N° d'ordre :02 /2007-M/MT

RÉPUBLIQUE ALGÉRIÈNNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENNE

FACULTÉ DES MATHÉMATIQUES

MÉMOIRE présenté pour l'obtention du diplôme de MAGISTER
En MATHÉMATIQUES

Spécialité : Analyse complexe

Par

DEGAICHI Nouar

THÈME

ETUDE DU GROUPE DES TRESSES

Soutenu publiquement, le 08/02/2007 devant le jury composé de :

Mr.	**R. BEBBOUCHI**	Professeur	U.S.T.H.B.	Président.
Mr.	**A. AROUCHE**	Maître de Conférences	U.S.T.H.B.	Directeur de thèse.
Mr.	**K. BETINA**	Professeur	U.S.T.H.B.	Examinateur.
Mr.	**M.S. HACHAICHI**	Maître de Conférences	U.S.T.H.B.	Examinateur.
Mr.	**M.S. REZAOUI**	Maître de Conférences	U.S.T.H.B.	Examinateur.

Remerciements

Je tiens en premier lieu à exprimer mes plus vifs remerciements à Monsieur ***A. AROUCHE*** *mon Directeur de thèse pour l'intéressant sujet qu'il m'a proposé. Je lui suis également reconnaissant pour la confiance qu'il ma accordée. Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes.*

J'exprime ici ma profonde gratitude à Monsieur ***R. BEBBOUCHI*** *Professeur à l'U.S.T.H.B pour m'avoir fait l'honneur de présider mon jury de thèse.*

Je remercie vivement Messieurs ***K. BETINA*** *Professeur à l'U.S.T.H.B ,* **M.S. HACHAICHI** *Maître de Conférences à l'U.S.T.H.B et* ***M.S. REZAOUI*** *Maître de Conférences à l'U.S.T.H.B qui ont bien voulu faire partie du jury.*

Pour finir mes derniers mots de remerciements vont tout naturellement à ma famille et mes amis, en particulier mes parents et mon frère ***RACHID*** *pour leur soutien tout au long de mes études.*

Etude du groupe des tresses

Résumé

Nous nous intéressons ici à l'étude du groupe de tresses. Le but poursuivi est de traiter la pluspart des propriétés de ces groupes, l'élément centralisateur de ce groupe et le groupe de tresses pure, ensuite nous donnons les solutions de deux problèmes algorithmiques essentiels dans le groupe de tresses qui sont respectivement le problème du mot et le problème de conjugaison, ensuite on démontre que le groupe de tresses possède un ordre dont nous donnons certaines constructions.

Enfin on va montrer que le groupe de tresses fournit un cadre adapté à la cryptographie.

Mots-clés : Groupes des tresses, groupes des tresses pures, problème du mot, problème de conjugaison, ensemble summit, système autodistributif, réduction de poignée, diagramme de courbe, cryptographie basée sur les tresses.

Table des matières

Liste des Figures

Introduction

Avec l'avènement des technologies numériques qui contrairement aux technologies analogiques nous cantonnent au monde du dénombrable, l'étude des structures mathématiques discrètes revêt une importance considérable et l'informatique en est à la fois une application directe et un moyen d'étude privilégié.

On peut distinguer deux grandes catégories de structures discrètes, d'une part les structures commutatives telles celles étudiées en théorie des nombres et d'autre part les structures non commutatives; les groupes de tresses font partie de cette seconde catégorie et ont fait l'objet de nombreux travaux depuis leur introduction en 1925 par E. Artin.

L'objectif de cette thèse est l'étude des propriétés algorithmiques et structurelles des groupes de tresses, ainsi que leur application à la cryptographie. Plusieurs années après l'introduction des groupes de tresses par E. Artin, des extensions naturelles de ces groupes sont apparues en 1966; J. Tits introduit ce qu'il appelle groupes de tresses généralisées et que nous désignerons par groupes d'Artin-Tits.

Peu après, apparaît des travaux fondamentaux sur les groupes de tresses et les groupes d'Artin-Tits, notamment par Garside en 1969 qui a donné une autre démonstration du problème du mot, il a aussi donné une solution pour le problème de conjugaison qu'on renconrera au chapitre 2 et en 1972 par P.Deligne et autres mathématiciens.

Dans ces travaux sont mises en évidences des propriétés fondamentales de finitude et de divisibilité qui donnent au groupes de tresses et à certains groupes d'Artin-Tits leur structure particulière. Mentionnons enfin la découverte un peu plus tardive, fin 1991, de l'ordonnabilité des groupes de tresses par Dehornoy.

Aujourd'hui, la recherche dans le domaine des groupes de tresses et leurs extensions est active, et porte à la fois sur les aspects algébriques combinatoires, géométriques et topologiques. Récemment de nombreuses passerelles ont été jetées entre ces aspects, avec par exemple la définition des monoïdes de tresses duaux.

Notre travail est consacré essentiellement aux propriétés algébriques, algorithmiques, combinatoires et géométriques des groupes de tresses.

