde{W} contenant W tel que si $w \in \tilde{W}$, alors $w^{-1} \in \tilde{W}$ où w^{-1} est le mot inverse de w sur X). Clairement W et \tilde{W} engendrent le même sous-groupe de $F(X)$, et on peut donc considérer dans la suite un ensemble W , symétrisé. Tous les mots seront vus comme des mots sur X .

La démonstration utilise la notion de transformations de Nielsen. Nous allons démontrer, que pour toute famille W vérifiant les hypothèses, on peut construire une suite finie de transformations de Nielsen, changeant W , en une base de Nielsen de G .

On appelle Produit propre (PP) U'_i de U_i (par U_j), le mot réduit $U'_i =_F U_i U_j$, ou $U'_i =_F U_j U_i$; où $U_i, U_j \in W$, et $U_i \neq U_j$, et $U_i \neq U_j^{-1}$.

On appelle produit propre de longueur moindre (PPLM), un produit propre U'_i de U_i , tel que $\text{lgr}_X(U'_i) < \text{lgr}_X(U_i)$.

Une transformation de Nielsen réduisant les longueurs (TNRL) de W est une transformation de $W = \langle U_1, \dots, U_i, \dots, U_k, \dots, U_n \rangle$, en $\langle U_1, \dots, U'_i, \dots, U'_k, \dots, U_n \rangle$, où U'_i est un PPLM de U_i par U_j , et où $U'_k = U_i^{-1}$ et $U'_i = U_k^{-1}$. Il est clair qu'une telle transformation change une famille symétrique finie, génératrice de G , en une famille symétrique, finie ; génératrice de G , puisque $\bar{U}_i = \bar{U}'_i \bar{U}_j$. Remarquons qu'un PPLM peut être un mot figurant déjà dans l'ensemble, et alors le nombre d'éléments peut être diminué de 2. De plus chaque TNRL, diminue (strict) la longueur de 2 de ses éléments. Donc puisque W est fini et que tout élément de W est de longueur minoré, toute suite de TNRL appliquée à W est finie.

Etant donné W , on peut effectivement construire une suite de

TNRL ,s'appliquant à W ,et aboutissant à W (i.e. $W \longrightarrow \dots \longrightarrow W$,où chaque flèche symbolise une TNRL) ,tel que W n'admette pas de PPLM .Pour cela on énumère tous les PPLM de W (en formant les produits propres de générateurs ,puis en les réduisant ,on peut décider si il s'agit d'un PPLM) ,ils sont en nombre fini (puisque W est fini) .Etant donné un PPLM ,on peut effectuer une TNRL ,et on réitère alors ce procédé à l'ensemble obtenu .Puisque toute suite de TNRL est fini ,on aboutit à un ensemble symétrique ,fini W ,engendrant G ,tel que pour tout PP V'_i ,de V_i dans W , $\text{lgr}_X(V'_i) \geq \text{lgr}_X(V_i)$,et donc tout PP de 2 éléments de W simplifie au plus la moitié de chaque générateurs .Si $W \neq W$ alors le cardinal de W est au plus le cardinal de W ,et la longueur des mots de W a été strictement diminuée ,par rapport à la longueur des mot de W .

Considérons maintenant un tel ensemble W .Il peut y avoir un mot de longueur paire de W , V_i ayant samoitié de droite et sa moitié de gauche se simplifiant par PP .Soit $V_i, V_j, V_l \in W$,tels que $V_i \equiv G D$ avec $\text{lgr}_X(G) = \text{lgr}_X(D) = \frac{1}{2} \text{lgr}_X(V_i)$; $V_j \equiv V'_j G^{-1}$; $V_l \equiv D^{-1} V'_l$ (On dit que V_i est simplifiable) .Puisque les simplifications réduisent au plus la moitié des générateurs , $\text{lgr}_X(V_j) \geq \text{lgr}_X(V_i)$,et $\text{lgr}_X(V_l) \geq \text{lgr}_X(V_i)$.Dans ce cas ,on appelle Transformation de Nielsen de même longueur (TNML) ,la transformation de W ,consistant à remplacer tous les éléments de la forme $V_j \equiv V'_j G^{-1}$,par les mots réduits de la forme $W_j =_F V'_j V_i =_F V'_j D$,et les V_j^{-1} par les W_j^{-1} .Il est clair que la famille obtenue est une famille symétrique ,fini ,et engendrant G .De plus $\text{lgr}_X(W_j) = \text{lgr}_X(V_j)$ (en fait $W_j \equiv V'_j D$) .En effet si l'on a $W_j \equiv V'_{j1} D_1^{-1} D_1 D_2$,avec $D \equiv D_1 D_2$,et D_1 est non vide ,alors V_j simplifie plus de la moitié de V_i .

Considérons une famille W ,comme précédemment .On peut lui appliquer une suite finie de TNML aboutissant à une famille finie symétrique génératrice de G ,n'ayant pas d'élément simplifiable .On procède de la façon suivante .

Prenons $W = \langle V_1, \dots, V_n \rangle$ où l'on a ordonné les éléments dans l'ordre de leur longueur .Supposons qu'il existe $i \in \langle 1, \dots, n \rangle$ tel que pour tout élément V_j avec $\text{lgr}_X(V_j) < \text{lgr}_X(V_i)$,n'est pas simplifiable .Supposons que W_i soit simplifiable .Alors on applique une TNML ,comme précédemment .Les nouveaux éléments sont de même longueur

,et prennent donc la même place .Remarquons que ce sont des éléments au moins de même longueur que V_i .Cette transformation ne change pas des éléments de longueur au plus la longueur de V_i ,non simplifiables ,en des éléments simplifiables .En effet supposons que $V_j \equiv L R$, $\text{lgr}_X(V_j) \leq \text{lgr}_X(V_i)$, $\text{lgr}_X(L) = \text{lgr}_X(R) \leq \text{lgr}_X(D)$.Supposons que $W_k \equiv V'_k D$,rende V_j simplifiable .Alors puisque $\text{lgr}_X(V'_k) \geq \text{lgr}_X(D)$,on a un des cas suivants :

1^{er} cas : L^{-1} est un sous-mot terminal de D ,et alors , V_j est aussi simplifiable en utilisant V_i .

2^{ème} cas : R^{-1} est un sous mot initial de V'_k et alors , V_j est aussi simplifiable en utilisant V_k .

Ainsi si V_j n'est pas simplifiable avant la TNML et si la longueur de V_j est au plus V_i , V_j n'est pas simplifiable après (et est inchangé).

Ainsi on peut alors effectuer des TNML successives à tous les éléments de même longueur que V_i ,et refaire l'opération avec $i + 1$,etcPuisque le cas $i = 1$ est vrai ,on peut alors effectuer une suite de TNML dans l'ordre des éléments de W .Puisque W est fini avec ce qui précède ,la suite de TNML est fini .On peut donc ,en testant successivement pour tout élément si il est simplifiable ,construire une suite finie de TNML ,aboutissant à un ensemble symétrique fini ,engeandrant G ,n'ayant pas d'éléments simplifiable .(par contre on peut avoir fait apparaître des PPML).

Revenons à W .On lui applique une suite de TNRL tant que c'est possible ,puis une suite de TNML ,tant que c'est possible ,et ainsi de suite .Une telle suite est finie .En effet ,chaque TNRL diminue les longueurs ,les TNML laissent les longueurs inchangées ,et le nombre d'éléments non vide est décroissant .Ainsi on aboutit au bout d'un temps fini ,en un ensemble W ,symétrique ,fini ,engendrant G .On considère W^* l'ensemble obtenu en retirant tous les inverses de W .Nous allons démontrer que W^* est une base de Nielsen pour G .

Soit ω un mot réduit sur W^* .On peut voir ω comme un mot positif sur W , $\omega \equiv W_{i(1)} \dots W_{i(k)}$.Alors au plus la moitié de chaque élément de W se réduit et ,aucun n'est simplifiable ,donc on vérifie (1) pour W^* .

On démontre (2) par induction sur la longueur de ω , k .

Si $k = 1$,la condition (2) et la moitié terminale du dernier

relateur n'est pas simplifiée .

Si (2) est vérifiée pour un mot w de longueur $k \geq 1$,et que la moitié terminale de dernier relateur de w n'est pas simplifiée ,
 ,on forme le mot réduit dans W^* , $w' = w W_{i(k+1)}$. Alors la réduction simplifie au plus la moitié de $\min \langle \text{lgr}_X(W_{i(k)}) , \text{lgr}_X(W_{i(k+1)}) \rangle$. Et donc $\text{lgr}_X(w') \geq \text{lgr}_X(w) + \text{lgr}_X(W_{i(k+1)}) - \min \langle \text{lgr}_X(W_{i(k)}) , \text{lgr}_X(W_{i(k+1)}) \rangle$

ce qui établit clairement (2) . De plus la moitié terminale de $W_{i(k+1)}$ n'est pas simplifiée . ■

Corollaire III.1.1 : Le problème du mot généralisé est résoluble dans la classe des groupes libres .

Démonstration : Considérons un ensemble fini W de mots réduits sur X . W engendre un sous-groupe G de $F(X)$. On applique la proposition III.1.2 pour construire une base de Nielsen \bar{W} de G . Considérons un mot w réduit sur X . Si $w \in G$, alors w est la réduction d'un mot U sur \bar{W} , et avec la condition (1) , $\text{lgr}_G(U) \leq \text{lgr}_X(w)$. De plus avec la condition (2) , chaque élément de \bar{W} a pour longueur dans X , au plus la longueur de w . On peut donc constituer tous les mots de \bar{W} , de longueur dans G , au plus $\text{lgr}_X(w)$, s'écrivant sur des mots de \bar{W} de longueur au plus , $\text{lgr}_X(w)$, puis en les réduisant librement , on peut décider si $w \in G$, et si c'est le cas , l'écrire comme un mot sur \bar{W} .

III.2 PROBLEMES DE DEHN ET CONSTRUCTIONS ALGEBRIQUES

Le but de ce paragraphe est d'étudier l'effet des constructions algébriques élémentaires sur des groupes f.p , sur les problèmes de Dehn locaux . Les constructions utilisées sont :

- Produit libre
- Produit direct
- Produit libre amalgamé sur des sous-groupes f.e.
- split extension

- HNN extension et extension de Britton

En particulier , nous établirons des résultats sur des groupes construits de façon élémentaire , sur des groupes libres . Les groupes libres sont intéressants , car tous les problèmes de Dehn sont résolubles pour les groupes libres . De plus ils ont un rôle fondamental en théorie des groupes .

Remarquons , que si deux groupes sont finiment présentés , le groupe construit dessus par les constructions précédentes sont f.p. . Pour les produits libres , produits libres amalgamés , extensions de Britton , et produit direct , ce résultat se vérifie immédiatement , en regardant la présentation canonique . Pour les splits extensions , le résultat est clair , puisque être f.p. est une poly-propriété . Remarquons de plus que toute HNN extension est une extension de Britton , et que tout produit direct de G et H , est une split extension de G par H (ou de H par G) .

Nous appellerons construction de niveau 1 , un produit libre , produit direct , produit libre amalgamé , de deux groupes libres ; une split extension d'un groupe libre par un groupe libre ; une HNN ou extension de Britton d'un groupe libre . Nous appellerons construction de niveau 2 , un produit libre , direct , ou libre amalgamé , d'un (resp^t) produit libre , direct , libre amalgamé de niveau 1 ; une split extension par un groupe libre , d'une split extension de niveau 1 ; une HNN ou extension de Britton d'une extension de Britton de niveau 1 . Similairement nous parlerons de construction de niveau N , une construction analogue sur un groupe de niveau $N - 1$. Tous les résultats de ce chapitre sur les constructions de niveau n sont regroupés dans le tableau 1

III.2.1 Produit libre

Dans tout ce paragraphe , on considère deux groupes f.p. $G = \langle S \mid R \rangle$ et $H = \langle S' \mid R' \rangle$. On se donne $G * H$ par sa présentation canonique $G * H = \langle S \cup S' \mid R \cup R' \rangle$ où $S \cap S' = \emptyset$, et donc $R \cap R' = \emptyset$. D'après le théorème d'écriture normale , tout élément g de $G * H$ peut s'écrire de façon unique comme une séquence g_1, \dots, g_n , où $\forall i = 1 \dots n - 1$, $g_i \neq 1$, et si $g_i \in G$ alors $g_{i+1} \in H$; si $g_i \in H$, $g_{i+1} \in G$, et $g_1 \in G$ ou H , tel que $g =$

$g_1 \dots g_n$. On définit alors la longueur d'un élément g par $\text{lgr}(g) = n$.

Remarquons que le produit libre de deux groupes libres, est encore un groupe libre. Ainsi pour tout produit libre de niveau n , ($n \in \mathbb{N}$), tous les problèmes de Dehn sont solubles.

Lemme III.2.1 : Si l'on a une solution au problème du mot de G et H , alors on a une procédure permettant d'exprimer tout mot de $G * H$, sous sa forme normale.

Démonstration : Prenons un mot w de $G * H$. Alors il s'écrit $w \equiv C_1 \dots C_n$ où C_1 est un mot sur S , C_2 est un mot sur S' etc... (Le cas dual est similaire et ne sera pas traité). Or puisque G (resp^t H) se plonge naturellement dans $G * H$ (i.e. par l'inclusion sur les générateurs), si C s'écrit sur S (resp^t S'), $\bar{C} \in G$ (resp^t H), où \bar{C} représente l'élément de $G * H$, représenté par le mot C . On a alors une écriture de w sous forme normale ssi $\forall i, C_i \neq 1$; c'est à dire ssi $C_1 \neq_G 1, C_2 \neq_H 1$, etc... Il est donc clair que si G et H ont un problème du mot soluble, on peut effectivement donner une écriture sous forme normale de tout mot exprimé sur la présentation de $G * H$. ■

Proposition III.2.1 : $G * H$ a un problème du mot soluble ssi G et H ont un problème du mot soluble.

Démonstration : Soient deux mots w et w' de $G * H$. D'après le lemme III.2.1, on peut donner une forme normale de w et w' . Puisque l'écriture sous forme normale est unique, si w et w' sont donnés par leur forme normale respective, g_1, \dots, g_n et h_1, \dots, h_m , $w = w'$ dans $G * H$ ssi $n = m$, et $g_i = h_i, \forall i = 1..n$. Ainsi puisque les g_i et h_i sont donnés par des mots de G ou de H , si l'on peut résoudre le problème du mot dans G et H , on peut résoudre le problème du mot dans $G * H$.

Réciproquement, $G \hookrightarrow G * H$, et $H \hookrightarrow G * H$, ainsi $WP(G) \leq WP(G * H)$, et $WP(H) \leq WP(G * H)$. ■

Pour le produit libre de deux groupes ayant un problème de conjugaison soluble, on a une solution au problème de conjugaison, similaire à celle des groupes libres.

Définition : considérons un élément g de $G * H$, ayant pour forme

normale g_1, \dots, g_n . g est dit cycliquement réduit si g_1 et g_n sont dans deux groupes (G ou H) distincts ou si $\text{lgr}(g) = 1$. Un conjugué cyclique de g est un élément $g' = g_{i+1} \dots g_n g_1 \dots g_i$ (en particulier c'est un conjugué de g). Remarquons que si g est cycliquement réduit, $g_{i+1}, \dots, g_n, g_1, \dots, g_i$ est une forme normale de g' , et g' est cycliquement réduit.

Si g n'est pas cycliquement réduit, on appelle réduction cyclique de g , l'élément g' cycliquement réduit, obtenu à partir de g par une suite de transformations de la forme :

$g \rightarrow g_0$, si g_1, \dots, g_n est une forme normale de g , g n'est pas cycliquement réduit, et $g_0 = g_1^{-1} g g_1$.

Puisque être conjugué est une relation transitive, il est clair que deux mots sont conjugués ssi leur réduction cyclique, sont conjuguées.

Proposition III.2.2 : Soient deux éléments cycliquement réduits, g et g' . Ils sont conjugués dans $G * H$ ssi

- (i) si $\text{lgr}(g) \neq 1$, alors g' est un conjugué cyclique de g .
- (ii) si $\text{lgr}(g) = 1$, alors $\text{lgr}(g') = 1$, et g et g' sont deux éléments conjugués dans G (resp^t dans H).

Démonstration : (\Rightarrow) (i) Supposons $\text{lgr}(g) \neq 1$. Soit h tel que $g' = h^{-1} g h$. Prenons g_1, \dots, g_n et h_1, \dots, h_m les formes normales respectives de g et h . $g' = h_m^{-1} \dots h_1^{-1} g_1 \dots g_n h_1 \dots h_m$. Puisque g_1 et g_n sont dans deux sous-groupes distincts, soit g_1 , soit g_n est dans le même sous-groupe que h_1 . Considérons le premier cas, le deuxième étant similaire. Alors puisque g' est cycliquement réduit, $h_m^{-1}, \dots, (h_1^{-1} g_1), \dots, g_n, h_1, \dots, h_m$ n'est pas une forme normale de g' (h_m^{-1} et h_m sont dans le même sous-groupe) et donc $h_1 = g_1$. On peut alors utiliser le même raisonnement jusqu'à arriver à un des 3 cas suivants :

1^{er} cas : si $m < n$, alors $g_i = h_i, \forall i = 1 \dots m$ et donc :

$$g' = g_{m+1} \dots g_n h_1 \dots h_m = g_{m+1} \dots g_n g_1 \dots g_m$$

et donc g' est un conjugué cyclique de g .

2^{ème} cas : si $m = n$, alors $g_i = h_i \forall i = 1 \dots n$, et donc $h = g$

et $g' = g$.

3^{ème} cas : si $n < m$, alors $h_i = g_i \quad \forall i = 1 \dots n$, et donc :

$$\begin{aligned} g' &= h_m^{-1} \dots h_{n+1}^{-1} h_1 \dots h_m \\ &= h_m^{-1} \dots h_{n+1}^{-1} g_1 \dots g_n h_{n+1} \dots h_m \\ &= h'^{-1} g h' \end{aligned}$$

avec h' ayant pour forme normale $h_{n+1} \dots h_m$, et donc $\text{lgr}(h') < \text{lgr}(h)$. On peut alors réutiliser les arguments de la démonstration avec h' en place de h . Et puisque $\text{lgr}(h') < \text{lgr}(h)$, on finira par arriver dans un des cas 1 ou 2. \square

$$\begin{aligned} (\Rightarrow)(ii) \quad g \text{ a pour forme normale } g_1, \text{ et } g' &= h^{-1} g h \\ &= h_m^{-1} \dots h_1^{-1} g_1 h_1 \dots h_m \end{aligned}$$

Or g' est cycliquement réduit et donc (par exemple) $g_1 = h_1$. D'où $g' = h_m^{-1} \dots h_2^{-1} h_1 \dots h_m = h_m^{-1} \dots h_2^{-1} g_1 h_2 \dots h_m$. On peut donc successivement utiliser le même argument et montrer que $h_i = g_i$ ou $h_i = g_i^{-1}, \forall i = 1 \dots m$. Donc h et g , et donc g' sont tous deux dans G (resp^t dans H), et g et g' sont donc conjugués dans G (resp^t dans H), et $\text{lgr}(g') = 1$. \square

(\Leftarrow) les cas (i) et (ii) sont triviaux \blacksquare

Proposition III.2.3 : $G * H$ a un problème de conjugaison soluble ssi G et H ont un problème de conjugaison soluble.