Ce manuscrit est structuré de la manière suivante:

Dans le premier chapitre, nous introduisons le groupe des tresses en définissant les propriétés essentielles telles que la présentation du groupe de tresses, groupe de tresses pures, groupe dérivé, élément de Garside ...etc.

Le deuxième chapitre est consacré à l'étude de deux problèmes algorithmiques spécifiques au goupe des tresses, à savoir le problème du mot et le problème de conjugaison.
Concernant le premier problème on va utiliser la méthode de E Artin [3] appelée tresses peignées, Par contre dans le deuxième problème on utilise la technique de F Garside **[15]** qui est basée sur l'élément

$$\Delta_n = (\sigma_1\sigma_2...\sigma_{n-1})\,(\sigma_1\sigma_2...\sigma_{n-2})\,...\,(\sigma_1\sigma_2)\,(\sigma_1)$$

Dans le troisième chapitre, nous présentons:
- Le caractère ordonnable du groupe des tresses étudié par P Dehornoy **[7].**
- Les différentes méthodes basées sur les systèmes autodistributifs, la méthode de la réduction de poignée et la méthode des diagrammes des courbes qui ont été proposées par d'autres mathématiciens [11] en démontrant deux propriétées essentielles la propriété d'acyclicité et la propriété de comparaison. Avec ces deux propriétés nous pouvons alors définir un ordre total invariant par multiplication à gauche sur le groupe des tresses qui coincide avec l'ordre de Dehornoy.

Dans le quatrième chapitre, on étudie la cryptographie basée sur les tresses en commençant par des problèmes difficiles dans ce groupe, puis on va utiliser le cryptosystème de Ko et al [18].

En fin dans le dernier chapitre on achève ce travail par une conclusion.

1

Généralités sur les groupes des tresses

L'objectif de ce chapitre est de donner des généralités du groupe des tresses qui a été introduit explicitement en 1925 par E. Artin.

D'abord nous donnons les définitions des tresses, les tresses équivalentes, la projection d'une tresse, l'invariant des tresses et les tresses pures.

Définition 1.0.1 *Soit D le cube unité:*

$$D=\left\{(x,y,z)\in\mathbb{R}^3/\ 0\leq x,y,z\leq 1\right\}$$

Sur la face supérieure du D , on place n points $A_1, A_2, ..., A_n$ et sur la face inférieure du même cube on place les n points $B_1, B_2, ..., B_n$.(figure (1.0.1))On pose

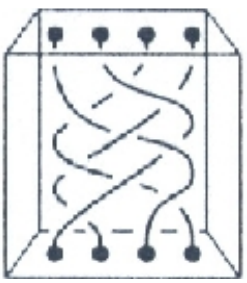

Figure 1.0.1 : Tresse à 4 brins

$A_1=\left(\frac{1}{2},\frac{1}{n+1},1\right),...,A_n=\left(\frac{1}{2},\frac{n}{n+1},1\right)$
$B_1=\left(\frac{1}{2},\frac{1}{n+1},0\right),...,B_n=\left(\frac{1}{2},\frac{n}{n+1},0\right)$
On joint les points A_i avec les points B_j.par des courbes $d_1, d_2, ..., d_n$. Les courbes d_i sont telles que les trois conditions sont satisfaites:

1- $d_1, d_2, ..., d_n$ sont disjointes.
2- Pour $i, j, k \in \{1, 2, ..., n\}$ chaque d_i relie un A_j avec un B_k tel que j, k égaux ou différents , mais d_i ne joint jamais A_j avec A_k ou B_j avec B_k.
3- chaque plan E_s d'équation $(z = s$ tel que $0 \leq s \leq 1)$ parallèle avec le plan (xy) intersecte d_i en un seul point pour $i = 1, 2, ..., n$.
Une telle configuration des n arcs $d_1, d_2, ..., d_n$ est appelée tresse à n brins.

Notation 1.0.1 *On note l'ensemble des n tresses par $\boldsymbol{B}_n$.*

1.0.1 Mouvement élémentaire et tresses équivalentes

Définition 1.0.2 *1- Si on remplace le brin AB par $AC \cup CB$ tels que A, B et C trois points dans le cube unité on note cette opération par Ω.*
2- Si on remplace $AC \cup CB$ par le brin AB
on note cette opération par Ω^{-1}, un mouvement élémentaire sur les tresses est l'une des deux opérations définies au-dessus.(voir figure (1.0.2))

Figure 1.0.2 : Mouvement élémentaire sur les tresses

1.0.2 Tresses équivalentes

Définition 1.0.3 *Une n tresse β et dite équivalente à une n tresse β' si on peut transformer β à β' par une suite finie de mouvements élémentaires à l'intérieur de D. Autrement dit β est équivalente à β' s'il existe une suite finie $\beta = \beta_0 \xrightarrow{\Omega^{\pm 1}} ... \xrightarrow{\Omega^{\pm 1}} \beta_m = \beta'$ pour $i = 1, 2, ..., m$, et la n tresse β_i est obtenue à partir de β_{i-1} par application de l'une des opérations Ω ou Ω^{-1}.*
Dans le cas contraire, on dit que β est non équivalente à β'

1.0.3 Projection d'une tresse

Définition 1.0.4 *Soit P l'application définie par: $P : D \to \mathbb{R}^3$ telle que*

$$P(x, y, z) = (0, y, z)$$

L'éffet de P sur la tresse β est d'afficher l'ensemble des n courbes $d_1, d_2, ..., d_n$ sur le plan (yz) (voir figure (1.0.3)).