Démonstration : (\Leftarrow) Si G et H ont un problème de la conjugaison alors ils ont un problème du mot soluble. Pour deux mots w et w' de $G * H$ on peut donc déterminer une écriture sous forme normale (lemme III.2.1). De plus on peut effectivement réduire cycliquement ces formes normales par le procédé suivant. Si g_1, \dots, g_n est une forme normale non cycliquement réduite (ce que l'on peut aisément décider), on forme $g_2, \dots, g_n g_1$. Alors si $g_n g_1 \neq 1$, c'est cycliquement réduit. sinon on forme $g_3, \dots, g_{n-1} g_2$, et l'on réitère le procédé. Puisque G et H ont un problème du mot soluble, ce procédé est effectif. Alors avec la proposition III.2.2, si les formes normales de w et w' sont cycliquement réduites de longueur > 1 , w et w' sont conjugués ssi un conjugué cyclique de w' est égal à w . Puisque l'on peut se donner tous

les conjugués cycliques de w' , et que le problème du mot de $G * H$ est soluble, on peut décider si w et w' sont conjugués.

Si la lgr de w est 1, avec la proposition III.2.2 ; on peut utiliser la solution au problème de la conjugaison dans G ou H .

(\Rightarrow) prenons un élément de G (le cas de H est similaire). Il est de longueur 1, et donc d'après la proposition III.2.2, un élément lui est conjugué dans G ssi il lui est conjugué dans $G * H$. ■

III.2.2 Produit direct

On considère deux groupes finiment présentés $G = \langle S / R \rangle$ et $H = \langle S' / R' \rangle$. On se donne alors $G \times H$ par la présentation canonique : $G \times H = \langle S \cup S' / R \cup R' \rangle$, $[g, h] \forall g \in G, \forall h \in H$ (où $S \cap S' = \emptyset$). Alors pour tout mot sur cette présentation, $w \equiv g_1 h_1 \dots g_n h_n$, où les $g_i \in G$ et les $h_i \in H$. On peut l'écrire sous la forme canonique $(g_1 \dots g_n, h_1 \dots h_n)$ (les éléments de G et de H commutent).

PROPOSITION III.2.4 : Soient deux groupes finiment présentés, F et G , $G \times H$ a un problème du mot (resp^t de conjugaison) soluble ssi G et H ont un problème du mot (resp^t de conjugaison) soluble.

Démonstration : $(g, h) = (g', h')$ dans $G \times H \iff g =_G g'$ et $h =_H h'$. Donc si l'on a une solution au problème du mot dans G et H , on peut résoudre le problème du mot de $G \times H$.

On a de plus $G \hookrightarrow G \times H$ et $H \hookrightarrow G \times H$ donc $WP(G) \leq WP(G \times H)$ et $WP(H) \leq WP(G \times H)$.

Deux éléments de $G \times H$, (g, h) et (g', h') sont conjugués ssi $\exists (g_1, h_1)$ tel que $(g_1, h_1)^{-1} (g, h) (g_1, h_1) = (g_1^{-1} g g_1, h_1^{-1} h h_1) = (g', h')$

Donc ssi g et g' sont conjugués dans G , et h et h' sont conjugués dans H . Donc si l'on peut résoudre le problème de conjugaison dans G et dans H , on peut le résoudre dans $G \times H$.

Réciproquement deux éléments $(g, 1)$ et $(g', 1)$ sont conjugués dans $G \times H$ ssi $\exists (g_1, h_1)$ tel que $(g_1, h_1)^{-1} (g, 1) (g_1, h_1) = (g_1^{-1} g g_1, 1)$

$$= (g', 1)$$

donc ssi g et g' , pris comme éléments de G ($G \cong G \times \langle 1 \rangle$), sont conjugués dans G . Ainsi $\mathcal{PC}(G) \leq \mathcal{PC}(G \times H)$, et de façon similaire on montre que $\mathcal{PC}(H) \leq \mathcal{PC}(G \times H)$ ■

Corollaire III.2.1 : Tout produit direct de niveau n ($n \in \mathbb{N}$) a un problème du mot et de conjugaison soluble.

Démonstration : Par récurrence. La proposition III.2.1 nous donne l'étape de récurrence. De plus toujours grâce à la proposition III.2.1 et puisque les problèmes du mot et de la conjugaison sont solubles pour les groupes libres, on a l'étape initiale. ■

Théorème III.2.1 : (Mihailova)

Soit Γ un groupe de présentation finie. Soit $H \leq \Gamma$ un sous-groupe finiment présenté, quotient de Γ , tel que H a un problème du mot de degré $D > 0$. Alors $\exists L_H$ sous-groupe de $\Gamma \times \Gamma$, f.e., tel que $\mathcal{GWP}(L_H; \Gamma \times \Gamma)$ a pour degré D .

Démonstration : Soit $\Gamma = \langle s_1, \dots, s_n \mid r_1, \dots, r_m \rangle$ une présentation de Γ . Alors H , quotient de Γ , peut se donner par la présentation $H = \langle s_1, \dots, s_n \mid r_1, \dots, r_l \rangle$ où $l > m$.

Considérons le sous-groupe L_H de $\Gamma \times \Gamma$ engendré par les éléments :

$$\alpha_i = (s_i; s_i) \quad i \in \langle 1, \dots, n \rangle$$

$$\text{et } \beta_j = (1; r_j) \quad j \in \langle 1, \dots, l \rangle$$

Le résultat découle du lemme suivant :

Lemme III.2.2 : $\forall x, y \in \Gamma ; (x; y) \in L_H \Leftrightarrow x =_H y$

Démonstration : On considère la projection canonique $\pi : \Gamma \twoheadrightarrow H$ et l'épimorphisme $\psi : \Gamma \times \Gamma \twoheadrightarrow H \times H$, défini par $\forall a, b \in \Gamma$, $\psi((a; b)) = (\pi(a); \pi(b))$.

Alors $\psi(r_j) = (1; 1) \quad \forall j \in \langle 1, \dots, l \rangle$, et $\psi(r_i)$ est un élément diagonal de $H \times H$, $\forall i \in \langle 1, \dots, n \rangle$. D'où $\forall x, y \in \Gamma ; (x; y) \in L_H \Rightarrow (x; y)$ est un élément diagonal de $H \times H$, i.e. $x =_H y$.

Supposons maintenant que $x =_H y$. Alors $y x^{-1} =_H 1$ i.e. $y x^{-1}$ est librement égal à $\prod p^{-1} r_{v(i)} p$. Alors $(1; y x^{-1}) \in L_H$.

Or $(x;x) \in L_H$ donc $(x;y) \in L_H$ ■

Définition : Soient G ,un groupe f.p. ,et H un groupe récursivement présenté , et un plongement Π ,de H dans G . Π est appelé plongement récursif ,si le problème du mot généralisé de H dans G est soluble .

Remarque : Alors si $\mathcal{WPC}(H,G)$ a pour degré D ,et si on a un plongement récursif de A dans H ,alors $\mathcal{WPC}(A,G)$ a pour degré D .

Corollaire III.2.2 : Soit F_n ,le groupe libre de rang n ($n \geq 2$) .
 $F_n \times F_n$ a un sous-groupe L tel que $\mathcal{WPC}(L;F_n \times F_n)$ a pour degré D .En particulier ,le problème du mot généralisé de $F_n \times F_n$,est récursivement insolvable .

Démonstration : D'après le corollaire II.3.1.1 ,et le théorème de Mihailova ,la proposition est vraie pour $n = 2$.

Considérons le sous groupe de F_2 engendré par $\alpha , \beta^{-1}\alpha \beta , \dots , \beta^{-(n-1)}\alpha \beta^{n-1}$.D'après le théorème de Nielsen-Schreier ,c'est un groupe libre .De plus il est engendré librement par ces générateurs ,puisque'un produit de puissances de générateurs ,laisse les sous-mots médians des générateurs ,inchangé .On considère le plongement de F_n dans F_2 sur ces générateurs .Il s'étend en un épimorphisme de $F_n \times F_n$ dans $F_2 \times F_2$,qui est un plongement récursif

III.2.3 HNN extensions et extensions de Britton

a) Problème du mot et problème du mot généralisé

On utilisera les notations de I.5

Remarquons que si un groupe G f.p. a un problème du mot généralisé soluble ,alors étant donné un sous-groupe f.e. A de G ,et un mot ω de G appartenant à A ,on peut donner une écriture de $\bar{\omega}$ sur les générateurs de A .En effet ,si $\omega \in A$,on énumère tous les éléments de A ,écrit comme mots sur G ,et pour chacun on décide si il est égal à ω ce qui est possible puisque $\mathcal{WP}(G) \leq \mathcal{WPC}(G)$.

Proposition III.2.5 : Une extension de Britton d'un groupe ayant un problème du mot généralisé soluble a un problème du

mot soluble .

Démonstration : Considérons G^* ,extension de Britton d'un groupe $G = \langle S / R \rangle$ ayant un problème du mot généralisé soluble ; avec pour lettres stables T .Considérons un mot w sur $S \cup T$.On peut alors décider si $w =_H 1$,grâce à la procédure suivante :

1^{er} cas : Si w est un mot sur S ,puisque G est plongé naturellement dans G^* (thm I.5.1), $w =_G 1$ ssi $w =_{G^*} 1$.Or G a un problème du mot généralisé soluble ,et donc un problème du mot soluble .Ainsi dans ce cas on peut décider ,grâce à un algorithme pour G ,si $w = 1$ dans G^* .

2^{ème} cas : w est un mot sur T .Considérons Γ le sous groupe de G^* engendré par T .Et donc $w =_{G^*} 1$ ssi $w = 1$ dans Γ .Or Γ est un groupe libre (lemme I.5.3) ,et donc ,puisque tout groupe libre a un problème du mot soluble ,on peu décider si $w = 1$ dans G^* .

3^{ème} cas : w est un mot sur $S \cup T$,ayant des occurences d'éléments de S et de T .Alors avec le théorème I.5.1 si $w = 1$ dans G^* , w contient un pinch ,i.e. un sous-mot de la forme $p_y^{-1} X p_z$ (ou dualement $p_y X p_z^{-1}$) ,où X est un mot sur S , qui est dans le sous-groupe de G engendré par $\langle A_y \rangle$ (dualement $\langle B_y \rangle$) (avec les notations de I.5) et $z \in K_y$.

Pour décider si $w = 1$ dans G^* ,on peut énumérer tous les sous-mots de w de la forme $p_y^{-1} X p_z$,où X est un mot sur S ,et $z \in K_y$,car K_y est donné par la présentation canonique de G^* .Puisque G a un problème du mot étendu soluble ,on peut décider si $X \in A_y$,et dans ce cas donner son écriture sur les générateurs de A_y .Si c'est le cas ,on peut effectivement utiliser le thm I.5.1 pour extraire le pinch .On obtient alors une écriture de \bar{w} ,contenant moins d'occurence d'éléments de T .On recommence alors la procédure .Si ce n'est pas le cas ,alors $w \neq 1$. ■

Avec le corollaire III.1.1,le corollaire suivant est immédiat .

Corollaire III.2.3 : Une extension de Britton d'un groupe libre ,a un problème du mot soluble .

Proposition III.2.6 : Pour tout groupe libre de rang n ($n \geq 2$) , F_n ,il existe une HNN extension de F_n ,ayant un problème

du mot généralisé ,insoluble .

Démonstration : $F_n \times F_n$ donné par la présentation :

$$\langle \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n / [\alpha_i, \beta_j] ; i, j = 1 \dots n \rangle$$

est clairement une HNN extension de $F(\alpha_1, \dots, \alpha_n)$,ayant pour lettres stables $\langle \beta_1, \dots, \beta_n \rangle$.Or d'après le corollaire III.2.2 , $F_n \times F_n$ a un problème du mot généralisé ,insoluble . ■

Proposition III.2.7 : Si un groupe G a un problème du mot généralisé récursivement insoluble ,alors il existe une HNN extension de G ,ayant un problème du mot récursivement insoluble .

Démonstration : Considérons un sous-groupe H de G ,f.e. par $\langle \alpha_1, \dots, \alpha_n \rangle$, tel que $\mathcal{GWP}(H, G)$ soit récursivement insoluble .On construit alors G^* ,HNN extension de G ,ayant pour lettre stable $\langle t \rangle$,et pour relateurs de l'extension $t^{-1}\alpha_i t = \alpha_i$,pour tout $i = 1 \dots n$. Alors ,pour un mot w de G ,d'après le lemme de Britton $t^{-1}wt = w$ dans G^* ssi $w \in H$.Et ainsi $\mathcal{GWP}(H, G) \leq \mathcal{WP}(G^*)$. ■

Corollaire III.2.4 : Pour tout $n \geq 2$,il existe une HNN extension de niveau n ayant un problème du mot récursivement insoluble .

Démonstration : Par récurrence .Les propositions III.2.6 et III.2.7 nous donnent l'existence d'une HNN extension de niveau 2 ayant un problème du mot récursivement insoluble ce qui fournit l'étape initiale .

Supposons que E_n^* ,soit une HNN extension de niveau n ayant un problème du mot récursivement insoluble .Construisons E_{n+1}^* ,HNN extension ayant pour base E_n^* ,et donc de niveau $n + 1$.Alors puisque $E_n^* \hookrightarrow E_{n+1}^*$,et que le problème du mot est héréditaire (I.3.3) , E_{n+1}^* a un problème du mot récursivement insoluble .

C. Q. F. D. ■

b) Problème de la conjugaison

Soient $H = \langle s_1, \dots, s_n / r_1, \dots, r_n \rangle$,un groupe finiment présenté

, ayant un problème du mot insoluble ; et $F = \langle k, s_1, \dots, s_n \rangle$, le groupe libre de rang $n + 1$, sur les générateurs k, s_1, \dots, s_n .

Définissons le groupe f.p. ,G par la donnée d'une présentation :

Générateurs : $k, s_1, \dots, s_n, t_1, \dots, t_m, d_1, \dots, d_n$

Relations : (i) $t_i^{-1} k t_i = k R_i$
(ii) $t_i^{-1} s_a t_i = s_a$
(iii) $d_b^{-1} s_a d_b = s_a$
(iv) $d_a^{-1} k d_a = s_a^{-1} k s_a$

où $1 \leq i \leq m$; $1 \leq a \leq n$; $1 \leq b \leq n$

et où les R_i sont les mots sur s_1, \dots, s_n apparaissant dans la présentation de H donnée précédemment .

Lemme III.2.3 : G est une HNN extension de F ayant pour lettres stables $\langle t_1, \dots, t_m, d_1, \dots, d_n \rangle$.

Démonstration : G a pour base F et pour lettres stables $\langle t_1, \dots, t_m, d_1, \dots, d_n \rangle$. Les sous groupes de Britton sont tous F . On vérifie donc la condition de l'isomorphisme , et on a donc le résultat. ■

En utilisant le lemme III.2.3 et le corollaire III.2.3 , on a donc :

Lemme III.2.4 : G a un problème du mot récursivement soluble .

NOTATIONS : Soient X un mot sur s_1, \dots, s_n . On note $X(d_\alpha)$ le mot obtenu en remplaçant dans X toutes les occurrences de s_α par d_α ($\alpha = 1 \dots n$) . On note T le sous-groupe de G engendré par t_1, \dots, t_m et d_1, \dots, d_n . Remarquons que les mots sur s_1, \dots, s_n commutent dans G avec les éléments de T , ce grâce aux relateurs (ii) et (iii) de la présentation de G .

Quelques remarques et calculs préliminaires seront utiles à la suite . Toutes les égalités considérées ont lieu dans G . Soit Z un mot sur s_1, \dots, s_n ; $Z \equiv s_{j_1}^{\zeta_1} \dots s_{j_p}^{\zeta_p}$; où $\zeta_1, \dots, \zeta_p \in \{-1; 1\}$, et $j_1, \dots, j_p \in \{1, \dots, n\}$.

$$\begin{aligned} Z^{-1} k Z &\equiv s_{j_p}^{-\zeta_p} \dots s_{j_1}^{-\zeta_1} k s_{j_1}^{\zeta_1} \dots s_{j_p}^{\zeta_p} \\ &= s_{j_p}^{-\zeta_p} \dots d_{j_1}^{-\zeta_1} k d_{j_1}^{\zeta_1} \dots s_{j_p}^{\zeta_p} \end{aligned} \quad (\text{avec (iv)})$$

$$\begin{aligned}
&= d_{j_1}^{-\zeta_1} s_{j_P}^{-\zeta_P} \dots s_{j_2}^{-\zeta_2} k s_{j_2}^{\zeta_2} \dots s_{j_P}^{\zeta_P} d_{j_1}^{\zeta_1} \quad (\text{avec (iii)}) \\
\dots &= d_{j_1}^{-\zeta_1} \dots d_{j_P}^{-\zeta_P} k d_{j_P}^{\zeta_P} \dots d_{j_1}^{\zeta_1} \quad (\text{après réitération}) \\
&= Z(d_{\alpha}^{-1}) k Z(d_{\alpha}^{-1})^{-1}
\end{aligned}$$

De même $Z k Z^{-1} = Z(d_{\alpha}^{-1})^{-1} k Z(d_{\alpha}^{-1})$

Et puisque les mots sur s_1, \dots, s_n commutent avec les éléments de T .

$$\begin{aligned}
Z(d_{\alpha}^{-1}) Z k Z(d_{\alpha}^{-1})^{-1} &= Z Z(d_{\alpha}^{-1}) k Z(d_{\alpha}^{-1})^{-1} \\
&= Z Z^{-1} k Z \\
&= k Z
\end{aligned}$$

De plus on a $t_i^{-1} k t_i = k R_i$ (relateur (i))

soit $t_i^{-1} k t_i R_i^{-1} k^{-1} = 1$

$t_i^{-1} k R_i^{-1} t_i k^{-1} = 1$

$k R_i^{-1} t_i k^{-1} t_i^{-1} = 1$ après conjugaison cyclique

soit $t_i k^{-1} t_i^{-1} = R_i k^{-1}$

et donc $t_i k t_i^{-1} = k R_i^{-1}$

Avec $W \equiv Z(d_{\alpha}^{-1}) t_i^{\varepsilon} Z(d_{\alpha}^{-1})^{-1}$ où $\varepsilon = \pm 1$

$$\begin{aligned}
W^{-1} k W &\equiv Z(d_{\alpha}^{-1}) t_i^{-\varepsilon} Z(d_{\alpha}^{-1})^{-1} k Z(d_{\alpha}^{-1}) t_i^{\varepsilon} Z(d_{\alpha}^{-1})^{-1} \\
&= Z(d_{\alpha}^{-1}) t_i^{-\varepsilon} Z k Z^{-1} t_i^{\varepsilon} Z(d_{\alpha}^{-1})^{-1} \\
&= Z(d_{\alpha}^{-1}) Z t_i^{-\varepsilon} k t_i^{\varepsilon} Z^{-1} Z(d_{\alpha}^{-1})^{-1} \\
&= Z(d_{\alpha}^{-1}) Z k R_i^{\varepsilon} Z^{-1} Z(d_{\alpha}^{-1})^{-1} \\
&= Z(d_{\alpha}^{-1}) Z k Z(d_{\alpha}^{-1})^{-1} R_i^{\varepsilon} Z^{-1} \\
&= k Z R_i^{\varepsilon} Z^{-1}
\end{aligned}$$

Lemme III.2.5 : Soient X_1, X_2, Y_1, Y_2 des mots sur s_1, \dots, s_n .