Figure 1.0.3 : Projection d'une tresse

Notation 1.0.2 *On note $\widehat{\beta}$ l'image de β par P.*

Pour $i \in \{1, 2, ..., n\}$ soit $\widehat{d_i}$ l'image de la courbe d_i par P et on suppose que $\widehat{d_i}$ satisfait les trois conditions suivantes:

1-$\widehat{\beta}$ a un nombre fini de points d'intersection.

2-Si Q est un point d'intersection de $\widehat{\beta}$ alors $P^{-1}(Q) \cap \beta$ a deux points d'intersection.

3-L'image d'un sommet de β n'est jamais un point double de $\widehat{\beta}$.

Définition 1.0.5 *Une projection $\widehat{\beta}$ qui satisfait les conditions au-dessus est dite projection régulière de β.*

Maintenant, soit β une tresse et $\widehat{\beta}$ sa projection régulière

$\widehat{\beta}$ représente la tresse β sauf au point d'intersection, donc on ne peut pas distinguer entre deux brins lequel passe sur (sous) l'autre.

Pour cela en coupe un petit morceau au voisinage du point double dans les deux côtés et dans ce cas la projection régulière est dite diagramme régulier.

1.0.4 Tresses de permutations et tresses pures

Définition 1.0.6 *On definit l'application* $f : \mathcal{B}_n \to \Sigma_n$ *par:*

$f\ (\beta) = \left({}^{1\ \ 2\ \ n}_{j(1)...j(2)\ \ j(n)} \right)$
telle que Σ_n est le groupe des permutations.

Définition 1.0.7 *Soient* $\beta\ ,\ \beta' \in \mathcal{B}_n$ *telles que* β *est equivalente à* β' *alors pour chaque* $i = 1, 2, ..., n$ *les brins* d_i *et* d_i' *ont le même point final, donc ils ont la même permutation. Cette permutation est appelée permutation des tresses et q'on note* $\pi(\beta)$.
Une tresse $\beta \in \mathcal{B}_n$ *est dite tresse pure si la tresse de permutation* $\pi(\beta)$ *est triviale.*

Le produit $\beta_1\beta_2$ de deux tresses β_1 et β_2 est obtenu en joignant les extrémités inférieures des brins de β_1 aux extrémités supérieures de β_2 (voir figure (1.0.4))

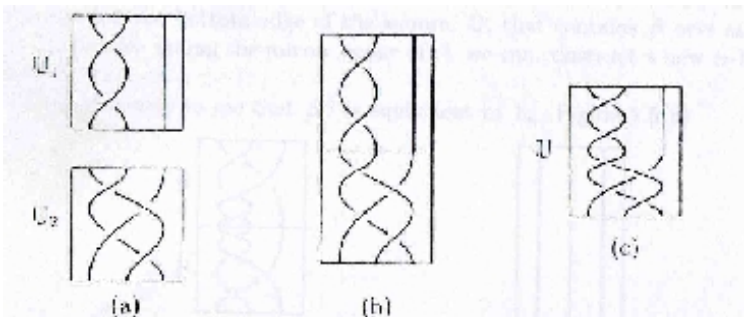

Figure 1.0.4 : Le produit de deux tresses

La relation d'equivalence définie précédemment nous permet de définir une structure de groupe sur les tresses, en effet soit $[\beta]$ la classe de β alors: $[\beta_1\beta_2]$ est bien définie car $[\beta_1\beta_2] = [\beta_1]\,[\beta_2]$.

L'ensemble des classes d'equivalence forme un groupe qu'on note $\mathcal{B}_n$, il est rengendré par $(n-1)$ générateurs $\sigma_1, ..., \sigma_{n-1}$

1.0.5 Présentation du groupe des tresses

Définition 1.0.8 *Un mot de tresses* w *est un élément de* $\mathcal{B}_n$ *, il s'écrit en fonction des éléments de* $\mathcal{B}_n^+$ *et de* $\mathcal{B}_n^-$ *tels que* $\mathcal{B}_n^+ = \{\sigma_1, ..., \sigma_{n-1}\}$ *avec des puissances positives et* $\mathcal{B}_n^- = \left\{\sigma_1^{-1}, ..., \sigma_{n-1}^{-1}\right\}$ *avec des puissances négatives*

Tout élément $\beta \in \mathcal{B}_n$ s'écrit

$$\beta = \sigma_{i_1}^{\varepsilon_1}\sigma_{i_2}^{\varepsilon_2}...\sigma_{i_k}^{\varepsilon_k}$$

avec $i = 1, 2, ..., n-1$
$\varepsilon_i = \pm 1$ pour $i = 1, 2, ..., k$
et $1 \leq i_1, i_2, ..., i_k \leq n-1$.

Définition 1.0.9 *Pour tout $n \geq 1$ le groupe des tresses $\mathcal{B}_n$ a la présentation suivante*

$$\mathcal{B}_n = \langle \sigma_1, \sigma_2...\sigma_{_{n-1}} / \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ si } |i-j| = 1 \text{ et } \sigma_i\sigma_j = \sigma_j\sigma_i \text{ si } |i-j| > 1 \rangle$$

1.1 Propriétés élémentaires du groupe des tresses

Proposition 1.1.1 *Soit $\Delta_n = (\sigma_1\sigma_2...\sigma_{n-1})^n$ et pour $1 \leq i \leq n-1$*

$$\Delta_n\sigma_i = (\sigma_1\sigma_2...\sigma_{n-1})^n\,\sigma_i = \sigma_i\Delta_n$$

Pour tout $1 \leq m \leq n$ l'application $\mathcal{X} : \mathcal{B}_m \longrightarrow \mathcal{B}_n$ définie par:
$\mathcal{X}(\sigma_i) = \sigma_i$ pour $i = 1, 2, ..., m-1$ est un morphisme de $\mathcal{B}_m$ à $\mathcal{B}_n$, de plus $\mathcal{X}$ est injectif donc $\mathcal{B}_m$ est un sous groupe de $\mathcal{B}_n$.

Preuve. Pour montrer que $\mathcal{X}$ est un morphisme il suffit de montrer que chaque relation pour $\mathcal{B}_m$ est satisfaite aussi pour $\mathcal{B}_n$.
montrons maintenant que $\mathcal{X}$ est injectif.

On suppose que $\mathcal{X}(\beta) = 1_n$ pour un certain $\beta \in \mathcal{B}$ c'est à dire il existe une tresse a m brins β telle que si on ajoute $(n-m)$ segments à β on obtient la tresse triviale qu'on note 1_n.
l'égalité $\mathcal{X}(\beta) = 1_n$ implique qu'il existe une suite finie

$$\mathcal{X}(\beta) = \beta_0 \longrightarrow \beta_1 \longrightarrow ... \longrightarrow \beta_k = 1_n \tag{1.1.1}$$

telle que β_i est une $n-$tresse et β_{i+1} est obtenue à partir de β_i par une application d'un mouvement élémentaire à β_i.
Maintenant si on fait bouger le $(n-m)$ brin final de chacune des β_i à $\widehat{\beta_i}$ donc (1.1.1) induit la suite finie

$$\beta = \widehat{\beta_0} \longrightarrow \widehat{\beta_1} \longrightarrow ... \longrightarrow \widehat{\beta_l} \longrightarrow 1_n$$

telle que l'un des β_{i+1} est obtenue de $\widehat{\beta_i}$ par une application d'un mouvement élémentaire à $\widehat{\beta_i}$ ou $\widehat{\beta_{i+1}}$ s'identifiée avec $\widehat{\beta_i}$.

Ce dernier se présente si un mouvement élémentaire est appliqué à la $l \overset{ème}{=}$ brin de β_i avec $m < l \leq n$ donc $\beta \backsim 1_n$. ■

Définition 1.1.1 *Pour $n \geq 1$: Soit $f : \mathcal{B}_n \longrightarrow \Sigma_n$ le morphisme de groupes defini par:*
$\sigma_i \longmapsto (i, i+1)$
où $\mathcal{B}_n$ est le groupe des tresses et Σ_n est le groupe de permutations
Le noyau de f est appelé groupe des tresses pures qu'on note $\mathcal{P}_n$.

Proposition 1.1.2 *Le groupe des tresses pures $\mathcal{P}_n$ est un sous-groupe normal de $\mathcal{B}_n$. De plus le groupe quotient $\mathcal{B}_n/\mathcal{P}_n$ est isomorphe à Σ_n , le groupe de permutations, et donc*

$$[\mathcal{B}_n : \mathcal{P}_n] = n!$$

Preuve. Montrons tout d'ordre que $\mathcal{P}_n$ est un sous groupe de $\mathcal{B}_n$.

$\mathcal{P}_n$ est constitué de n tresse β telle que $\pi(\beta)$ est la permutation triviale qu'on note (1) et π est un morphisme de groupes.

Soient β_1 β_2 deux n tresses pures et puisque $\pi(\beta_1\beta_2) = \pi(\beta_1).\pi(\beta_2) = (1)$ cela implique que $\beta_1\beta_2$ est une n tresse pure c'est à dire

$$\beta_1\beta_2 \in \mathcal{P}_n$$

De plus si $\beta \in \mathcal{P}_n$ donc $\pi\left(\beta^{-1}\right) = \pi(\beta)^{-1} = (1)$ et cela implique que

$$\beta^{-1} \in \mathcal{P}_n$$

Donc $\mathcal{P}_n$ est un sous groupe de $\mathcal{B}_n$.