(i) $(\exists W \in T) (W^{-1} X_1 k Y_1 W =_{\sigma} X_2 k Y_2) \Leftrightarrow (X_1 Y_1 =_H X_2 Y_2)$

(ii) $(X_1 k Y_1 \sim_{\sigma} X_2 k Y_2) \Leftrightarrow (X_1 Y_1 \sim_H X_2 Y_2)$

Démonstration : (i) Condition nécessaire

Soit $\psi : \langle k, s_1, \dots, s_n, t_1, \dots, t_m, d_1, \dots, d_n \rangle \longrightarrow H$; défini par
 $\psi(k) = 1$; $\psi(t_i) = 1$; $\psi(d_{\alpha}) = 1$; $\psi(s_{\alpha}) = s_{\alpha}$
 avec $i = 1 \dots m$ et $\alpha = 1 \dots n$. ψ s'étend naturellement sur le
 groupe libre engendré par $k, s_1, \dots, s_n, t_1, \dots, t_m, d_1, \dots, d_n$ en un

homomorphisme surjectif. Les relateurs de G (pris comme éléments du groupe libre) sont dans le noyau de Ψ . On peut donc passer au quotient, et l'on a $\Psi / \ker(\Psi) : G \rightarrow H$ homomorphisme surjectif. L'image de $W^{-1} X_1 k Y_1 W$ par cet homomorphisme est $X_1 Y_1$, l'image de $X_2 k Y_2$ est $X_2 Y_2$, on a donc $X_1 Y_1 =_H X_2 Y_2$. \square

(i) Condition suffisante

$X_1 Y_1 =_H X_2 Y_2$, alors $X_2 Y_2 = \left(\prod_{i=1}^k Z_i R_{p(i)}^{\varepsilon(i)} Z_i^{-1} \right) X_1 Y_1$ dans le groupe libre, où $p : \langle 1, \dots, k \rangle \rightarrow \langle 1, \dots, m \rangle$ et $\varepsilon : \langle 1, \dots, k \rangle \rightarrow \langle -1, 1 \rangle$. On note $\theta_i \equiv Z_i (d_\alpha^{-1}) t_{p(i)}^{\varepsilon(i)} Z_i (d_\alpha^{-1})^{-1}$ et $W^* \equiv \theta_k \dots \theta_1$. On a alors :

$$\begin{aligned} W^{*-1} k X_1 Y_1 W^* &\equiv \theta_1^{-1} \dots \theta_k^{-1} k X_1 Y_1 \theta_k \dots \theta_1 \\ &=_{\mathcal{G}} \theta_1^{-1} \dots \theta_k^{-1} k \theta_k \dots \theta_1 X_1 Y_1 \\ &=_{\mathcal{G}} \theta_1^{-1} \dots k Z_k R_{p(k)}^{\varepsilon(k)} Z_k^{-1} \dots \theta_1 X_1 Y_1 \\ &=_{\mathcal{G}} \theta_1^{-1} \dots \theta_{k-1}^{-1} k \theta_{k-1} \dots \theta_1 Z_k R_{p(k)}^{\varepsilon(k)} Z_k^{-1} X_1 Y_1 \\ &\vdots \\ &=_{\mathcal{G}} k X_2 Y_2 \end{aligned}$$

En posant $W \equiv X_1 (d_\alpha^{-1})^{-1} W^* X_2 (d_\alpha^{-1})$

$$\begin{aligned} W^{-1} X_1 k Y_1 W &\equiv X_2 (d_\alpha^{-1})^{-1} W^{*-1} X_1 (d_\alpha^{-1}) X_1 k Y_1 X_1 (d_\alpha^{-1})^{-1} W^* X_2 (d_\alpha^{-1}) \\ &=_{\mathcal{G}} X_2 (d_\alpha^{-1})^{-1} W^{*-1} X_1 X_1 (d_\alpha^{-1}) k X_1 (d_\alpha^{-1})^{-1} Y_1 W^* X_2 (d_\alpha^{-1}) \\ &=_{\mathcal{G}} X_2 (d_\alpha^{-1})^{-1} W^{*-1} X_1 X_1^{-1} k X_1 Y_1 W^* X_2 (d_\alpha^{-1}) \\ &=_{\mathcal{G}} X_2 (d_\alpha^{-1})^{-1} W^{*-1} k X_1 Y_1 W^* X_2 (d_\alpha^{-1}) \\ &=_{\mathcal{G}} X_2 (d_\alpha^{-1})^{-1} k X_2 Y_2 X_2 (d_\alpha^{-1}) \\ &=_{\mathcal{G}} X_2 (d_\alpha^{-1})^{-1} k X_2 (d_\alpha^{-1}) X_2 Y_2 \\ &=_{\mathcal{G}} X_2 k X_2^{-1} X_2 Y_2 \\ &=_{\mathcal{G}} X_2 k Y_2 \end{aligned}$$

Et on a donc trouvé $W \in T$ comme désiré. \square

(ii) Condition suffisante

$X_1 Y_1 \sim_H X_2 Y_2$ i.e. $\exists X$ mot sur s_1, \dots, s_n avec $X^{-1} X_1 Y_1 X =_H X_2 Y_2$.
D'après (i) $\exists W \in T$ tel que $W^{-1} X^{-1} X_1 k Y_1 X W =_{\mathcal{G}} X_2 k Y_2$

$$(X W)^{-1} X_1 k Y_1 X W =_{\mathcal{G}} X_2 k Y_2$$

soit

$$X_1 k Y_1 \sim_{\mathcal{G}} X_2 k Y_2 \quad \square$$

(ii) Condition nécessaire

$X_1 k Y_1 \sim_G X_2 k Y_2$ i.e. $\exists \theta \in G$ tel que $\theta^{-1} X_1 k Y_1 \theta =_G X_2 k Y_2$
 On note $\phi = \Psi / \ker \Psi$. Alors $\phi(\theta^{-1} X_1 k Y_1 \theta) =_H \phi(X_2 k Y_2)$
 $\phi(\theta^{-1}) X_1 Y_1 \phi(\theta) =_H X_2 Y_2$
 et donc $X_1 Y_1 \sim_H X_2 Y_2$ ■

Puisque tout élément X de H peut s'écrire $X_1 Y_1$, le lemme III.2.5 (ii) a pour conséquence $CP(H) \leq CP(G)$. Or H a un problème du mot récursivement insoluble, et donc un problème de conjugaison récursivement insoluble. On a donc le résultat suivant

Lemme III.2.6 : G a un problème de conjugaison récursivement insoluble.

Les résultats suivants sont alors immédiats.

Proposition III.2.8: Il existe une HNN extension d'un groupe libre ayant un problème de conjugaison récursivement insoluble.

Et avec le corollaire III.2.3 :

Corollaire III.2.5 : Il existe un groupe ayant un problème du mot soluble et un problème de la conjugaison récursivement insoluble.

III.2.4 Produit libre amalgamé

On se donne deux groupes f.p. $G_1 = \langle S_1 / R_1 \rangle$ et $G_2 = \langle S_2 / R_2 \rangle$, deux sous-groupes isomorphes f.e. $H_1 \subseteq G_1$ et $H_2 \subseteq G_2$, ainsi que $\Psi : H_1 \longrightarrow H_2$ par l'image des générateurs de H_1 . On considère alors le produit libre amalgamé de G_1 et G_2 , sur H_1 et H_2 , par Ψ ; donné par la présentation canonique :

$G = \langle S_1 \cup S_2 / R_1 \cup R_2, \Psi(a_i) = a_i, i \in I \rangle$, où $\{a_i, i \in I\}$ est une famille génératrice finie de H_1 .

Pour tout élément $g \in G$ il existe une unique séquence g_1, \dots, g_n, h , appelée forme normale telle que : si $g_i \in G_1 \setminus H_1$ alors $g_{i+1} \in G_2 \setminus H_2$ (et inversement), $\forall i = 1 \dots n$, $g_i \neq 1$, et $g_1 \in G_1$ ou G_2 , $h \in H_1 = H_2$, et $g = g_1 \dots g_n h$.

Proposition III.2.9 : Si G est le produit libre de G_1 et G_2 , amalgamé sur des sous-groupes f.e., $H_1 \subseteq G_1$ et $H_2 \subseteq G_2$, tels que $\mathcal{GWP}(H_1, G_1)$ et $\mathcal{GWP}(H_2, G_2)$ sont solubles et que G_1 et G_2 ont un problème du mot soluble, alors, le problème du mot de G est soluble.

Démonstration : Considérons la présentation de G citée ci-dessus. On peut alors déterminer l'image par ψ^{-1} des générateurs de H_2 , simplement en énumérant les images des mots de H_1 (par longueur croissante, par exemple), et en décidant si elles sont égales dans H_2 , à un générateur.

Prenons un mot ω de G s'écrivant $C_1 D_1 \dots C_n D_n$, où les C_i sont des mots sur S_1 , les D_i sont des mots sur S_2 ($i = 1 \dots n$), tous non vides (Tout autre cas est analogue). D'après le théorème d'unicité de l'écriture normale, ω s'écrit de façon unique sous la forme $\alpha_1 \beta_1 \dots \alpha_N \beta_N h$; où $\forall i = 1 \dots N$, α_i est un mot sur S_1 , β_i un mot sur S_2 , $\alpha_i \in G_1 \setminus H_1$, $\beta_i \in G_2 \setminus H_2$, $\alpha_1 \beta_1, \alpha_2 \beta_2, \dots, \alpha_N \beta_N$ sont non triviaux, et $h \in H_1 = H_2$. Sous les hypothèses de la proposition, on peut effectivement déterminer une telle écriture pour ω . Prenons $\omega \equiv C_1 D_1 \dots C_n D_n$ comme précédemment. On peut tester pour tout mot C_i (resp^t D_i), si $C_i \in H_1$ (resp^t H_2). Si c'est le cas on peut écrire C_i sur les générateurs de H_1 , et alors transformer l'écriture de ω en $C_1 D_1 \dots D'_{i-1} C'_i \dots D'_{n-1}$, où $D'_{i-1} \equiv D_{i-1} \Psi(C_i)$, et $C'_i = C_{i+1}$ etc ... (et dualement avec H_2 à la place de H_1 , Ψ^{-1} à la place de Ψ). Et on réitère le même procédé, jusqu'à ce que cela ne soit plus possible. On a alors une écriture sous forme normale de ω . Si ω s'écrit $h \in H_1$ (ou H_2), on peut décider si $\omega = 1$. Sinon d'après l'unicité de l'écriture sous forme normale, $\omega \neq 1$.

Remarque : Il apparaît dans cette démonstration que sous ces hypothèses on a une procédure pour écrire tout mot sous sa forme normale.

Proposition III.3.10 : Il existe un produit libre de groupes libres, amalgamé sur des sous-groupes finiment engendrés, ayant un problème de la conjugaison, (resp^t

du mot généralisé) ,récurivement insoluble .

Démonstration : Reprenons les notations du théorème I.5.1 .Dans la démonstration de ce théorème apparaît le groupe \bar{E} ,qui est produit libre amalgamé sur des sous-groupes finiment engendrés ,de $F = \langle a_v, v \in V \rangle * E$,et $G = \langle b_v, v \in V \rangle * E$.Il est clair que si E est libre , F et G sont libres.De plus avec les changements de Tietze :

$$\begin{aligned}\bar{E} &= \langle S, a_v, b_v, v \in V / D, a_{y(i)}^{-1} A_i a_{z(i)} = b_{y(i)} B_i b_{z(i)}^{-1}, i \in I \rangle \\ &\cong \langle S, a_v, b_v, p_v, v \in V / D, p_v = a_v b_v, p_{y(i)}^{-1} A_i p_{z(i)} = B_i, i \in I \rangle \\ &\cong \langle S, a_v, p_v, v \in V / D, p_{y(i)}^{-1} A_i p_{z(i)} = B_i, i \in I \rangle \\ &\cong E^* * \langle a_v, v \in V \rangle\end{aligned}$$

Et donc $\mathcal{WP}(E^*) \leq \mathcal{WP}(\bar{E})$ (prop III.2.3) ,et $\mathcal{GWP}(E^*) \leq \mathcal{GWP}(\bar{E})$ (car le plongement est récursif).Or cet argument est vrai pour toute extension de Britton .Donc puisqu'il existe une HNN extension de niveau 1 ,ayant un problème du conjugaison (resp^t du mot généralisé) récurivement insoluble ,il existe un produit libre finiment amalgamé ,de niveau 1 ,ayant un problème de conjugaison (resp^t du mot généralisé) récurivement insoluble . ■

Lemme III.2.7 : Si G a un problème du mot généralisé récurivement insoluble ,alors il existe un produit libre amalgamé de deux copies de G ,sur des sous-groupe finiment engendrés,ayant un problème du mot récurivement insoluble

Démonstration : Soit un sous-groupe H f.e. de G tel que $\mathcal{GWP}(H,G)$ soit récurivement insoluble .Prenons H' et G' copies de H et G ,et formons $K = G \underset{H=H'}{*} G'$.Alors avec le théorème d'écriture normale ,pour un mot $h \in H$,et pour tout mot w de G , $w h w' h' = 1$ dans K ssi $w \in H$ (avec w' et h' copies de w et h) .Ainsi on a $\mathcal{GWP}(H,G) \leq \mathcal{WP}(K)$. ■

Proposition III.2.11 : Pour tout $n \geq 2$,il existe un produit libre amalgamé de niveau n ,ayant un problème du mot insoluble .

Démonstration : Par récurrence .La proposition III.2.10 ,et le

lemme III.3.7 nous donnent l'étape initiale .L'étape de récurrence elle ,provient du fait que si K est un produit libre amalgamé de G $G \hookrightarrow K$,et que le problème du mot est héréditaire . ■

III.2.5 Split extension

Proposition III.2.12 : Toute split extension de niveau n ($n \in \mathbb{N}^*$) ,a un problème du mot soluble .

Démonstration : Résultat trivial ,avec le fait que le problème du mot est une poly-propriété . ■

Proposition III.2.13 : Pour tout n ,il existe une split extension de niveau n ayant un problème du mot généralisé récursivement insoluble .

Démonstration : Trivial puisqu'un produit direct de niveau n est une split extension de niveau n . ■

Proposition III.2.14 : Pour tout n ,il existe une split extension de niveau n ,ayant un problème de la conjugaison récursivement insoluble .

Démonstration : On le démontre pour $n = 1$.Alors étant donnée une telle split-extension A , $A \times \mathbb{Z}^{n-1}$,est une split extension de niveau n ,ayant un problème de la conjugaison insoluble .

Considérons le groupe G de III.2.3.b) .Nous allons démontrer qu'il s'agit d'une split extension d'un groupe libre par un autre .Le résultat sera alors établi .

Considérons les sous-groupes de G , $F = \langle k, s_1, \dots, s_n \rangle_G$,et $T = \langle t_1, \dots, t_m, d_1, \dots, d_n \rangle_G$.Au vu des relateurs de G ,il est clair que pour tout $g \in G$, $g = g_1 g_2$ où $g_1 \in F$ et $g_2 \in T$.Ainsi $G = F T$.De plus ,il est clair que F est distingué dans G ,et F est libre. G est une HNN extension de F ayant pour lettres stables les générateurs de T ,et donc (lemme I.5.3) , T est libre .Il nous suffit donc de démontrer que $F \cap T = \langle 1 \rangle$.

Soit $g_1 \in F$, $g_2 \in T$,tels que $g_1 =_G g_2$.Alors $g_1 g_2^{-1} = 1$,et donc d'après le théo. I.5.1 ,il contient un pinch .Or toutes les

occurrences de lettres stables sont dans g_2^{-1} , et donc il est clair que $g_2^{-1} = 1$, et donc $g_1 = g_2 = 1$. ■

Constr- uction niveau	HNN extension et extension de Britton	Produit libre amalgamé	Produit direct	Split extension
niveau 3 (et plus)	⋮	⋮	⋮	⋮
niveau 2	-WP	-WP	⋮	⋮
niveau 1	+WP -CP -GWP	+WP -CP -GWP	+WP +CP -GWP	+WP -CP -GWP

(tableau 1)

où +WP signifie que le problème du mot est soluble, -WP signifie qu'il existe un groupe ayant un problème du mot insoluble (De même avec CP et GWP).

III.3 PROBLEMES DE SOLUBILITE DANS DES CLASSES ALGEBRIQUES

Le but de ce paragraphe est d'établir des résultats d'insolubilité (et accessoirement de solubilité), dans des classes de groupes définis par des propriétés simples. Nous avons déjà vu que dans les groupes libres tous les problèmes sont solubles. Il en est de même dans des classes algébriques très simples telles que les groupes finis, les groupes abéliens, les groupes nilpotents. Ainsi Considérons un groupe G fini. Il existe une liste exhaustive, finie g_1, \dots, g_n de ses éléments (deux à deux distincts), et une table finie de multiplication, i.e. toutes les relations de la forme $g_i g_j = g_{i,j}$, pour tout $i, j \in \langle 1, \dots, n \rangle$, avec $g_{i,j} \in \langle g_1, \dots, g_n \rangle$.

Il est aisé de vérifier que la présentation :

$$\langle g_1, \dots, g_n \mid g_i g_j = g_{i,j}; i, j \in \langle 1, \dots, n \rangle \rangle$$

est une présentation canonique de G . Alors le problème de l'isomorphisme pour les groupes finis est résoluble, en employant les changements de Tietze. De plus tout mot sur cette présentation $g_{i(1)} \dots g_{i(k)}$ peut canoniquement et effectivement s'écrire sous la forme $g \in \langle g_1, \dots, g_n \rangle$. Tous les problèmes de Dehn sont alors résolubles.

Le théorème de Kronecker établit que tout groupe abélien f.e. est isomorphe à un unique groupe de la forme $\mathbb{Z}^q \times \mathbb{Z}_{k(1)} \times \dots \times \mathbb{Z}_{k(n)}$

où $q, k(1), \dots, k(n) \in \mathbb{N}$, et $k(i)$ divise $k(i+1)$ pour tout $i = 1, \dots, n-1$. Tout groupe abélien f.e. admet donc la présentation finie canonique :

$$\langle a_1, \dots, a_{q+n} \mid a_{q+i}^{k(i)} = 1, i = 1, \dots, n; [a_j, a_l], j, l = 1, \dots, q+n \rangle$$

Le problème de l'isomorphisme est donc soluble pour les groupes abéliens. De plus avec la proposition III.2.4, tout groupe abélien s'exprimant comme produit direct de groupes cycliques, le problème du mot, et le problème de la conjugaison sont solubles. Le problème du mot généralisé est aussi soluble.

III.3.1 Groupes résiduellement finis, nilpotents, libres.

Tout groupe f.p. résiduellement nilpotent est résiduellement fini, tout groupe f.p. résiduellement libre est résiduellement nilpotent, et donc résiduellement fini, tout groupe f.g. nilpotent est f.p. et résiduellement nilpotent et donc résiduellement fini. On peut résoudre le problème du mot dans un groupe f.p., G résiduellement fini, par la procédure suivante :

Considérons un groupe G , f.p. résiduellement fini, et un mot w sur la présentation finie de G . On effectue alors deux énumérations simultanées. On énumère tous les éléments triviaux de G , ainsi que l'image de w par tout morphisme de G dans un groupe fini. La procédure effectuant la première énumération consiste, à énumérer les mots s'écrivant comme produits de conjugués de relateurs (par exemple par longueur croissante), puis de les réduire librement. Pour la deuxième énumération, on commence par énumérer toutes les présentations canoniques de groupes finis (les relateurs fournissant explicitement une table de multiplication). De façon simultanée, on peut pour un groupe fini A , déterminer tous les homomorphismes de G dans A . Il suffit de considérer toutes les applications de l'ensemble des générateurs de G , dans A . Ces applications s'étendent en un unique homomorphisme du groupe libre sous-jacent à G , dans A . Ces homomorphismes passent au quotient G , si l'image des relateurs de G , est triviale, ce que l'on peut déterminer, en utilisant l'algorithme pour le problème du mot dans A . On peut alors pour tout homomorphisme de G dans A

,calculer l'image de ω ,et décider si elle est triviale dans A .
 Si $\omega =_G 1$,alors ω sera énuméré par la première énumération .
 Si $\omega \neq_G 1$.Puisque G est résiduellement fini ,il existe un sous-groupe normal N ne contenant pas ω tel que G/N est fini ,et donc il existe un homomorphisme de G dans un groupe fini ,dont l'image de ω est non triviale .

Ainsi en effectuant cette procédure pour un élément ω ,on peut décider si $\omega =_G 1$,en attendant que ω soit énuméré par la première procédure ,ou que l'on ait énuméré un homomorphisme de G dans un groupe fini ,dont l'image de ω est non triviale .

Proposition III.3.2 : Il existe un groupe résiduellement fini f.p. ayant un problème de la conjugaison récursivement insoluble .

Démonstration : Pour démontrer ce résultat considérons le groupe G de III.2.3.b) .D'après la proposition III.2.14 , G est une split extension de deux groupes libres f.p. .Puisque un groupe libre f.e. ,est résiduellement fini ,le résultat est immédiat avec le résultat suivant . ■

Lemme III.3.1 : (Lemme d'extension)

Si $1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1$,est une suite exacte de groupes ,si K et Q sont résiduellement finis ,et si K est f.g. ,alors si l'on a une des conditions suivantes :

- (1) K a un centre trivial .
 - (2) G est une split extension de K par Q
- alors G est résiduellement fini .

Pour une démonstration de ce résultat voir [26]

Proposition III.3.3 : Il existe un groupe résiduellement libre ayant un problème du mot généralisé récursivement insoluble .

Remarque: Et donc le problème de la conjugaison est aussi récursivement insoluble dans la classe des groupes résiduellement nilpotents (resp^t résiduellement finis) .

Démonstration : Considérons $F_2 \times F_2$, produit direct de deux groupes libres de rang 2. Considérons un élément non trivial $g = (g_1, g_2) \in F_2 \times F_2$. Alors soit g_1 soit g_2 est non trivial (prenons par exemple g_1), alors $\langle 1 \rangle \times F_2$ est un sous-groupe normal de $F_2 \times F_2$ ne contenant pas g , et $F_2 \times F_2 / \langle 1 \rangle \times F_2 \cong F_2$ est libre. Avec le corollaire III.2.2, on a le résultat. ■

III.3.2 : résultats d'insolvabilité dans des sous-groupes de groupes élémentaires.

Proposition III.3.4 : Soit F un groupe libre de rang au moins 2. Il existe un sous-groupe f.e. L , de $F \times F$ tel que L a un problème de la conjugaison récursivement insoluble.

Démonstration : Puisque $F_n \times F_n$, où F_n est un groupe libre de rang au moins 2, se plonge dans $F_3 \times F_3$, il suffit de démontrer la proposition pour $n = 3$.

Considérons $H = \langle s_1, s_2 \mid r_1, \dots, r_m \rangle$, un groupe f.p. avec 2 générateurs, ayant un problème du mot insoluble. $\langle H, s_3 \mid s_3 \rangle$ est une présentation de H . Considérons $F_3 = \langle s_1, s_2, s_3 \mid \rangle$. H est un quotient de F_3 , et on forme alors le sous-groupe de $F_3 \times F_3$, L , de la même façon que dans la démonstration du théorème III.2.1, et alors, avec le théorème III.2.1, L est f.e., et $\mathcal{CWP}(L, F_3 \times F_3)$ est récursivement insoluble.

Soit ω un mot de F_3 . Alors d'après le lemme III.2.2, $(s_3, \omega^{-1}s_3\omega)$ est un élément de L puisque $s_3 =_H 1 =_H \omega^{-1}s_3\omega$. On a besoin du lemme suivant :

Lemme III.3.2 : (s_3, s_3) est conjugué à $(s_3, \omega^{-1}s_3\omega)$ dans L , ssi $\omega =_H 1$.

Démonstration : Supposons que $\omega =_H 1$. Alors d'après le lemme III.2.2, $(1, \omega) \in L$. Et donc (s_3, s_3) et $(s_3, \omega^{-1}s_3\omega)$ sont conjugués dans L .

Réciproquement, supposons qu'il existe $(X, Y) \in L$, tel que $(X^{-1}s_3X, Y^{-1}\omega^{-1}s_3\omega Y) = (s_3, s_3)$ dans L , et donc dans $F_3 \times F_3$. Et alors, $X^{-1}s_3 = s_3X^{-1}$ et $Y^{-1}\omega^{-1}s_3 = s_3Y^{-1}\omega^{-1}$. Or dans un groupe libre, les seuls éléments commutant avec s_3 , sont les mots sur s_3 . Ainsi $X = s_3^p$, et $\omega Y = s_3^k$ dans F_3 . Et puisque $s_3 =_H 1$, $X =_H 1$, et

$\omega Y =_H 1$. Or d'après le lemme III.2.2, $X =_H Y$, et donc $\omega =_H 1$ \square

Nous pouvons alors reprendre la démonstration. Avec le lemme III.3.2, $WPCH \leq \mathcal{PCL}$, et donc puisque H a un problème du mot insoluble, il en est de même de L . ■

Remarque : Avec le théorème de Higman, le sous-groupe L , est récursivement présenté. De plus $F \times F$ a un problème de la conjugaison soluble. Donc le problème de la conjugaison n'est pas une propriété héréditaire dans la classe des présentations récursive de groupe.

Lemme III.3.3 : Soit F un groupe libre de rang $m \geq 2$. Alors $F \times F$ est récursivement plongé dans $SL(n, \mathbb{Z})$, ainsi que dans $GL(n, \mathbb{Z})$ pour tout $n \geq 4$.

Démonstration : On montre d'abord que le groupe libre de rang 2, F_2 , est plongé récursivement dans $SL(2, \mathbb{Z})$. Considérons le sous-groupe T de $SL(2, \mathbb{Z})$ engendré par les matrices :

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Sanov a montré [36] que T est librement engendré par ces matrices, et que de plus, pour une 2×2 matrice arbitraire (à coefficients dans \mathbb{Z}) :

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$M \in T$ ssi les conditions suivantes sont satisfaites :

- (1) $ad - bc = 1$
- (2) a et d sont congruent à 1, modulo 4
- (3) b et c sont pairs

Puisque T est libre de rang 2, F_2 se plonge dans $SL(2, \mathbb{Z})$ sur T . Et puisque les conditions précédentes sont effectivement calculables, pour une matrice M arbitraire, F_2 se plonge récursivement dans $SL(2, \mathbb{Z})$.

Or $T \times T$ se plonge récursivement dans $SL(4, \mathbb{Z})$ par l'application :

$$(U, V) \longrightarrow \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix}$$

et $SL(4, \mathbb{Z})$ se plonge récursivement dans $SL(n, \mathbb{Z})$ ($n \geq 4$) par

l'application :

$$x \longrightarrow \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

Et donc $F_2 \times F_2$ se plonge récursivement dans $SL(n, \mathbb{Z})$. De plus si F est le groupe libre de rang $m \geq 2$, $F \times F$ se plonge récursivement dans $F_2 \times F_2$, et donc dans $SL(n, \mathbb{Z})$. De plus $SL(n, \mathbb{Z})$ est le sous-groupe de $GL(n, \mathbb{Z})$, des matrices ayant pour déterminant 1. Puisque le déterminant d'une matrice est calculable, $SL(n, \mathbb{Z})$ se plonge récursivement dans $GL(n, \mathbb{Z})$ et donc il en est de même de $F \times F$ ($n \geq 4$). ■

Avec le corollaire III.2.2, la proposition III.3.4, et le lemme III.3.3, la proposition suivante est immédiate.

Proposition III.3.6 : Pour $n \geq 4$, $SL(n, \mathbb{Z})$ (resp^t $GL(n, \mathbb{Z})$) a un sous-groupe L finiment engendré tel que (i) L a un problème de la conjugaison récursivement insoluble. (ii) Le problème du mot généralisé de L dans $SL(n, \mathbb{Z})$ (resp^t $GL(n, \mathbb{Z})$) est récursivement insoluble.

CHAPITRE IV :

ETUDE GEOMETRIQUE DES PROBLEMES DE DEHN

Dans ce chapitre nous résolvons le problème du mot pour de larges classes de groupes par une méthode géométrique .La méthode géométrique en théorie des groupes a été initiée par Dehn ,qui résoud le problème du mot pour les groupes de surfaces compactes orientables ,fermées de genre $g \geq 2$,en considérant le revêtement universel de la surface ,qu'il obtient par un pavage du plan hyperbolique par des $4g$ -gônes .Par des considérations purement géométriques il établit un algorithme pour le problème du mot connu aujourd'hui sous le nom d'algorithme de Dehn .Greendlinger ,généralise sa méthode combinatoirement ,pour des groupes à petite simplification . C'est Van Kampen et surtout Lyndon ,qui établissent la version géométrique de la théorie des petites simplifications .

Nous nous intéresserons ,aux méthodes de résolution du problème du mot ,en géométrie des groupes : algorithme de Dehn ,et inégalités isopérimétriques .Dans un premier temps nous établirons de tel algorithmes ,pour des groupes à petite simplification .Nous caractériserons ensuite les groupes admettant un algorithme de Dehn :ce sont les groupes hyperboliques

L'intérêt de cette méthode est multiple ,premièrement les démonstrations sont courtes et élégantes .Deuxièmement Il y a "beaucoup" de groupes hyperboliques ,et de groupe à petites simplifications

IV.1 INEGALITE ISOPERIMETRIQUE ET ALGORITHMES DE DEHN

IV.1.1 Diagramme de Lyndon-Van Kampen

Considérons un ensemble de mots R . R est dit symétrique si tous les éléments de R sont cycliquement réduits, et si lorsqu'un élément est dans R , tous ses conjugués cycliques sont dans R .

Etant donné un ensemble fini de mots R , on peut déterminer son symétrisé R_* , c'est à dire le plus petit ensemble contenant toutes les réductions cycliques des éléments de R , et stable par conjugaison cyclique. Si $\langle S / R \rangle$ est une présentation d'un groupe G , il est clair qu'il en est de même de $\langle S / R_* \rangle$.

Notation : Dans toute cette partie, étant données une présentation $\langle S / R \rangle$, on note N la clôture normale de R .

Définition : Soit $\langle S / R \rangle$ une présentation de groupe, un élément réduit $\omega_0 \in N$. On appelle diagramme de Lyndon-Van Kampen, de ω_0 sur $\langle S / R \rangle$, (M, f, P) , où M est un 2-complexe fini pointé en u_0 , P est un lacet fermé bordant M , débutant et terminant en u_0 , f est une fonction de label, tel que :

(1) L'espace topologique sous-jacent à M , est homéomorphe à un fermé simplement connexe du plan.

(2) f associe à chaque arête orientée x de M , un élément de $S \cup S^{-1}$, et $f(x^{-1}) = f(x)^{-1}$, et $f(x_1 \dots x_n) = f(x_1) \dots f(x_n)$, pour tout lacet $x_1 \dots x_n$ de M .

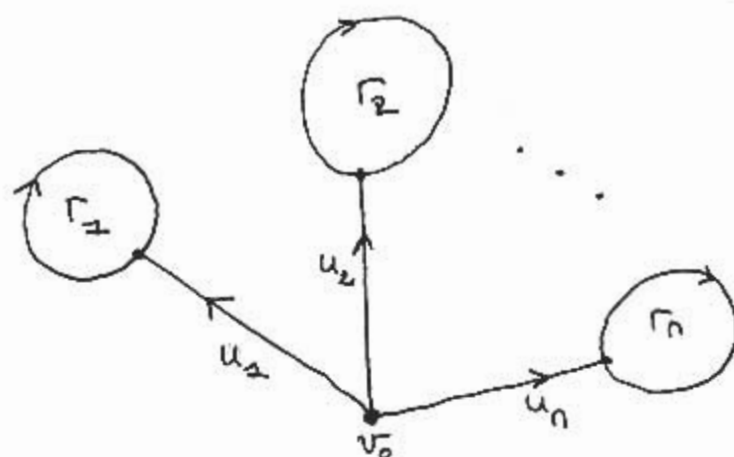
(3) le label d'un lacet fermé simple bordant une 2-cellule de M , est un élément de R_* .

(4) P a pour label ω_0 .

Etant données une présentation $\langle S / R \rangle$ et $\omega \in N$, peut-on construire un diagramme de Lyndon-Van Kampen.

$$\omega =_F \prod_{i=1}^n u_i r_i u_i^{-1} \equiv W, \quad \text{où } r_i \in R_*$$

On peut alors considérer le 2-complexe M pointé par v_0 , et une fonction de label, tel que le label du lacet bordant M débutant et finissant en v_0 est W . Si on identifie toutes les arêtes débutant ou finissant au même point, portant le même label, alors on obtient un deux complexe ayant pour label au bord (débutant en v_0) ω . Mais le 2-complexe peut ne pas rester planaire (cf [13] p



Théorème IV.1.1 : Pour toute présentation $\langle S / R \rangle$, et pour tout $w \in N$, il existe un diagramme de Lyndon-Van Kampen de w sur $\langle S / R \rangle$.

IV.1.2 Inégalité isopérimétrique

Définitions : Soit $\langle S / R \rangle$ une présentation de groupe. On dit que $\langle S / R \rangle$ satisfait une inégalité isopérimétrique, si il existe une fonction récursive $D : \mathbb{N} \rightarrow \mathbb{N}$, tel que si $w \in N$ alors

$$w =_F \prod_{i=1}^N p_i^{-1} r_i p_i, \text{ où } r_i \in R, \text{ et } N \leq D(\text{lgr}(w)).$$

D s'appelle fonction de Dehn.

On dit qu'un groupe satisfait une inégalité isopérimétrique si une de ses présentations admet une inégalité isopérimétrique.

On dit qu'un groupe satisfait une inégalité isopérimétrique linéaire (resp^t quadratique, exponentielle) si il admet une inégalité isopérimétrique, avec D linéaire (resp^t quadratique, exponentielle).

Théorème IV.1.2 : Un groupe f.p. a un problème du mot soluble ssi il admet une inégalité isopérimétrique.

Démonstration : On se donne une présentation finie $\langle S / R \rangle$ de G . On peut sans perte de généralité supposer que R est symétrisé.

(\Rightarrow) Si $\langle S / R \rangle$ a un problème du mot soluble on construit D de la façon suivante : pour $n \in \mathbb{N}^*$, on considère tous les mots de longueur n triviaux (ils sont en nombre fini). On peut pour chacun

en donner une écriture sous forme de produits de conjugués de relateurs (en énumérant ces écritures et en décidant si elle représente l'élément considéré). On définit alors $\mathcal{D}(n)$ comme la longueur maximale du nombre de relateurs dans une telle écriture pour tous les éléments triviaux de longueur n . Puisque \mathcal{D} est constructible, elle est récursive.

(\Leftarrow) On note ρ la longueur maximale d'un relateur. Etant donné un élément trivial réduit ω , on lui associe son diagramme de Van Kampen. Alors chaque u_i dans son écriture comme produit de conjugués de relateurs, est le label d'un lacet \bar{u}_i de M . On supprime dans \bar{u}_i les sous lacets fermés.

On obtient alors un lacet qui ne passe pas 2 fois par la même arête. Le label de lacet est u'_i , et $u_i = u'_i$ dans G (tout lacet fermé borde un disque puisque M est simplement connexe. Il y a au plus $\text{lgr}(\omega) + \rho \mathcal{D}(\text{lgr}(\omega))$ arêtes dans M , et donc :

$\text{lgr}(u'_i) \leq \text{lgr}(\omega) + \rho \mathcal{D}(\text{lgr}(\omega))$. Le membre de droite est récursif

et $\omega =_F \prod_{i=1}^N u'_i r_i u'_i$, et $N \leq \mathcal{D}(\text{lgr}(\omega))$

Puisque toutes les grandeurs sont bornées, on peut décider si ω s'écrit ainsi, et donc si $\omega =_G 1$. ■

IV.1.3 Algorithmes de Dehn

Définition : Soit $\langle S / R \rangle$ une présentation finie de groupe. On dit que $\langle S / R \rangle$ admet un algorithme de Dehn si il existe un ensemble fini Δ , $R \subseteq \Delta \subseteq N$, tel que pour tout mot $\omega \in N$, ω contient un sous-mot u , où $u, v \in \Delta$, et $\text{lgr}(v) < \text{lgr}(u)$.