Pour démontrer que $\mathcal{P}_n$ est normal dans $\mathcal{B}_n$, on considère $\gamma \in \mathcal{B}_n$ et $\beta \in \mathcal{P}_n$.

$$\begin{aligned} \pi\left(\gamma\beta\gamma^{-1}\right) &= \pi(\gamma)\,\pi(\beta)\,\pi\left(\gamma^{-1}\right) \\ &= \pi(\gamma)\,\pi(\beta)\,\pi(\gamma)^{-1} = 1_n = \pi\left(\gamma\gamma^{-1}\right) \end{aligned}$$

donc $\gamma\beta\gamma^{-1} \in \mathcal{P}_n$ mais $\gamma\beta\gamma^{-1} \in \mathcal{P}_n \Longrightarrow \gamma\mathcal{P}_n \subset \mathcal{P}_n\gamma$ pour tout n tresse $\gamma \in \mathcal{B}_n$ et par suite $\mathcal{P}_n$ est normal dans $\mathcal{B}_n$

Pour démontrer que $\mathcal{B}_n/\mathcal{P}_n \backsimeq \Sigma_n$, on considère l'application $f : \mathcal{B}_n \to \Sigma_n$ qui est induie par la permutation π c'est à dire

$$f\ (\beta) = \pi(\beta)$$

Pour tout $\beta_1, \beta_2 \in \mathcal{B}_n$

$$\begin{aligned} f\ (\beta_1.\beta_2) &= \pi(\beta_1\beta_2) \\ &= \pi(\beta_1)\,\pi(\beta_2) \\ &= f\ (\beta_1)\, f\ (\beta_2) \end{aligned}$$

Donc f est un morphisme de groupes.

On suppose maintenant $\rho \in \Sigma_n$ c'est à dire

$$\rho = \begin{pmatrix} 1 & n \\ i_1 & i_n \end{pmatrix}$$

On construit une n tresse β basée sur ρ commençant par n points $A_1, A_2, ..., A_n$ sur la droite (l_1) et un autre ensemble de n points $B_1, B_2, ..., B_n$ sur la droite (l_2) telle que (l_1) est parallèle à (l_2), on joint les A_j aux B_j, par des segments d_j , et on choisit arbitrairement A_j se croise sous (sur) B_j en chaque point de d_j on peut donc former une n tresse γ telle que $\pi(\gamma) = \rho$ et donc $f\ (\gamma) = \rho$.
Alors f est surjective et le noyau de f est l'ensemble des $n-$tresses pures $\mathcal{P}_n$
et par conséquent $\mathcal{B}_n/\ker f \backsimeq \Sigma_n$

$$\mathcal{B}_n/\mathcal{P}_n \backsimeq \Sigma_n$$

■

Invariants de $\mathcal{B}_n$

Définition 1.1.2 *Soit β une m tresse telle que:*

$$\beta = \sigma_{i_1}^{\varepsilon_1}\sigma_{i_2}^{\varepsilon_2}...\sigma_{i_k}^{\varepsilon_k} \ \textit{avec}\ \varepsilon_i = \pm 1$$

1-L'élément

$$\exp(\beta) = \varepsilon_1 + \varepsilon_2 + ... + \varepsilon_k$$

est appelé exponentielle de β qu'on note $\exp(\beta)$.
2-Si tous les ε_i sont positifs β est dite tresse positive.

Proposition 1.1.3 *Soient $\beta_1, \beta_2 \in \mathcal{B}_n$ deux tresses telles que $\beta_1 \backsim \beta_2$*
Alors

$$\exp(\beta_1) = \exp(\beta_2)$$

Preuve. $\beta_1 \backsim \beta_2 \Longleftrightarrow \exists$ une suite finie

$$\beta_1 = \gamma_0 \longrightarrow \gamma_1 \longrightarrow ... \longrightarrow \gamma_m = \beta_2$$

telle que γ_i sont des mots dans $\sigma_1^{\pm 1}, \sigma_2^{\pm 1}, ..., \sigma_{n-1}^{\pm 1}$ et γ_{i+1} est obtenu à partir de γ_i par l'ajout ou la suppression d'un mot de la forme $\mu R^{\pm 1} \mu^{-1}$ tel que R est l'un des relations de définition du groupe des tresses $\mathcal{B}_n$.

Puisque

$$\exp(R) = 0$$

cela implique $\exp(\gamma_i) = \exp\left(\gamma_{i+1}\right)$ pour $i = 1, 2, ..., m-1$ donc

$$\exp(\beta_1) = \exp(\gamma_0) = ... = \exp(\gamma_m) = \exp(\beta_2)$$

■

Définition 1.1.3 *L'élément* exp *est un invariant pour le groupe des tresses* $\mathcal{B}_n$.

Pour présenter le groupe des tresses pures $\mathcal{P}_n$ par générateurs et relations on a besoin de la méthode suivante.

1.2 Présentation du groupe de tresses pures

Pour trouver une présentation du groupe de tresses pures on a besoin de la méthode suivante:

La méthode de REIDEMEISTER-SCHREIER

Cette méthode nous permet de trouver explicitement la présentation d'un sous-groupe à partir d'une présentation donnée d'un groupe. Pour cela on considère le groupe G qui a la présentation $G =< x_1, x_2, ..., x_n \ / R_1 = 1, R_2 = 1, ..., R_m = 1 >$ et soit H un sous groupe de G.