Un algorithme de Dehn, donne une solution au problème du mot (effective). En effet considérons un mot ω . Si $\omega \in N$, alors on peut remplacer un sous-mot de ω , par un sous-mot de longueur moindre, préfixe d'un élément de Δ . En réitérant ce procédé on arrive au mot vide.

Proposition IV.1.1 : Si $\langle S / R \rangle$ admet un algorithme de dehn, alors $G = \langle S / R \rangle$, satisfait une inégalité

isopérimétrique linéaire .

Démonstration : On prend pour présentation de G , $\langle S / \Delta \rangle$. Si $\omega \in N$, alors $\omega \equiv \alpha u \beta$, où $r \equiv u v \in \Delta$, et $\text{lgr}(v) < \text{lgr}(u)$. Alors $\omega =_F \alpha v^{-1}(v r v^{-1}) \beta$, et $\omega =_G \alpha v^{-1} \beta \equiv \omega_1$ avec $\text{lgr}(\omega_1) < \text{lgr}(\omega)$.

On réitère ce procédé à ω_1 .

1^{er} cas : α (ou β) contient u' où $r' \equiv u' v' \in \Delta$, et $\text{lgr}(v') < \text{lgr}(u')$

alors $\omega =_F \alpha_1 v'^{-1}(v' r' v'^{-1}) \alpha_2 v^{-1}(v r v^{-1}) \beta$.

2^{ème} cas : v' n'est un sous-mot ni de α ni de β .

$$\begin{aligned} \text{alors } \omega &= _F \alpha v^{-1} \beta \beta^{-1}(v r v^{-1}) \beta \\ &= _F \alpha_1 v'^{-1}(v' r' v'^{-1}) \beta_1 \beta^{-1}(v r v^{-1}) \beta \\ &= _F \alpha_1 v'^{-1}(v' r' v'^{-1}) \beta_2^{-1}(v r v^{-1}) \beta \end{aligned}$$

où $\beta = \beta_1 \beta_2$.

En réitérant ce procédé, on obtient des mots de longueur décroissante (strict), et chaque application du procédé fait apparaître un conjugué de relateurs dans ω . Finalement on arrive à un mot vide, et ω s'écrit alors comme conjugués de relateurs. Puisque l'on peut effectuer ce procédé au plus $\text{lgr}(\omega)$ fois, ω s'écrit :

$$\omega =_F \prod_{i=1}^N u_i r_i u_i^{-1}, \text{ où } N < \text{lgr}(\omega).$$

Définition : On dit qu'une présentation de groupe vérifie un algorithme de Dehn pour le problème de la conjugaison, si lorsque ω et ω' sont conjugués sur cette présentation, alors il existe h , tel que $\omega' = h^{-1} \omega h$, et $\text{lgr}(h) \leq K (\text{lgr}(\omega) + \text{lgr}(\omega'))$.

Il est clair que pour une présentation f.e., on a alors une solution au problème de conjugaison.

IV.2 GROUPES A PETITES SIMPLIFICATIONS

IV.2.1 Hypothèses de petites simplifications

On considère une présentation de groupe $\langle S/R \rangle$, où R est un ensemble de mots cycliquement réduits sur S . On note R_* le

symétrisé de R (alors les éléments de R_* sont des mots cycliquement réduits sur S) .

On appelle pièce (relative à R) , tout mot u préfixe de deux éléments de R_* , i.e. $\exists r_1, r_2 \in R_*$, tel que $r_1 \equiv u r'_1$ et $r_2 \equiv u r'_2$

Soit $\lambda \in \mathbb{R}_+$. On dit que R satisfait la condition $C'(\lambda)$, si $\text{lgr}(u) < \lambda \text{lgr}(r)$ pour tout $r \in R_*$ et tout préfixe u de r qui est une pièce .

Remarquons que $C'(\lambda) \Rightarrow C'(\lambda') ; \forall \lambda' \geq \lambda$

Soit $p \in \mathbb{N}$. R satisfait la condition $C(p)$, si aucun élément de R_* n'est un produit de moins (st^t) de p pièces .

Remarque : pour $n \in \mathbb{N}_*$; si R satisfait $C'(\frac{1}{n})$ alors R satisfait $C(n+1)$.

En effet supposons que $r \in R_*$ s'écrive $r \equiv u_1 \dots u_p$ où les u_i sont des pièces et $p < n+1$. Alors puisque r satisfait $C'(\frac{1}{n})$ $\text{lgr}(u_i) < \frac{1}{n} \text{lgr}(r)$. Et donc puisque $\text{lgr}(r) = \sum \text{lgr}(u_i)$, c'est contradictoire .

Soit un entier $q \geq 3$. R satisfait la condition $T(q)$ si pour tout entier $l ; 3 \leq l < q$, et pour tout l -uplet d'éléments de R_* (r_1, \dots, r_l) , on a :

si $r_1 \neq r_2^{-1}, \dots, r_{l-1} \neq r_l^{-1}, r_l \neq r_1^{-1}$, alors au moins un des mots $r_1 r_2 ; \dots ; r_{l-1} r_l ; r_l r_1$ est librement réduit .

Remarquons que tout ensemble R satisfait $T(3)$.

La condition $C'(p)$ est appelé condition métrique .

IV.2.2 Interprétation géométrique .

Considérons une présentation de groupe $\langle S \mid R \rangle$, ω_0 un mot réduit de $N = \text{gp}_{F(S)}(R)$, et un diagramme de Lyndon-Van Kampen (M, f, p) de ω_0 sur $\langle S \mid R \rangle$. On appelle sous-disque extremum D , de M ; un sous-disque de M relié au reste de M par un segment , ou par identification d'un point . Puisque M est simplement connexe , soit M est un disque , soit il contient au moins un sous-disque

extremum .

On appelle consolidation de D , l'opération consistant à éliminer les sommets de degré 2 , en consolidant les arêtes concourants en ce point i.e. si $(v_1;v_2)$ et $(v_2;v_3)$ sont des arêtes orientées ,on les remplace par $(v_1;v_3)$.

Ceci définit une nouvelle fonction de label sur D ; (D,f_d) ; qui envoie chaque arête sur un mot réduit sur s ,tel que

$$f_d((v_1;v_3)) \equiv f((v_1;v_2));f((v_2;v_3))$$

Clairement ,la structure simpliciale (et donc l'espace topologique sous-jacent) est inchangée .

Un sommet de D sera dit extérieur si il est sur ∂D . Autrement il sera dit intérieur .Une arête sera dite extérieure si au moins un de ses sommets est intérieur ,et autrement sera dite intérieure .Une face B de D sera dite extérieure si une des arêtes de ∂B est extérieure ,et sinon sera dite intérieure .

On peut alors donner une interprétation de la notion de pièce . Soit D un sous-disque de (M,f,p) ,et considérons une arête v qui est sur le bord de 2-cellules B_1 et B_2 .Si le label d'un lacet fermé de ∂B_1 débutant par l'arête orientée v ,est différent du label d'un lacet fermé de ∂B_2 débutant en v ,alors $f(v)$ est une pièce relative à R .

On dit qu'un diagramme est réduit s'il ne contient pas une arête orientée v de $\partial B_1 \cap \partial B_2$, de telle façon que le label de lacets fermés de ∂B_1 et ∂B_2 débutant en v aient même label .Dans un diagramme réduit ,toute 1-cellule (éventuellement consolidée) est une pièce .

Théorème IV.2.1 : (Lyndon)

Soit $\langle S / R \rangle$ une présentation , ω_0 un élément réduit de $N = gp_{f(s)}(R)$;alors il existe un diagramme réduit (M_0,f_0,P_0) , avec P_0 ayant pour label ω_0 .

Pour une démonstration ,voir [21] .

Dans un diagramme réduit , on peut donner une interprétation géométrique de conditions non-métriques $C(p)$ et $T(q)$.

Proposition IV.2.1 : Considérons (M_0,f_0,P_0) un diagramme réduit sur $\langle S/R \rangle$,

(1) si R satisfait $C(p)$ pour $p \geq 3$, alors chaque face intérieure d'un sous-disque de M_0 , a au moins p arêtes consolidées.

(2) Si R satisfait $T(q)$ pour $q \geq 4$ alors chaque sommet intérieur d'un sous-disque de M_0 , a pour degré p ; où $q \leq p$ ou $p = 2$.

Démonstration : (1) Soit D un sous disque de M_0 . On considère (D, f_D) la consolidation de D . On peut supposer que D a plus d'une face. Considérons alors une face intérieure B de D . puisque (M_0, f_0, P_0) est réduit, toutes les arêtes de ∂B sont des pièces. Puisque le label de $\partial B \in R_*$, le résultat provient de la définition de $C(p)$.

(2) Soit v un sommet intérieur de v , et e_1, \dots, e_d qui soient dans l'ordre, les arêtes orientées débutant en v . Supposons que $d \geq 3$, et que $d \leq q$. Pour tout $i = 1, \dots, d-1$, e_i et e_{i+1} sont respectivement la première et la dernière arête d'un lacet fermé, bordant une face de M_0 . De même e_d et e_1 sont respectivement l'arête initiale et l'arête terminale d'un lacet bordant une face. On note r_1, r_2, \dots, r_d les labels des faces correspondantes. Alors aucun des produits $r_1 r_2 \dots r_d r_1$ ne se réduit librement. Or puisque M_0 est un diagramme réduit $r_1 \neq r_2^{-1}$, etc... Ceci contredit la condition $T(q)$ ■

IV.2.3 Formules et inégalités pour des disques

Notations : Soit T un 2-complexe fini dont l'espace topologique sous-jacent est un disque. on note $d(s)$ le degré d'un sommet, i.e. le nombre d'arêtes orientées débutant en s . On note $d(B)$ le degré d'une face B , i.e. le nombre d'arêtes constituant ∂B . $e(B)$ et $i(B)$ représentent respectivement, le nombre d'arêtes extérieures et intérieures de ∂B . On note S le nombre de sommets de T , A le nombre d'arêtes, et F le nombre de faces.

Considérons un 2-complexe fini T , dont l'espace topologique sous-jacent est un disque. La caractéristique d'Euler donne l'équation: (1) $1 = S - A + F$

Les équations (2) et (3) sont aisées à établir par le décompte des

arêtes .

$$\left\{ \begin{array}{l} (1) \quad 1 = S - A + F \\ (2) \quad 2 A = \sum_s d(s) \\ (3) \quad 2 A = \sum_B d(B) + d(D) \end{array} \right.$$

Prenons (p,q) ,qui soit un des couples $(6,3)$; $(4,4)$; ou $(3,6)$. Dans les 3 cas ,on a $p = 2((p/q) + 1)$.En utilisant le covecteur $(p ; -p/q ; -1)$ et le système $(*)$,on obtient l'équation :

$$p - 2 \frac{p}{q} A - 2 A = p S - p A + p F - \frac{p}{q} \sum_s d(s) - \sum_B d(B) - d(D)$$

$$\Leftrightarrow p = (p S - \frac{p}{q} \sum_s d(s)) + (p F - \sum_B d(B)) - d(D)$$

$$\Leftrightarrow p = \frac{p}{q} \sum_s (q - d(s)) + (p F - \sum_B d(B)) - d(D) \quad (4)$$

Si $(p,q) = (6,3)$ on utilise $d(D) = \sum_B e(B) = \sum_{e(B)=1} 1 + \dots + \sum_{e(B)=k} k + \dots$

ainsi que $F = \sum_{e(B)=0} 1 + \sum_{e(B)=1} 1 + \dots$;et $d(B) = e(B) + i(B)$,sur les

2 derniers termes de (4) .On obtient l'égalité (5) :

$$6 = 2 \sum_s (3 - d(s)) + \sum_{e(B)=0} (6 - i(B)) + \sum_{e(B)=1} (4 - i(B)) + \sum_{\substack{e(B)=k \\ k \geq 1}} (6 - 2k - i(B))$$

Si $(p,q) = (4,4)$,on décompose la première somme en une somme sur les sommets intérieurs (indiquée par sint) ,et une somme sur les sommets extérieurs (indiquée par sext) et on utilise alors le fait que $d(D) = \sum_{sext} 1$.On décompose la deuxième de façon analogue au

cas $(6,3)$ (à part que l'on n'utilise pas $d(D)$ dans cette décomposition) .On obtient l'équation (6) :

$$4 = \sum_{sint} (4 - d(s)) + \sum_{sext} (3 - d(s)) + \sum_{e(B)=0} (4 - i(B))$$

$$+ \sum_{e(B)=1} (3 - i(B)) + \sum_{\substack{e(B)=k \\ k \geq 1}} (4 - k - i(B))$$

Si $(p,q) = (3,6)$, on utilise $-\frac{3}{2}d(D)$ dans la somme indicée sur les sommets extérieurs, et $\frac{1}{2}d(D)$ dans le dernier terme. On obtient l'équation (7) :

$$3 = \frac{1}{2} \sum_{s \in I} (6 - d(s)) + \frac{1}{2} \sum_{s \in E} (3 - d(s)) + \sum_{e(B)=0} (3 - i(B)) \\ + \sum_{e(B)=1} (\frac{3}{2} - i(B)) + \sum_{\substack{e(B)=k \\ k \geq 1}} (3 - \frac{k}{2} - i(B))$$

Théorème IV.2.2 : (Lyndon)

Soit (p,q) une des paires $(6,3)$; $(4,4)$; $(3,6)$. Soit T la consolidation d'un 2-simplexe fini D , dont l'espace topologique sous-jacent est un disque. Si tout sommet s , a un degré $d(s) \geq 3$, si tout sommet intérieur a un degré $d(s) \geq q$, et si toute face intérieure de T a un degré $d(B) \geq p$, alors on a l'inégalité suivante :

$$p \leq \sum_{e(B)=1} (\frac{p}{q} + 2 - i(B)) \quad \blacksquare$$

Démonstration : On utilise les égalités précédemment établies, (5), (6) et (7). Puisque pour tout sommet intérieur s , $d(s) \geq q$, le premier terme de (6) et (7) est négatif. Puisque tout sommet a un degré $d(s) \geq 3$, le premier terme de (5) et le deuxième terme de (6) et (7) sont négatifs. Puisque toute face intérieure de T a au moins p arêtes, le deuxième terme de (5), et le troisième terme de (6) et (7) sont négatifs. Puisque des arêtes extérieures d'une face ne sont jamais adjacentes (T est consolidé) alors pour une face extérieure (i.e. $e(B) > 0$) $i(B) \geq e(B)$, et alors le dernier terme de (5), (6) et (7) est négatif. Ainsi on a les inégalités :

$$\text{si } (p,q) = (6,3) \quad ; \quad 6 \leq \sum_{e(B)=1} (4 - i(B))$$

$$\text{si } (p,q) = (4,4) \quad ; \quad 4 \leq \sum_{e(B)=1} (3 - i(B))$$

$$\text{si } (p,q) = (3,6) \quad ; \quad 3 \leq \sum_{e(B)=1} \left(\frac{5}{2} - i(B)\right)$$

Et alors si (p,q) est un des couples $(6,3)$; $(4,4)$; $(3,6)$, on a l'inégalité :

$$p \leq \sum_{e(B)=1} \left(\frac{p}{q} + 2 - i(B)\right) \quad \blacksquare$$

Remarque : Cette propriété est géométrique ,et c'est géométriquement que Lyndon l'a démontrée .Les couples $(6,3)$, $(4,4)$, $(3,6)$ correspondent aux trois pavements réguliers du plans ,respectivement par des hexagones ,des carrés ,des triangles .La relation établie ,représente alors une relation de courbure .Par exemple dans le cas $(6,3)$,elle représente le résultat ,que dans le pavage régulier du plan par des hexagones ,chaque hexagone extérieur ($e(B) = 1$) contribue à $\frac{\pi}{3} (4 - i(B))$ de la courbure totale .

IV.2.4 Algorithme de Dehn et inégalité isopérimétrique linéaire pour des groupes à petites simplifications .

Théorème IV.2.1 : Soit $\langle S / R \rangle$ une présentation telle que R satisfait $C'(1/6)$,ou $C'(1/4)$ et $T(4)$,ou $C'(1/3)$ et $T(6)$.Alors si ω_0 est un mot réduit non vide ,trivial dans $\langle S / R \rangle$,alors ω_0 contient un sous-mot u ,préfixe d'un élément $u v$ de R_* ,tel que $\text{lgr}(v) < \text{lgr}(u)$.

Démonstration : Considérons un diagramme réduit (M,f,P) ayant pour label sur son bord ω_0 (d'après le théorème IV.2.1 un tel diagramme existe .Puisque M est fini et simplement complexe ,c'est un disque ,ou alors il contient un sous-disque extremum D relié au reste du diagramme par v_1 (nous effectuerons sans perte de généralité la démonstration dans ce dernier cas) .Si D contient une unique 2-cellule ,alors le label du segment bordant D

, débutant en v_1 est un élément de R_* et un sous-mot de ω_0 , est donc dans ce cas la conclusion est vraie.

Si D contient plus d'une 2-cellule, on consolide D . Alors puisque $C'(1/n) \Rightarrow C(n+1) \Rightarrow C(n)$ avec le théorème IV.2.2, et la proposition IV.2.1, on a pour $(p,q) = (6,3)$ ou $(4,4)$ ou $(3,6)$:

$$p \leq \sum_{e(B)=1} (p/q + 2 - i(B))$$

Puisque $i(B) \geq 1$ pour toute face extérieure B de D , on peut vérifier pour (pq) donné comme précédemment que chaque terme de la somme est au plus $p/2$. Et donc, au moins deux faces B_1 et B_2 ($e(B_1) = e(B_2) = 1$) contribuent positivement (strict¹) à la somme. Il est aisé de vérifier que le label de ∂D débutant en v_1 , contient le label de $\partial B_1 \cap \partial D$ ou de $\partial B_2 \cap \partial D$ comme sous-mot. Considérons par exemple le 1^{er} cas, et notons u le label de $\partial B_1 \cap \partial D$, et alors uv est le label d'un circuit constituant ∂B_1 , où uv est un élément de R_* (R_* est clos par conjugaison cyclique, et tous ses éléments sont cycliquement réduits). Or puisque B_1 contribue positivement à la somme, $i(B_1) \leq p/q + 1$, et donc v est un produit d'au plus $p/q + 1$ pièces. Or puisque R satisfait $C'(1/p)$, on a :

$$\begin{aligned} \text{lgr}(v) &< (p/q + 1) \times 1/p \times \text{lgr}(uv) = (1/p + 1/q) \times \text{lgr}(uv) \\ &= \frac{\text{lgr}(uv)}{2} \end{aligned}$$

et donc $\text{lgr}(v) < \text{lgr}(u)$ ■

Corollaire IV.2.1.1 : Des groupes f.p., vérifiant $C'(\frac{1}{6})$, ou $C'(\frac{1}{4})$ et $T(4)$, ou $C'(\frac{1}{3})$ et $T(6)$ ont un algorithme de Dehn.