Pour trouver une présentation de H en termes de générateurs et des relations de G on définit un système complet de représentants des classes à droites $M = \{M_1, M_2, ..., M_n\}$ appelé système de Schreier**.** Soit maintenant $g \in G$, alors la méthode de Reidemeister-Schreier nous permet de trouver les représentants des classes à droite M_j qui représentent Hg

Notation 1.2.1 *On note* $\overline{g}$ *le représentant de la classe à droite* Hg *dans* M

Proposition 1.2.1 *1-pour tout élément $g \in G, M_i \in M$.pour $i = 1, 2, ...$*
$\rho(M_i, g) = M_i g \left(\overline{Mg}\right)^{-1} \in H$ *tel que* $M_i = \sigma_{n-1}\sigma_{n-2}...\sigma_{n-i+1}$
2- pour $j = 1, 2, ..., n$ *et* $k = 1, 2, ..., [G : H]$
On pose $y_{j,k} = \rho(M_k, x_j)$ *alors* H *est engendré par les* $y_{j,k}$ *est ses inverses*

Preuve. 1- puisque $M_i g, \overline{M_i g}$ ont le même représentant des classes à droités de H alors $M_i g \left(\overline{M_i g}\right)^{-1} \in H$
2-$\rho(M_k, x_j) = y_{j,l}^{-1}$ pour un certain l tel que $M_k = \overline{M_l x_j}$
Soit $h \in H$
$h = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}$
$\overline{h} = \overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}}$ on transforme h comme suit $h = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}$
$= \left(1 x_{i_1}^{\epsilon_1} \overline{x_{i_1}^{\epsilon_1}}^{-1}\right)\left(\overline{x_{i_1}^{\epsilon_1}}\, x_{i_2}^{\epsilon_2} \overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}}^{-1}\right) ... \left(\overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_{p-1}}^{\epsilon p-1}}^{-1} x_{i_p}^{\epsilon_p}\right)$
$= \rho\left(1, x_{i_1}^{\epsilon_1}\right) \rho\left(\overline{x_{i_1}^{\epsilon_1}}, x_{i_2}^{\epsilon_2}\right) ...\rho\left(\overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_{p-1}}^{\epsilon p-1}}, x_{i_p}^{\epsilon_p}\right)$
On note cette transformation par τ alors
$\tau\left(x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}...\right) = \rho\left(1, x_{i_1}^{\epsilon_1}\right) \rho\left(\overline{x_{i_1}^{\epsilon_1}}, x_{i_2}^{\epsilon_2}\right) ...\rho\left(\overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_{p-1}}^{\epsilon p-1}}, x_{i_p}^{\epsilon_p}\right) = y_{i_1,\lambda_1}^{\varepsilon_1} y_{i_2,\lambda_2}^{\epsilon_2}...y_{i_p,\lambda_p}^{\epsilon_p}$ alors chaque facteur est $y_{j,k}$ ou bien son inverse ■

Proposition 1.2.2 *Le groupe des tresses pures $\mathcal{P}_n$ a la présentation suivante:*
les générateurs: $A_{j,k} = \sigma_{k-1}\sigma_{k-2}...\sigma_{j+1}\sigma_j^2\sigma_{j+1}^{-1}...\sigma_{k-2}^{-1}\sigma_{k-1}^{-1}$ *pour* $1 \leq j < k \leq n$ *et les relations:*
A- Si $1 \leq r < s < i < j \leq n$ *ou* $1 \leq r < i < j < s \leq n$ *on a:*

$$A_{r,s}A_{i,j} = A_{i,j}A_{r,s}$$

B- Si $1 \leq r < s < j \leq n$ *on a:*

$$A_{r,s}A_{r,j}A_{r,s}^{-1} = A_{s,j}^{-1}A_{r,j}A_{s,j}$$

C- Si $1 \leq r < s < j \leq n$ *on a:*

$$A_{r,s}A_{s,j}A_{r,s}^{-1} = A_{s,j}^{-1}A_{r,j}^{-1}A_{s,j}A_{r,j}A_{s,j}$$

D- Si $1 \leq r < s < i < j \leq n$ *on a:*

$$A_{i,j}^{-1}A_{s,j}A_{i,j}A_{r,i} = A_{r,i}A_{i,j}^{-1}A_{s,j}A_{i,j}$$

Preuve. Le groupe $\mathcal{P}_n$ est d'indice $n!$ dans $\mathcal{B}_n$.

Soit $M = \left\{\Pi_{j=2}^{n} M_{j,k_j} \text{ ,} 1 \leq k_j \leq j\right\}$ tel que $M_{j,i} = \sigma_{j-1}\sigma_{j-2}...\sigma_i$ est un système de Schreier de représentant des classes à droite de $\mathcal{P}_n$ dans $\mathcal{B}_n$.

On applique la méthode de Reidemeister-Schreier on obtient la présentation de $\mathcal{P}_n$. ■

1.2.1 Présentation du groupe dérivé du groupe des tresses

Exercice 1.2.1 *Montrer que le groupe dérivé du groupe de tresses est caractérisé par:*

$$H_n = \{\beta \in \mathcal{B}_n / \exp(\beta) = 0\}$$

Solution 1.2.1 *Montrons que H_n est un sous groupe normal de $\mathcal{B}_n$*
alors soient $\beta_1, \beta_2 \in \mathcal{B}_n$.
Montrons que H_n est un sous groupe de $\mathcal{B}_n$.
$\forall\ \beta_1,\ \beta_2 \in H_n$, $\beta_1\beta_2^{-1} \in H_n$.
$\exp(\beta_1\beta_2^{-1}) = \exp(\beta_1) - \exp(\beta_2) = 0$
cela implique que $\beta_1\beta_2^{-1} \in H_n$ donc H_n est un sous groupe de $\mathcal{B}_n$.
Montrons maintenant que H_n est normal dans $\mathcal{B}_n$.
H_n est normal dans $\mathcal{B}_n$ $\iff$ $\beta H_n \beta^{-1} \in H_n$ $\forall h \in H_n$ et $\forall \beta \in \mathcal{B}_n$. $\exp(\beta h \beta^{-1}) = \exp(\beta) + \exp(h) - \exp(\beta) = 0$ *donc* $\beta h \beta^{-1} \in H_n$
$\forall h \in H_n$ *et* $\forall \beta \in \mathcal{B}_n$.
Soit $M = \left\{..., \sigma_1^{-k}, ..., \sigma_1^{-1}, 1, \sigma_1, ..., \sigma_1^k, ...\right\}$ *un système de Schreier de représentants des classes à droite de H_n dans $\mathcal{B}_n$.*
$H_2 = \{1\}$ et H_3 est un groupe libre engendré par $a_0 = \sigma_2\sigma_1^{-1}$ et $a_1 = \sigma_1\sigma_2\sigma_1^{-2}$.
H_2 est un sous groupe de $\mathcal{B}_2 = \langle \sigma_1 / - \rangle$ tel que $\forall \beta \in \mathcal{B}_2$ $\exp(\beta) = 0$ donc H_2 ne contient que le mot vide alors $H_2 = \{1\}$.
$\mathcal{B}_3 = \langle \sigma_1, \sigma_2 /. \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$
$H_3 = \{\beta \in \mathcal{B}_3 / \exp(\beta) = 0\}$, *M est un système de Schreier de représentants des classes à droite de H_3 dans $\mathcal{B}_3$,alors $H_3 = \langle y_{j,k}./R_k \rangle$ avec $y_{j,k} = \rho(M_k,\ \sigma_j)$ et $\sigma_j \in \mathcal{B}_3$*
$\rho(M_k,\ \sigma_j) = M_k\sigma_j\overline{M_k\sigma_j}^{-1}$, $M_k = \sigma_1^k$
$\rho(M_k,\ \sigma_1) = \sigma_1^k\sigma_1\overline{\sigma_1^k\sigma_1}^{-1} = 1 = y_{1,k}$
$\rho(M_k,\ \sigma_2) = \sigma_1^k\sigma_2\overline{\sigma_1^k\sigma_2}^{-1} = \sigma_1^k\sigma_2\overline{\sigma_1^{k+1}} = \sigma_1^k\sigma_2\sigma_1^{-(k+1)}$
$\left[y_{2,k} = \sigma_1^k\sigma_2\sigma_1^{-(k+1)}\right]$
Reste à déterminer R_k telle que $R_k = \tau(M_k R M_k^{-1})$ et $R = \sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$

alors

$$\begin{aligned}
R_k &= \tau(\sigma_1^k\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-k}) \\
&= \tau(\sigma_1^k\sigma_1\sigma_1^{-(k+1)}\sigma_1^{(k+1)}\sigma_2\sigma_1^{-(k+2)}\sigma_1^{(k+2)}\sigma_1\sigma_1^{-(k+3)}\sigma_1^{(k+3)}(\sigma_1^k\sigma_2\sigma_1\sigma_2)^{-1}) \\
&= \tau(\sigma_1^k\sigma_1\sigma_1^{-(k+1)}\sigma_1^{(k+1)}\sigma_2\sigma_1^{-(k+2)}\sigma_1^{(k+2)}\sigma_1\sigma_1^{-(k+3)}\sigma_1^{(k+3)} \\
&\qquad (\sigma_1^k\sigma_2\sigma_1^{-(k+1)}\sigma_1^{(k+1)}\sigma_1\sigma_1^{-(k+2)}\sigma_1^{(k+2)}\sigma_2\sigma_1^{-(k+3)}\sigma_1^{(k+3)})^{-1} \\
&= \rho\left(M_k,\sigma_1\right)\rho\left(M_{k+1},\sigma_2\right)\rho\left(M_{k+2},\sigma_1\right)\rho^{-1}\left(M_{k+2},\sigma_2\right)\rho^{-1}\left(M_{k+1},\sigma_1\right)\rho^{-1}\left(M_k,\sigma_2\right) \\
&= \rho\left(M_{k+1},\sigma_2\right)\rho^{-1}\left(M_{k+2},\sigma_2\right)\rho^{-1}\left(M_k,\sigma_2\right) \\
&= y_{k+1}y_{k+2}^{-1}y_k^{-1}
\end{aligned}$$