Et alors avec la proposition IV.1.1

Corollaire IV.2.1.1 : Des groupes f.p., vérifiant $C'(\frac{1}{6})$, ou $C'(\frac{1}{4})$ et $T(4)$, ou $C'(\frac{1}{3})$ et $T(6)$ satisfont une inégalité isopérimétrique.

IV.3 GROUPES HYPERBOLIQUES

IV.3.1 Structure métrique dans un groupe f.e.

Soit G un groupe , et S un système fini de générateurs de G .
On définit une métrique du mot dans G sur l'alphabet S ,de la façon suivante :

Si w est un mot sur S (i.e. sur $S \cup S^{-1}$ où S^{-1} est l'ensemble des inverses des éléments de S , dans G) , $w \equiv g_1 \dots g_n$ avec pour tout $i = 1 \dots n$, $g_i \in S \cup S^{-1}$; on définit la longueur de w comme étant le nombre n de lettres composants w .

On la note $lg_s(w)$.

On définit alors une distance sur G (par rapport à S) de la façon suivante :

Soit $g \in G$ $d_s(1;g) := \text{Inf} \{ lg_s(w) \mid w \text{ est un mot sur } s \text{ et } w =_G g \}$

Soient $g_1, g_2 \in G$ $d_s(g_1;g_2) := d_s(1;g_1^{-1}g_2)$

A vérifier : (i) Séparation : $d_s(g_1;g_2) = 0 \Leftrightarrow d_s(1;g_1^{-1}g_2) = 0$

$$\Leftrightarrow g_1^{-1}g_2 = 1 \text{ dans } G$$

$$\Leftrightarrow g_1 = g_2 \text{ dans } G \quad \square$$

(ii) Symétrie : Si w est un représentant de $g_1^{-1}g_2$ dans G , alors \tilde{w} obtenu en remplaçant s^ϵ par $s^{-\epsilon}$ dans w ; $\forall s \in S \cup S^{-1}$; $\forall \epsilon = \pm 1$; est un représentant de $(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1$ (et réciproquement) , et donc :

$$\begin{aligned} d_s(g_1;g_2) &= d_s(1;g_1^{-1}g_2) \\ &= d_s(1;g_2^{-1}g_1) \\ &= d_s(g_2;g_1) \quad \square \end{aligned}$$

(iii) Inégalité triangulaire : Soient $g_1, g_2, g_3 \in G$
Si ω_1 est un représentant de $g_1^{-1}g_2$ et ω_2 est un représentant de $g_2^{-1}g_3$ alors $\omega \equiv \omega_1\omega_2$ (concaténation) est un représentant de $g_1^{-1}g_3$
et $lg_s(\omega) = lg_s(\omega_1) + lg_s(\omega_2)$

et donc $d_s(1;g_1^{-1}g_3) \leq d_s(1;g_1^{-1}g_2) + d_s(1;g_2^{-1}g_3)$

soit $d_s(g_1;g_3) \leq d_s(g_1;g_2) + d_s(g_2;g_3)$

■

La donnée d'un système générateur fini S de G nous permet donc de définir une métrique sur G . On note $(G;S)$ l'espace métrique

associé .

On peut reprocher à cette définition de distance de dépendre du choix du système de générateurs . Nous verrons que toutes les propriétés métrique qui nous intéresseront ne dépendent pas de ce choix .

Lorsque le contexte le permettra nous noterons lg (resp^t. d) .

Remarque : L'action de G sur lui-même , par translations à gauche s'effectue par isométrie i.e. $\forall g; g_1; g_2 \in G$.

$$d(gg_1; gg_2) = d(g_1; g_2) .$$

En effet tout représentant de $g_1^{-1}g^{-1}gg_2$ est un représentant de $g_1^{-1}g_2$

L'action à droite ne s'effectue pas par isométrie .

En effet dans le groupe libre $f(a; b)$, $d(1; a) < d(b; ab)$.

On notera $|g|$ pour $d(1, g)$.

IV.3.2 Graphe de cayley

Soit G un groupe engendré par S . Le graphe de cayley $\Gamma_S(G)$ de G , relativement à S , est la réalisation géométrique d'un complexe simplicial de dimension 1 , défini de la façon suivante :

- $\forall g \in G$ on associe un unique sommet noté $s(g)$
- $(s(g); s(g'))$ définit une arête orientée , étiquetée x si $gx = g'$ dans G avec $x \in S \cup S^{-1}$.

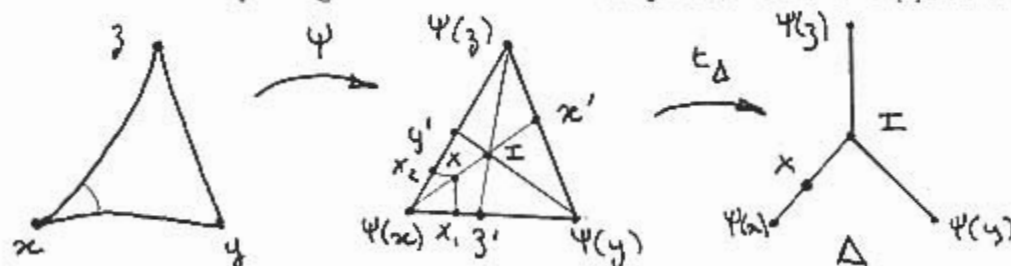
On munit $\Gamma_S(G)$ de la métrique simpliciale i.e. , la longueur d'un chemin , est le nombre d'arêtes le composant . La distance entre deux sommets , est la borne inférieure , de la longueur des chemins les reliant . Ainsi le plongement naturel de $(G; S)$, sur les sommets de $\Gamma_S(G)$ est une isométrie , et G agit à gauche sur $\Gamma_S(G)$ isométriquement par automorphismes simpliciaux . $\Gamma_S(G)$ devient donc un espace métrique géodésique construit sur un complexe simplicial de dimension 1 , connexe par arc , sans arêtes multiples et localement fini si S est fini .

Il existe une autre façon de définir le graphe de Cayley d'un groupe . Considérons un groupe f.p. $G = \langle S / R \rangle$. On a une façon "standard" de construire un 2.complexe simplicial ayant pour groupe fondamental G . Ce 2.complexe consiste en une 0.cellule , une

1.cellule orientée pour tout générateur (de telle façon que si $(v;v')$ est une 1.cellule ayant pour label $x \in S$, $(v';v)$ a pour label x^{-1}) et une 2.cellule pour tout relateur. On construit un "bouquet", en identifiant tous les sommets des 1.cellules, avec la 0.cellule. Pour tout relateur $r \in R$, il existe un lacet fermé dans le bouquet ayant pour label r . On identifie alors ce lacet avec le bord d'une 2.cellule. Après subdivision, on obtient alors un complexe simplicial K (abstrait), fini, et d'après le *théorème de Seifert-Van Kampen*, $\pi_1(K) \cong G$. Considérons le revêtement universel \tilde{K} de K . C'est un complexe simplicial de dimension 2, dans lequel on fixe un sommet v_0 . On considère alors le 1.squelette $\tilde{K}^{(1)}$ pointé sur v_0 . G agit simplement sur \tilde{K} , et pour $g \in G$, on donne le label g à $g.v_0$ (v_0 a alors pour label 1). Or puisque $G \cong \text{Aut}(\tilde{K})$, G agit par automorphismes simpliciaux, et donc on a une bijection Π de G , sur les sommets de $(\tilde{K}^{(1)}, v_0)$. Pour $x \in S$, on donne le label x , à toute arête $(\Pi(g), \Pi(g'))$ telle que $g' =_G g \times x$. $(\tilde{K}^{(1)}, v_0)$ est alors le graphe de Cayley $\Gamma_S(G)$.

IV.3.3 Espace hyperbolique

Soit E un espace métrique et (xyz) un triangle géodésique. On peut plonger isométriquement (xyz) dans un triangle du plan euclidien (un tel plongement existe toujours, on l'appellera ψ).



Considérons I intersection des bissectrices de $(\psi(x); \psi(y); \psi(z))$. La bissectrice des deux droites est l'ensemble des points à égale distance de ces deux droites. Donc $d(I; y') = d(I; z')$ (et toutes les autres égalités obtenues par permutations cycliques), où $x'; y'; z'$ sont l'intersection du cercle inscrit avec respectivement $[\psi(y); \psi(z)]$; $[\psi(x); \psi(z)]$; $[\psi(x); \psi(y)]$. On définit par morceaux l'application de $(\psi(x); \psi(y); \psi(z))$ dans le tripode Δ , par :

$$t_{\Delta x,y} : [\psi(x); y'] \longrightarrow [\psi(x); I]$$

(composée d'une rotation et d'une homothétie)

, tel que $\psi(x) \longrightarrow \psi(x)$; et $y' \longrightarrow I$.

On définit de même $t_{\Delta x,z}$; $t_{\Delta y,x'}$ etc...

Alors I admet 3 préimages par t_{Δ} , x', y', z' .

$\psi(x); \psi(y); \psi(z)$ admettent chacun 1 préimage (eux-même) et tout

$X \in]\psi(x); I[$ admet 2 préimages X_1 et X_2 tel que $X_1 \in]\psi(x); z'[$;

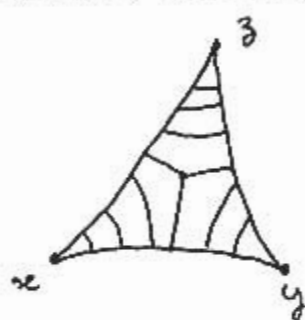
$X_2 \in]\psi(x); y'[$ et $d(\psi(x); X_1) = d(\psi(x); X_2)$

(de même pour les autres segments du tripode) .

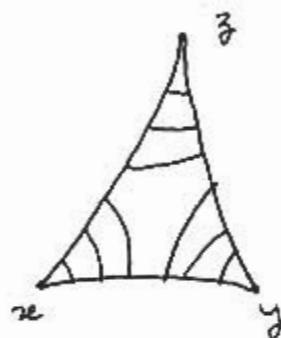
On peut alors dans (x, y, z) relier tous les points préimages d'un même élément par $t_{\Delta} \circ \psi$, par un segment géodésique . On obtient une **foliation** (unique) du triangle $(x; y; z)$.

Soit $(x; y; z)$ un triangle géodésique dans le graphe de Cayley $\Gamma_S(G)$

On a alors la foliation :



ou



si $d(\psi(x); y') \in \mathbb{N}$

(par exemple)

Définitions : Soit un espace métrique géodésique . Soit un triangle géodésique (xyz) et Δ son tripode associé . (xyz) est dit δ .fin si $\forall a \in \Delta$, $\text{diam}((t_{\Delta, o\psi})^{-1}(a)) \leq \delta$.

Soit E un espace métrique géodésique . E est dit δ .hyperbolique si tout triangle de E est δ .fin .

E est dit **hyperbolique** si il existe $\delta \in \mathbb{R}_+$ tel que E soit δ .hyperbolique .

Un groupe G donné par une présentation f.e. $\langle S / R \rangle$ est dit δ .hyperbolique (resp^t hyperbolique) . si $\Gamma_S(G)$ est un espace métrique δ -hyperbolique (respectivement hyperbolique) .

Remarques : Pour un groupe , être hyperbolique est défini pour une famille génératrice . Nous verrons néanmoins qu'être hyperbolique dépend pas du choix de la famille génératrice .

Exemples : -Les groupes libres de rang fini sont δ .hyperboliques . En effet son graphe de Cayley est un arbre (car un circuit correspondrait à un élément réduit non vide ,trivial) et donc tout triangle est plat .

-Les groupes finis sont hyperboliques , car les distances sont bornées .

Définition : Soit (xyz) un triangle géodésique dans un espace métrique . (x,y,z) est dit δ .mince si les segments $[x;y]$, $[y;z]$, $[y;z]$, $[x;z]$ se trouvent chacun dans un δ -voisinage fermé des deux autres , i.e. :

$$[x;y] \subseteq \bar{V}_\delta ([y;z] \cup [x;z])$$

$$[y;z] \subseteq \bar{V}_\delta ([x;y] \cup [x;z])$$

$$[x;z] \subseteq \bar{V}_\delta ([x;y] \cup [y;z])$$

Il est trivial de vérifier que δ .fin \Rightarrow δ .mince .De plus on a la réciproque (à une constante près)

δ .mince $\Rightarrow 4\delta$.fin . (cf [13]) .

Théorème IV.3.1 : Si G est un groupe δ .hyperbolique sur une présentation f.e. $\langle S / R \rangle$ alors :

(i) G admet une présentation finie

(ii) Le problème du mot est résoluble pour G .

Démonstration : Soit S système de générateur de G tel que $(G;S)$ est δ .hyperbolique .Considérons $\Gamma_S(G)$.

Soit ω un mot sur S tel que $\omega = 1$ dans G .

$\omega \equiv a_1 \dots a_i \dots a_n$. Soit $S(\omega)$ son image par le plongement naturel dans $\Gamma_S(G)$. Alors $S(\omega)$ est un circuit dans $\Gamma_S(G)$. Dans la suite on identifiera ω et $S(\omega)$.

On considère un triangle géodésique

$(1;g_{i-1};g_i)$ où $g_{i-1} = a_1 \dots a_{i-1}$

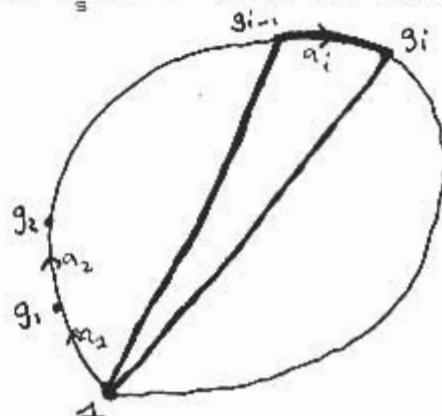
et $g_i = a_1 \dots a_n$

Puisque $(1;g_{i-1})$ et $(1;g_i)$ sont des

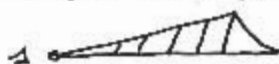
géodésiques , et que $d(g_{i-1};g_i) = 1$

forcément $|g_i| = |g_{i-1}| \pm 1$

ou $|g_i| = |g_{i-1}|$



Dans le premier cas le triangle est plat , et on a donc la foliation sur $(1;g_{i-1};g_i)$:



Dans le deuxième cas on a la foliation :



-notre objectif est de décomposer le circuit de label ω en lacets de longueur borné , et de majorer cette décomposition . On utilisera donc le cas 1 .

Le triangle $(1;g_{i-1};g_i)$ est géodésique donc son périmètre est inférieur à $lg(\omega) = n$.

Donc $lg([1;g]) \leq \frac{n}{2}$ et $lg([1;g]) \leq \frac{n}{2}$

On peut alors décomposer $(1;g_{i-1};g_i)$

en au plus $\frac{n}{2}$ petits lacets

de longueurs $\leq 2\delta + 2$.

On "conjugue" les lacets de façon

à leur donner pour point d'origine 1 .

Après avoir effectué le même procédé

pour tout triangle géodésique $[1;g_{i-1};g_i]$ $i = 2 \dots n$

On obtient une décomposition $\frac{n^2}{2}$ petits lacets de longueur $\leq 2\delta + 2$

Cette décomposition équivaut à une expression :

$$\omega =_F \prod_{i=1}^N u_i r_i u_i^{-1}$$

où $r_i = 1$ dans G et $l(r_i) \leq 2\delta + 2$, $l(p_i) \leq \frac{n}{2}$; et $N \leq \frac{n^2}{2}$

Et aussi tout élément trivial dans G , se décompose de la même façon .

On peut donc prendre tous les r_i ainsi obtenus comme relateurs .

Or δ est fixe ,et donc leur longueur est bornée ,Puisque la famille génératrice est finie les r_i sont en nombre fini . On a donc une présentation finie de G .

De plus on a alors une inégalité isopérimétrique quadratique ,et on peut donc résoudre le problème du mot dans G . ■

IV.3.4 Caractérisation des groupes ayant un algorithme de Dehn ou une inégalité isopérimétrique linéaire .

Définition : Un mot ω est λ -géodésique local ($\lambda \in \mathbb{R}_+$) ,si tout sous-mot de ω de longueur inférieure à λ est une géodésique .

Proposition IV.3.1 : Soit G un groupe δ -hyperbolique sur une présentation $\langle S \mid R \rangle$. Soit w un mot non vide sur cette présentation. Si w est une $(2\delta + 3)$ -géodésique locale, alors $w \neq_g 1$.

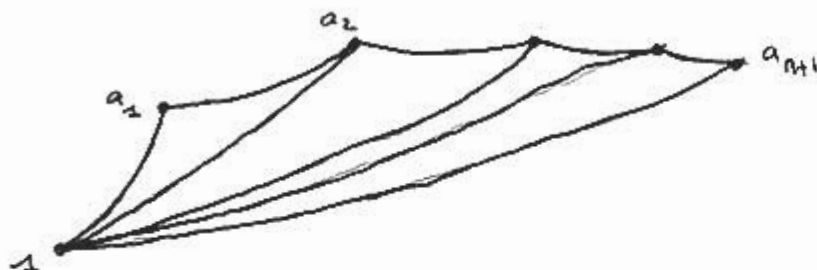
Démonstration : Si $\text{lgr}(w) \leq 2\delta + 3$, alors $w = 1$ ssi $w \equiv 1$. On peut donc supposer $\text{lgr}(w) \geq 2\delta + 3$.

On considère la présentation pour laquelle G est hyperbolique, et $\Gamma_S(G)$ son graphe de Cayley. On considère \tilde{w} un lacet de $\Gamma_S(G)$ ayant pour label w .

Il existe n tel que $w \equiv w_1 \dots w_n w_{n+1}$, et $\text{lgr}(w_i) = 2\delta + 3$ pour tout $i = 1 \dots n$, et $\text{lgr}(w_{n+1}) \leq 2\delta + 3$.

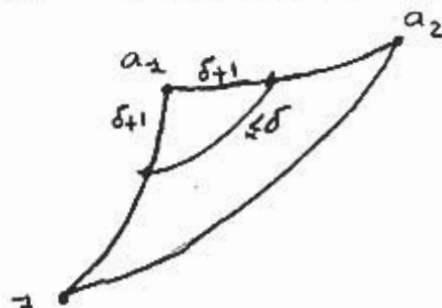
On pose $w_1 = a_1$, et pour $i = 1 \dots n$, $a_i w_{i+1} = a_{i+1}$ dans G .

On considère les triangles géodésiques $(1, a_i, a_{i+1})$ dans le graphe de Cayley. $i = 1 \dots n$.



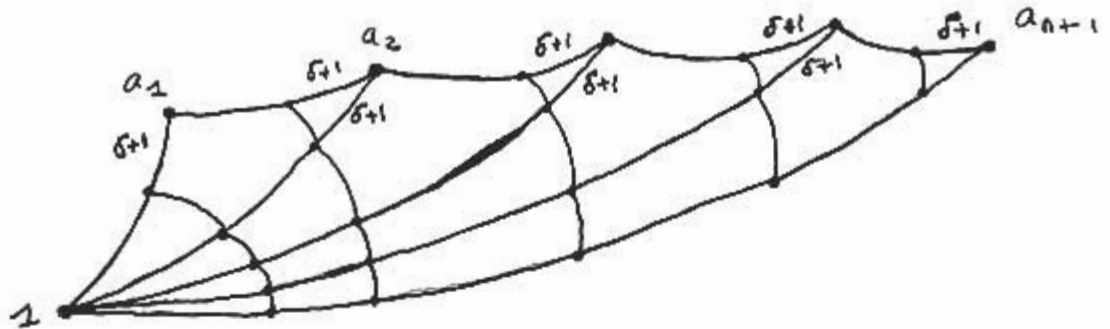
Lemme IV.3.1 : Au plus δ éléments de $[a_i, a_{i+1}]$ et de $[a_{i-1}, a_i]$, sont reliés par des arcs de foliations ($i = 1 \dots n-1$, et $a_0 = s(1)$).

Démonstration : Pour $i = 1$, considérons $(1, a_1, a_2)$ et les éléments de $[1, a_1]$ et $[a_1, a_2]$ à distance $\delta + 1$ de a_1 (on se rappelle que ces segments ont pour longueur $2\delta + 3$). Si ces points étaient reliés par un arc de foliation, alors un sous-mot de w de longueur $2\delta + 2$ n'est pas géodésique (contradiction avec le fait que w soit une $2\delta + 3$ géodésique locale).



Pour $i > 1$. Prenons les éléments de $[a_{i-1}, a_i]$ et $[a_i, a_{i+1}]$ à distance $\delta + 1$ de a_i . S'ils sont reliés par un arc de foliation, alors un sous-mot de w , de longueur $2\delta + 3$ n'est pas géodésique.

Revenons à la démonstration . Avec le lemme IV.3.1 , tout point à distance $\delta + 1$ de a_i ($i = 1 \dots n$) est relié par foliation à un point de $[1, a_{n+1}]$. Et par construction des foliations tous les points ainsi obtenus sur $[1, a_{n+1}]$ sont distincts .



Alors $[1, a_{n+1}]$ n'est pas le chemin nul , et donc ω qui correspond dans le groupe à a_{n+1} , n'est pas nul . ■

Théorème IV.3.2 : Un groupe hyperbolique admet un algorithme de Dehn pour sa présentation qui le rend hyperbolique .

Démonstration : Prenons pour Δ , tous les éléments de N de longueur au plus $4\delta + 5$. (Ils sont en nombre fini)

D'après la proposition IV.3.1 , si $\omega = 1$, alors ω n'est pas une $2\delta + 3$ géodésique locale . Et donc il existe un sous-mot μ de ω de longueur $\leq 2\delta + 3$, et un mot μ' tel que $\text{lgr}(\mu') < \text{lgr}(\mu) \leq 2\delta + 3$, et $\mu = \mu'$. Alors $\mu^{-1}\mu'$ est un élément de Δ . ■

Avec la proposition IV.1.1 , on a le corollaire suivant :

Corollaire IV.3.2.1 : Un groupe hyperbolique vérifie (pour un présentation adéquate) , une inégalité isopérimétrique linéaire .

Le résultat fondamental de ce chapitre est le suivant :

Théorème IV.3.3 : Soit un groupe G f.e. $G = \langle S / R \rangle$.
Les assertions suivants sont équivalentes :

(1) $\Gamma_S(G)$ est hyperbolique

- (2) G a un algorithme de Dehn sur cette présentation
 (3) G satisfait une inégalité isopérimétrique linéaire
 sur cette présentation .

Démonstration : Nous avons déjà démontré $(1) \Rightarrow (2) \Rightarrow (3)$.
 Nous allons démontrer $(3) \Rightarrow (1)$.

Nous effectuons la démonstration par l'absurde . On suppose qu'il n'existe pas une constante δ tel que tout triangle géodésique est δ -mince .

Alors pour tout $r > 0$, il existe un triangle géodésique xyz dans le graphe de Cayley Γ ; et un point $w \in [x;y]$ tel que :

$$\min (d(w;[y;z]);d(w;[x;z])) > 2r ,$$

Si xyz est dégénéré , alors il contient un triangle non dégénéré (ou un bigône) , contenant w ; vérifiant la même condition .

Alors sans perte de généralité , on considère que xyz est non dégénéré .

On prend une constante ε tel que $r > 6\varepsilon$.

$[xy]$ a une longueur au moins $24.\varepsilon$.

Tout point de $[x;y]$ à distance au plus 8ε de w ; est à une distance au moins 4ε des points de $[x;z]$ et de $[y;z]$.

Pour tout point $\alpha \in [x;z]$, $\beta \in [y;z]$; tel que $d(\alpha;x) \leq 10\varepsilon$

$$d(\beta;y) \leq 10\varepsilon$$

alors $d(\alpha,\beta) \geq 4\varepsilon$.

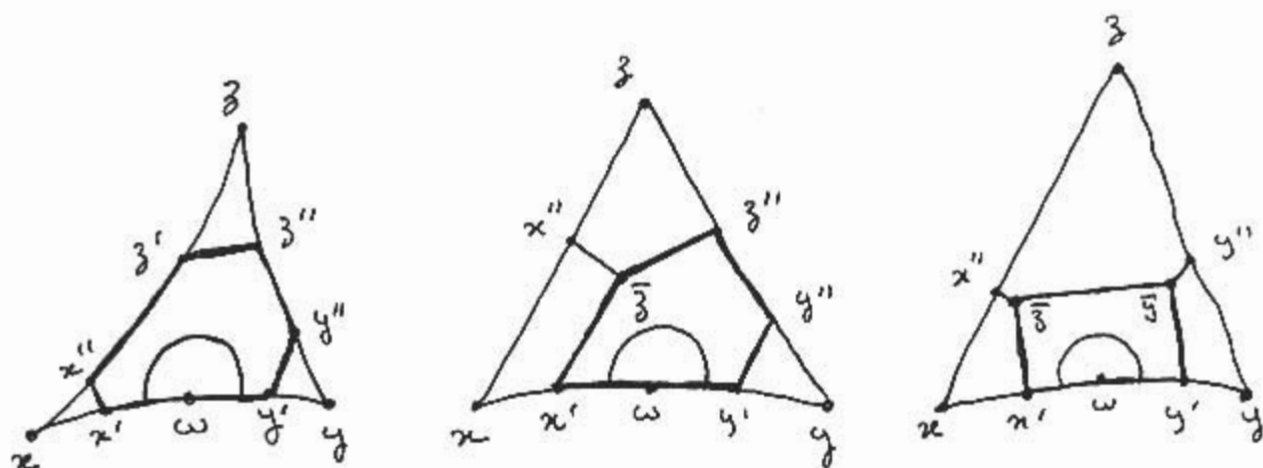
Pour r ,suffisamment grand $[x;z]$ et $[y;z]$ sont suffisamment grands .On peut considérer des points $x' \in [x;w] \setminus B(w,r)$; $y' \in [y;w] \setminus B(w,r)$; $x'';z' \in [x;z]$ et $y'';z'' \in [y;z]$ tels que tout point de $[x';y']$ (respectivement $[x'';z']$; $[y'';z'']$) est à une distance au moins 4ε des 2 autres côtés .On coupe alors les "coins" de xyz ; $[x';x'']$; $[y';y'']$; $[z';z'']$.

On obtient un des 3 cas suivants (fig 1)

- un hexagone non dégénéré .
- un pentagone non dégénéré .
- un quadrilatère non dégénéré .
- On considère le 1^{er} cas .

Si on appelle w le label de $(x'y'y''z''z'x''x')$, on identifie w ; avec le bord d'un diagramme de Van Kampen D ayant pour label w ; sur la présentation du groupe .

Ce diagramme a pour espace topologique sous-jacent un disque



puisque le lacet de label w est un cercle non singulier dans Γ .
On note α le lacet $[x'y']$; β le lacet $[x''z']$; γ le lacet $[z''y'']$
; θ le lacet (fermée) $(x'y'y''z''z'x'x')$.

On note $N(\alpha) = \text{Star}(\alpha)$ dans D .

On note ρ la longueur maximale des relateurs (on peut supposer $\rho > 1$ sinon G est 0-hyperbole . $N(\alpha)$ contient au moins $\text{lgr}(\alpha)/\rho$ 2-cellules .

On prend $\varepsilon > \rho$.

alors $N(\alpha)$ intersecte $[x';x'']$ et $[y'y'']$ en deux points x_1 et y_1

tels que $d(x';x_1) \leq \frac{\varepsilon}{2}$

$d(y';y_1) \leq \frac{\varepsilon}{2}$

On considère α_1 le lacet (x_1y_1) ne passant pas par ∂D .

On réitère alors cette opération $n = E(\frac{\varepsilon}{\rho})$ fois .

On a alors des points x_1, \dots, x_n sur $[x';x'']$; y_1, \dots, y_n sur $[y';y'']$
tel que $\alpha_1 = [x_1; y_1]$ est de longueur au moins $\text{lgr}(\alpha) - i\rho$ et tel que
tout point de $N(\alpha) = N(\alpha_1) \cup \dots \cup N(\alpha_n)$ est à une distance au plus
 ε de α .

N contient alors au moins

$$\frac{\text{l}(\alpha)}{\rho} + \frac{\text{l}(\alpha) - \rho}{\rho} + \dots + \frac{\text{l}(\alpha) - \varepsilon/\rho - 1}{\rho} \quad \text{2-cellules}$$

$$= \frac{\varepsilon}{\rho} \left(\frac{\text{l}(\alpha)}{\rho} \right) - \frac{\varepsilon(\varepsilon-1)}{2\rho} = \frac{\varepsilon}{\rho^2} \cdot \text{l}(\alpha) + K$$

où K est une constante ne dépendant que de ε .

On effectue la même opération sur β et γ .

Alors $N(\alpha) \cap N(\beta) = \emptyset$

$$N(\beta) \cap N(\gamma) = \emptyset$$

$$N(\alpha) \cap N(\gamma) = \emptyset$$

puisque ce sont de ε -Hausdorff voisinages de $\alpha; \beta; \gamma$ qui sont à une distance au moins 4ε l'un de l'autre.

Alors $N(\theta) = N(\alpha) \cup N(\beta) \cup N(\gamma)$ contient au moins

$$\begin{aligned} & \frac{\varepsilon}{\rho^2} \cdot (l(\alpha) + l(\beta) + l(\gamma)) + C \quad \text{2-cellules} . \\ & = \frac{\varepsilon}{\rho^2} l(\theta) + Q . \end{aligned}$$

Considérons $B(\omega; r)$. Elle n'intersecte pas $N(\beta)$ et $N(\gamma)$. Elle intersecte $N(\alpha)$ en des points à distance au plus ε de α . Et donc

$$B(\omega; r) \setminus N(\alpha) \text{ contient au moins } \frac{r-2\varepsilon}{\rho} \quad \text{2-cellules} .$$

Ainsi on peut remplir D par au moins

$$\frac{\varepsilon}{\rho^2} l(\theta) + \frac{r-2\varepsilon}{\rho} + K \quad \text{2-cellules} .$$

Puisque G satisfait une inégalité isopérimétrique linéaire ; on a

$$\frac{\varepsilon}{\rho^2} l(\theta) + \frac{r-2\varepsilon}{\rho} + K \leq N \cdot l(\theta) \quad \text{où } K \text{ et } N \text{ sont des constantes} .$$

en prenant $\varepsilon = N\rho^2$

$\frac{r-2\varepsilon}{\rho} + K \leq 0$ et alors r est borné ce qui est contradictoire. Le même argument s'applique aux deux autres cas. ■

IV.4 Quasi-isométries

Définition Deux espaces métriques (X, d_X) et (Y, d_Y) sont dits **quasi-isométriques**, si il existe des applications $f : X \rightarrow Y$, $g : Y \rightarrow X$, et des constantes $\lambda > 0$, et $\varepsilon \geq 0$, tel que :

$$d_Y(f(x), f(x')) \leq \lambda d_X(x, x') + \varepsilon \quad \forall x, x' \in X$$

$$d_X(g(y), g(y')) \leq \lambda d_Y(y, y') + \varepsilon \quad \forall y, y' \in Y$$

$$d_X(g \circ f(x), x) \leq \varepsilon \quad \forall x \in X$$

$$d_Y(f \circ g(y), y) \leq \varepsilon \quad \forall y \in Y$$

Proposition IV.3.1 : Etre quasi-isométrique est une relation d'équivalence sur les espaces métriques.

Démonstration : Il est clair que c'est une relation symétrique. De plus la relation est transitive, il suffit de considérer pour

un espace métrique X , $f = g = \text{Id}_X$, $\lambda = 1$, et $\varepsilon = 0$. Il nous reste à démontrer la transitivité.

Considérons trois espaces métriques (X, d_X) , (Y, d_Y) , (Z, d_Z) , où X et Y sont quasi-isométriques, avec $f : X \rightarrow Y$, $g : Y \rightarrow X$, et les constantes λ_1 et ε_1 ; et Y et Z sont quasi-isométriques, avec $h : Y \rightarrow Z$, $j : Z \rightarrow Y$, et les constantes λ_2 et ε_2 . Considérons alors $h \circ f : X \rightarrow Z$, et $g \circ j : Z \rightarrow X$. On a :

$$\begin{aligned} d_Z(h \circ f(x), h \circ f(x')) &\leq \lambda_2 d_Y(f(x), f(x')) + \varepsilon_2 \\ &\leq \lambda_2 \lambda_1 d_X(x, x') + \lambda_2 \varepsilon_1 + \varepsilon_2 \quad \forall x, x' \in X \end{aligned}$$

Ainsi que :

$$d_X(g \circ j(z), g \circ j(z')) \leq \lambda_1 \lambda_2 d_Z(z, z') + \lambda_1 \varepsilon_2 + \varepsilon_1 \quad \forall z, z' \in Z$$

Remarquons que :

$$d_Y(j \circ h \circ f(x), f(x)) \leq \varepsilon_2$$

Et donc :

$$\begin{aligned} d_X((g \circ j) \circ (h \circ f)(x), x) &\leq d_X(g \circ j \circ h \circ f(x), g \circ f(x)) + d_X(g \circ f(x), x) \\ &\leq \lambda_1 d_Y(j \circ h \circ f(x), f(x)) + \varepsilon_1 + \varepsilon_1 \\ &\leq \lambda_1 \varepsilon_2 + 2 \varepsilon_1 \end{aligned}$$

et de même :

$$d_Z((h \circ f) \circ (g \circ j)(x), x) \leq \lambda_2 \varepsilon_1 + 2 \varepsilon_2$$

Il suffit donc de prendre $\varepsilon = \max \{ \lambda_1 \varepsilon_2 + 2 \varepsilon_1, \lambda_2 \varepsilon_1 + 2 \varepsilon_2 \}$, et $\lambda = \lambda_1 \lambda_2$. ■

Proposition IV.3.2 : Si S et S' sont deux systèmes finis de générateurs d'un groupe G , alors (G, S) et (G, S') sont quasi-isométriques.

Remarque Il en est donc de même de leur graphe de Cayley.

Démonstration : Considérons $S = \langle u_i, i \in I \rangle$ et $S' = \langle v_j, j \in J \rangle$. Pour chaque élément u_k , on note $u_k(v)$ une écriture de \bar{u}_k sur S' . $\langle u_i(v), i \in I \rangle$ est un ensemble fini, on note $\lambda_1 = \max \text{lgr}_{S'}(u_i(v))$. Considérons un mot ω sur S_1 , et le mot ω' de S_2 obtenu en remplaçant dans ω les lettres u_i , par les mots $u_i(v)$. Il est clair que $\bar{\omega} = \bar{\omega}'$, et que $\text{lgr}_{S'}(\omega') \leq \lambda_1 \text{lgr}_S(\omega)$, et donc pour des éléments $g_1, g_2 \in G$, $d_{S'}(g_1, g_2) \leq \lambda_1 d_S(g_1, g_2)$. De la même façon

on peut trouver une constante λ_2 tel que $d_S(g_1, g_2) \leq \lambda_2 d_{S'}(g_1, g_2)$, et alors en prenant $f = g = \text{Id}_G$, $\lambda = \max(\lambda_1, \lambda_2)$, et $\varepsilon = 0$, on a vérifié les relations voulues. ■

Lemme IV.3.1 : Si Γ_X et Γ_Y sont quasi-isométriques, avec $(f, g, \lambda, \varepsilon)$ et Y est fini, alors

(i) L'image d'un lacet ω de longueur n est un lacet $f(\omega)$ de longueur au plus $(\lambda + \varepsilon)n$.

(ii) Il existe une fonction $A : \mathbb{N} \rightarrow \mathbb{N}$, tel que Si ω se décompose en N petits lacets de longueur au plus L , $f(\omega)$ a une décomposition en moins de $N A(L)$ petits lacets.

Démonstration : Si $\omega = (g_0, \dots, g_n)$ est un lacet de Γ_X (i.e. $g_0 = g_n$), alors $f(\omega) = (f(g_0), \dots, f(g_n))$ est un lacet de Γ_Y et puisque $d(f(g_i), f(g_{i+1})) \leq \lambda \times 1 + \varepsilon$, $f(\omega)$ a une longueur au plus $n(\lambda + \varepsilon)$.

Si ω se décompose en N petits lacets de longueur au plus L , alors l'image de ces lacets par f constitue une décomposition de $f(\omega)$ en au plus N lacets, de longueur au plus $(\lambda + \varepsilon)L$. Or Y est fini, et donc il existe un nombre fini de lacets (à translation près) de longueur au plus $(\lambda + \varepsilon)L$. Chacun des lacets admet une décomposition en petits lacets. Soit $A(L)$, Le nombre maximum de petits lacets nécessaire à la décomposition d'un lacet de longueur au plus $(\lambda + \varepsilon)L$. Alors $f(\omega)$ se décompose en moins de $N A(L)$ petits lacets. ■

Proposition IV.3.3 : Soient $G = \langle X \mid R \rangle$ et $H = \langle Y \mid S \rangle$ des présentations finies de groupe. Si $\Gamma_X(G)$ et $\Gamma_Y(H)$ sont quasi-isométriques, alors si \mathcal{D}_G est une fonction de Dehn pour $\langle X \mid R \rangle$; il existe des constantes A, B , et C tel que $\mathcal{D}_H = A \mathcal{D}_G(B \text{Id}) + C \text{Id}$, est une fonction de Dehn pour $\langle Y \mid S \rangle$.

Démonstration : Puisque G est f.p., remarquons que la longueur des petits lacets de $\Gamma_X(G)$ est bornée.

Soit ω un lacet fermé de $\Gamma_Y(H)$. Alors $f(\omega)$ est un lacet fermé de $\Gamma_X(G)$, de longueur au plus $(\lambda + \varepsilon) \text{lgr}(\omega)$ (lemme IV.3.1) et $f(\omega)$ se décompose en moins de $\mathcal{D}_G(B \text{lgr}(\omega))$ petits lacets étiquetés

dans R ($B = \lambda + \varepsilon$). On considère $g \circ f(\omega)$. c'est un lacet fermé contenu dans un C -voisinage de ω . De plus $g \circ f(\omega)$ se décompose en moins de $A \mathcal{D}_G(B \text{ lgr}(\omega))$ petits lacets. ω et $g \circ f(\omega)$ bordent un anneau. Si $\omega = (\omega_1, \dots, \omega_n)$, on décompose l'anneau par les lacets fermés $(\omega_i, \omega_{i+1}, g \circ f(\omega_{i+1}), g \circ f(\omega_i), \omega_i)$. On a alors au plus $\text{lgr}(\omega)$ lacets de longueur au plus $1 + 3\varepsilon + \lambda(\lambda + \varepsilon)$. Ces lacets étant de longueur borné, il existe C tel que chacun se décompose en moins de C petits lacets. Alors ω se décompose en moins de $A \mathcal{D}_G(B \text{ lgr}(\omega)) + C \text{ lgr}(\omega)$, petits lacets ■

Ainsi avoir une inégalité isopérimétrique linéaire (resp^t quadratique, exponentielle) ne dépend pas de la présentation. Ainsi avec les résultats du paragraphe précédent, avoir un algorithme de Dehn, être hyperbolique, est indépendant de la présentation f.e. choisie.

CHAPITRE V :

INSOLUBILITE EN TOPOLOGIE

Etant donnée une présentation finie $\Pi = \langle S / R \rangle$, on dispose d'une construction standard pour construire un 2-complexe abstrait ayant pour groupe fondamental $gp(\Pi)$. Ce complexe est constituée d'une 0 cellule, d'une 1 cellule pour chaque générateur et d'un disque pour chaque relateur. On identifie le bord des 1-cellules avec la 0-cellule de façon à former un bouquet. Chaque 1 cellule (orientée) est alors étiquetée par un générateur. Etant donné un relateur R on identifie un lacet fermé ayant pour label sur son bord R ; avec le bord d'un disque. D'après le théorème de Seifert Van-Kampen le 2 complexe ainsi construit a pour groupe fondamental $gp(\Pi)$, on le note $SC(\Pi)$. Il admet une réalisation géométrique dans \mathbb{R}^5 . On peut alors prendre dans \mathbb{R}^5 un ε -voisinage. Pour ε suffisamment petit; on construit ainsi une 5 variété topologique homéomorphe à $SC(\Pi) \times [1;1]$ que l'on note $M_\varepsilon(\Pi)$. $\pi_1(M_\varepsilon(\Pi)) \cong \pi_1(SC(\Pi)) \times \pi_1([1;1]) \cong \pi_1(SC(\Pi))$. C'est une variété à bord, et l'on peut montrer que son bord est une variété topologique fermée ayant pour groupe fondamental $gp(\Pi)$. Ainsi pour tout problème de décision insoluble dans la classe des groupes f.p., il existe un complexe simplicial fini de dimension 2; une 4-variété; et une 5-variété; ayant un groupe fondamental pour lequel le problème est insoluble.

Nous allons utiliser l'insolubilité du problème de l'isomorphisme pour établir une classe de variétés de dimension 5 et une classe de variétés fermées de dimension 4 ayant un problème de l'homéomorphisme insoluble. Nous considérons la classe des groupes finiment présentés, et construisons comme indiqué précédemment une classe de 5 variété, ou pour tout élément on a: $\pi_1(M_\varepsilon(\Pi)) \cong gp(\Pi)$, et de même la classe de variété fermé de dimension 4, qui sont les bords des $M_\varepsilon(\Pi)$. Une variété d'une telle classe, peut alors se donner explicitement par Π . Pour obtenir le résultat escompté il suffirait d'avoir:

$M_{\mathcal{E}}(\Pi)$ est homéomorphe à $M_{\mathcal{E}}(\Pi')$ ssi $gp(\Pi) \cong gp(\Pi')$.

Malheureusement deux variétés peuvent avoir même groupe fondamental sans être isomorphes. Ainsi, si l'on considère $S(\Pi)$ et Π' une autre présentation de Π obtenu en ajoutant à la présentation de Π , le relateur trivial (le mot vide), $\Pi' \cong \Pi$, mais $S(\Pi)$ et $S(\Pi')$ ne sont pas homéomorphes ; En effet nous avons incrémenté le 3ème nombre de Betti de 1. Markov contourne ce problème en remarquant, que dans les changements de Tietze seul l'adjonction de relateurs triviaux (T_1) change la classe d'homéomorphisme de $M_{\mathcal{E}}(\Pi)$.

Dans la suite nous noterons $\Pi * n$, la présentation obtenue à partir de celle de Π , en ajoutant n relateurs triviaux.

Définition : On considère une présentation $\langle a_1, \dots, a_m / r_1, \dots, r_n \rangle$. On appelle transformations spéciales de Tietze, les opérations suivantes :

T_2 : ajouter à la présentation le générateur a_{m+1} et le relateur

$$a_{n+1} = w(a_1, \dots, a_m)$$

T_{11} : remplacer r_i par $a_j a_j^{-1} r_i$ ou $a_j^{-1} a_j r_i$.

T_{12} : remplacer $r_i = uvw$ par vwu (conjugaison cyclique).

T_{13} : Remplacer r_i par r_i^{-1} .

T_{14} : remplacer r_i par $r_i r_j$ où $j \neq i$.

Ainsi que toutes les transformations inverses.

Il est clair que si une présentation Π' est obtenue à partir d'une présentation Π par une suite de transformations spéciales de Tietze ; alors $gp(\Pi) \cong gp(\Pi')$.

Lemme V.1 : Si $\Pi = \langle a_1, \dots, a_m / r_1, \dots, r_n \rangle$ et $\Pi' = \langle a_1, \dots, a_m / r_1, \dots, r_n ; s \rangle$ ou s est une conséquence de r_1, \dots, r_n , alors $\Pi * 2$ peut être transformé en $\Pi' * 1$ par une suite finie de transformations spéciales de Tietze.

Démonstration : Prenons $s = p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} \dots p_k r_{j_k}^{\varepsilon_k} p_k^{-1}$.

On applique à Π une suite de transformations spéciales de Tietze :

$$\begin{array}{ll}
r_1, \dots, r_n, 1, 1 & \\
\dots\dots\dots, 1, r_{j_1} & (T_{14}) \\
\dots\dots\dots, 1, r_{j_1}^{\varepsilon_1} & (\text{éventuellement}) (T_{13}) \\
\dots\dots\dots, 1, a_1^{-1} a_1 r_{j_1}^{\varepsilon_1} & (T_{11}) \\
\dots\dots\dots, 1, a_1 r_{j_1}^{\varepsilon_1} a_1^{-1} & (T_{12}) \\
\vdots & \\
\vdots & \text{puis successivement .} \\
\vdots & \\
\dots\dots\dots, 1, p_1 r_1^{\varepsilon_1} p_1^{-1} & \\
\dots\dots\dots p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} ; p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} & (T_{14}) \\
\dots\dots\dots p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} ; 1 & (T_{13}) \text{ et } (T_{14}) \text{ et } (T_{11}) \text{ plusieurs fois}
\end{array}$$

On effectue alors le même procédé

$$\begin{array}{ll}
\dots\dots\dots p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} ; p_2 r_{j_2}^{\varepsilon_2} p_2^{-1} & \\
\dots\dots\dots p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} p_2 r_{j_2}^{\varepsilon_2} p_2^{-1} ; p_2 r_{j_2}^{\varepsilon_2} p_2^{-1} & (T_{14}) \\
\dots\dots\dots p_1 r_{j_1}^{\varepsilon_1} p_1^{-1} p_2 r_{j_2}^{\varepsilon_2} p_2^{-1} ; 1 & (T_{13}) (T_{14}) \text{ et } (T_{11}) \text{ plusieurs fois} \\
\vdots & \\
\vdots & \\
\vdots & \\
\dots\dots\dots s ; 1 & \blacksquare
\end{array}$$

Lemme V.2 : si $\Pi = \langle a_1 \dots a_m ; r_1 \dots r_n \rangle$ et $\Pi' = \langle a'_1 \dots a'_m ; r'_1 \dots r'_n \rangle$
sont tels que $\text{gp}(\Pi) \cong \text{gp}(\Pi')$
alors $\Pi * (n + n' + 1)$ se transforme en $\Pi' * (n + n' + 1)$
par une suite finie de transformations spéciales de Tietze

Démonstration : On note α_i l'écriture de a_i sur les générateurs $a'_1 \dots a'_m$. On note α'_i l'écriture de a'_i sur les générateurs $a_1 \dots a_m$. On note $r_j(\alpha_i)$ le mot obtenu à partir de r_j en remplaçant les occurrences de a_i par α_i . (et de même on note $r'_j(\alpha'_i)$).

$$a_i / r_j(\alpha_i) * (n + n' + 1)$$

$$a_i / r_j(\alpha_i) ; r'_j(\alpha'_i) * (n + 1) \quad (\text{lemme V.1 appliqué } n' \text{ fois})$$

$a_i, a'_i / r_j(a_i) ; r'_j(a'_i) ; a'_i = \alpha'_i * (n+1) \quad (T_2) \text{ n' fois}$

$a_i, a'_i / r_j(a_i) ; r'_j(a'_i) ; a'_i = \alpha'_i * (n+1) \text{ (lemme V.1 n' fois)}$

$a_i, a'_i / r_j(a_i) ; r'_j(a'_i) ; a'_i = \alpha'_i ; a_i = \alpha_i * 1 \text{ (V.1 n fois)}$

de même on peut changer Π' . En cette même présentation, et donc par symétrie des transformations, $\Pi * (n+n'+1) \longrightarrow \Pi' * (n+n'+1)$

Proposition V.1 : Si Π' est obtenu à partir de Π par une suite de transformations spéciales de Tietze, alors $M_\varepsilon(\Pi')$ est homéomorphe à $M_\varepsilon(\Pi)$.

Démonstration : Les transformations T_{12} (permutation cyclique d'un relateur) et T_{13} (inversion d'un relateur), et leurs inverses ne changent pas $SK(\Pi)$; et donc si Π' est obtenu à partir de Π par une suite de telles transformations ; $M_\varepsilon(\Pi)$ et $M_\varepsilon(\Pi')$ sont homéomorphes. Considérons les transformations T_2 appliquées à Π (ajouter un générateur $a_{m+1} = \omega(a_1; \dots; a_m)$ $SK(\Pi')$ est obtenu en ajoutant à $SK(\Pi)$ un lacet fermé, et un disque dont le bord est identifié avec le lacet. Dans $M_\varepsilon(\Pi')$. Le générateur a_{m+1} ajoute une anse à $M_\varepsilon(\Pi)$. Supposons que le disque rencontre le bord de $M_\varepsilon(\Pi)$ (et alors aussi la anse), en une courbe simple cc' où c est l'intersection du disque avec la anse. Alors $M_\varepsilon(\Pi')$ est formé en attachant un voisinage du disque bordé par cc' . On peut alors contracter ce disque pour écraser la anse sur $M_\varepsilon(\Pi)$ et ainsi $M_\varepsilon(\Pi) \cong M_\varepsilon(\Pi')$.

Considérons la transformation T_{11} (remplacer r_i avec $a_j a_i^{-1} r_i$).

On considère la présentation Π^- qui est la relation Π dans laquelle on a retiré le relateur r_i .

Alors $SK(\Pi)$ est obtenu à partir de $SK(\Pi^-)$ en identifiant le bord d'un disque avec le lacet de label r_i ; alors que $SK(\Pi')$ est obtenu en identifiant sur le bord d'un disque sur le lacet de label $a_j a_i^{-1} r_i$. Ces disques coupent la bord de $M_\varepsilon(\Pi^-)$ en une courbe simple (car les disques sont identiques uniquement sur leur bords) ; respectivement d et d' . Ils sont très proches sauf en $a_i a_i^{-1}$ qui est une courbe simple. Mais si l'on considère un voisinage de ces disques, on peut alors glisser d' ; dans ce voisinage, pour arriver à d et donc $M_\varepsilon(\Pi)$ et $M_\varepsilon(\Pi')$ sont homéomorphes.

Considérons la transformation T_{14} (remplacer r_i par $r_i r_j$). $M_\varepsilon(\Pi')$ est obtenu à partir de $M_\varepsilon(\Pi)$ en prenant un voisinage d'un disque ayant pour bord d' de label $r_i r_j$ et $M_\varepsilon(\Pi)$ est obtenu en prenant le voisinage d'un disque ayant pour bord d . Mais puisque r_j est le label du bord d'un disque ; on peut glisser d' sur ce disque pour obtenir d . ■

Le résultat est alors immédiat .

Théorème V.1 : Le problème de l'homéomorphisme est insoluble pour les variétés de dimension 4 et 5 . Il existe une classe de variétés fermées de dimension 4 , ainsi qu'une classe de variétés de dimension 5 , données de façon explicites pour lesquelles , on ne peut décider si deux variétés données sont homéomorphes .

Dans [18] , Haken , Boone et Poénaru , utilisent une construction améliorée , pour démontrer que pour tout degré D , et pour tout $n \geq 4$, il existe une classe récursive de présentations de variétés de dimension n , pour laquelle le problème de l'homéomorphisme de l'équivalence combinatoire , du difféomorphisme sont de degré D . La difficulté provient essentiellement de l'établissement de présentation de variétés , c'est à dire d'une suite de de symboles , établissant les structures combinatoires topologiques et différentielles d'une variété .

Bibliographie

- [1] *S. Aanderaa* ,A proof of Higman's embedding theorem using Britton extension of groups .dans Word problem
- [2] *G. Baumslag, S. M. Gersten, M. Shapiro, H. Short* ,Automatic groups and amalgams .jour. of pure and applied algebra
- [3] *W. W. Boone* ,The word problem .Ann. of math. 70 (1959)
- [4] *W. W. Boone* ,Word problems and recursively enumerable degrees of unsolvability .A first paper on Thue system Ann. of Math. 83 (1966)
- [5] *W. W. Boone* ,Word problems and recursively enumerable degrees of unsolvability .A sequel on finitely presented groups .Ann. of Math. ,84 (1966)
- [6] *W. W. Boone* ,Decision problems about algebraic and logical systems as a whole and recursively enumerable degrees of unsolvability .Contribution to Math. logic, K. Schutte éditeur .
- [7] *W. W. Boone, H. Rogers jr.* On a problem of JHC Whitehead and a problem of Alonzo Church .Math. scand.19 (1966)
- [8] *J. L. Britton* ,The word problem .Ann. of Math. ,77 (1963)
- [9] *Coornaert, Delzant, Popadopoulos* ,Géométrie et théorie des groupes .Springer Verlag 1441
- [10] *M. Dehn* ,Lectures on surface topology .dans M. Dehn papers on group theory and topology
- [11] *M. Dehn* ,On infinite discontinuous groups ,même ouvrage
- [12] *S. M. Gersten, H. Short* ,small cancellation theory and

automatic groups

- [13] *E. Ghys, P. de la Harpe* éditeurs .Sur les groupes hyperboliques d'après Michael Gromov .Birkhäuser
- [14] *M. Greendlinger* ,Dehn's algorithm for the word problem comm.pure and applied Math.
- [15] *M. Greendlinger* ,On dehn's algorithm for the conjugacy and word problem .Comm.pure and appl.Math.13 (1960)
- [16] *M. Gromov* ,Hyperbolic groups dans Essays in group theory S.M.Gersten éditeur .Springer Verlag
- [17] *W. Haken* ,Connections between topological and groups theoritical decision problem dans Word problem .Boone Cannonito ,Lyndon éditeurs
- [18] *W. Haken, W.W. Boone, V. Poénaru* ,on recursively unsolvable problems in topology and their classification . Contribution to Math.Logic .K.Schutte éditeur
- [19] *P. Hall* ,Finiteness condition for soluble groups .Proc. London Math. Soc. 3 (1954)
- [20] *G. Higman* ,Subgroups of finitely presented groups .Proc. of Royal soc. 262 (1961)
- [21] *R.C. Lyndon, P.E. Schupp* ,Combinatorial group theory Springer (1977)
- [22] *R.C. Lyndon* ,On Dehn's algorithm .Math. Annalen 166 (1966)
- [23] *Magnus, Karass, Solitar* ,combinatorial group theory Wiley N.Y. (1966)
- [24] *A. A. Markov*,unsolvability of the problem homeomorphy Proc.Int.Conj.Math. (1958)

- [25] *K. A. Mihailova* ,the occurence problem for direct products of groups
- [26] *C.F. Miller III* ,Decision problem for groups .Survey and reflections .preprint
- [27] *C.F. Miller III* ,Some notes on geometry and complexity preprint
- [28] *C.F. Miller III* ,On group theoretic decision problems and classification .Annals of Math. studies Princeton
- [29] *C.F. Miller III* ,Decision problems in algebraic class of groups dans Word Problem
- [30] *J. Nielsen* ,A basis for subgroups of free groups .Math. scand. 3
- [31] *P. S. Novikov* ,Unsolvability of the conjugacy problems in the théorie of groups
- [32] *P. S. Novikov* ,On the algorithmic unsolvability of the word problem in groups
- [33] *M. D. Rabin* ,Recursive unsolvability of group theoretic decision problems .Ann. of Math. 67 (1958)
- [34] *H. Rogers. jr.* ,The theory of recursive fonctions and effective computability .Mc. Graw. Hill (1967)
- [35] *J. J. Rotman* ,Theory of groups (ver. 2) .Allyn & Bacon
- [36] *I. N. Sanov* ,A property of a certain representation of a free group .Doklady Akad. Nauk.
- [37] *J. J. Stillwell* ,Classical topology & combinatorial group theory .Springer Verlag