alors

$$y_{k+1} = y_k y_{k+2}$$

H_3 est un groupe libre engendré par $y_0 = \sigma_2\sigma_1^{-1}$
$y_1 = \sigma_1\sigma_2\sigma_1^{-2}$
Posons $z_m = \sigma_1^m\left(\sigma_2\sigma_1^{-1}\right)\sigma_1^{-m}$, $m \in \mathbb{Z}$ et $x_i = \sigma_i\sigma_1^{-1}$ pour $i = 3, ..., n-1$ et applique la méthode de Reidemeister-Schreier. On obtient la présentation suivante:

$$H_n = \langle \begin{array}{l} z_m = \sigma_1^m\left(\sigma_2\sigma_1^{-1}\right)\sigma_1^{-m}, m \in \mathbb{Z} \\ x_i = \sigma_i\sigma_1^{-1} pour i = 3, ..., n-1 \end{array} / \begin{array}{c} x_i x_j = x_j x_i \ si\ |i-j| > 1 \\ x_i x_j x_i = x_j x_i x_j \ si\ |i-j| = 1 \\ z_m z_{m+2} = z_{m+1}, m \in \mathbb{Z} \\ z_m x_3 z_{m+2} = x_3 z_{m+1} x_3 \ i = 4, ..., n-1 \ et\ m \in \mathbb{Z} \\ z_m x_i = x_i z_{m+1}\ ,\ i = 4, ..., n-1 \ et\ m \in \mathbb{Z} \end{array} \rangle.$$

Montrons que H_n est le groupe dérivé du groupe de tresses $\mathcal{B}_n$. Pour cela on considère le sous groupe $\mathcal{B}_n'$ engendré par tous les commutateurs et montrons que $\mathcal{B}_n' = H_n$.
Soit $l = \beta_1\beta_2\beta_1^{-1}\beta_2^{-1} \in \mathcal{B}_n'$, alors $\exp(l) = \exp(\beta_1\beta_2\beta_1^{-1}\beta_2^{-1}) = \exp(\beta_1) + \exp(\beta_2) - \exp(\beta_1) - \exp(\beta_2) = 0$
donc $\beta_1\beta_2\beta_1^{-1}\beta_2^{-1} \in H_n$
réciproquement soient $h = \sigma_i^{\varepsilon_i}\sigma_j^{\varepsilon_j}\sigma_k^{\varepsilon_k}...\sigma_r^{\varepsilon_r} \in H_n$ tel que $\exp(h) = 0$ et on utilise les relations de définition:

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \qquad si \qquad |i-j| = 1$$

et

$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad si \qquad |i-j| > 1$$

et on remplace dans h les facteurs $\sigma_i\sigma_j^{-1}$ par:
$\sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i = \left[\sigma_j^{-1}, \sigma_i^{-1}\right] \in \mathcal{B}_n'$ si $|i-j| = 1$
et par:

$\sigma_j^{-1}\left[\sigma_i\ ,\sigma_j\right]^{-1}\sigma_i = \sigma_j^{-1}\left[\sigma_j,\sigma_i\right]\sigma_i = \sigma_j^{-1}\sigma_i\left[\sigma_i^{-1},\sigma_j\right]$ *si* $|i-j|>1$

Mais $\sigma_j^{-1}\sigma_i\left[\sigma_i^{-1},\sigma_j\right] \in \mathcal{B}_n^{'}$ *car* $\mathcal{B}_n^{'}$ *est sous groupe de* $\mathcal{B}_n$ *.*

Donc h s'ecrit comme produit des commutateurs.

De ce qui précède il résulte que:

$$\mathcal{B}_n^{'} = H_n$$

2

Problèmes algorithmiques dans le groupe des tresses

Nous traitons dans ce chapitre deux problèmes classiques, le premier est le problème du mot. Il était résolu la première fois par E. Artin en 1947 [3] qui utilise une méthode dite (tresses peignées). On va présenter cette méthode ici. D'autres solutions ont été proposées par Garside [15] et un peu plus tard par Dehornoy [8]. Le deuxième problème a été résolu par Garside en 1969 [15] et sa démonstration est basée sur l'élément

$$\Delta_n = (\sigma_1\sigma_2...\sigma_{n-1})\,(\sigma_1\sigma_2...\sigma_{n-2})\,...\,(\sigma_1\sigma_2)\,(\sigma_1)$$

En 1992 Elrifai et Morton redémontrent ce problème [12]. En 1998, Birman et d'autres mathématiciens [5] découvrent une autre solution basée sur le monoïde dual du monoïde de Garside.

Nous donnons ici la solution de Garside.

2.1 Le problème du mot pour le groupe des tresses

Lorsqu'on se donne une présentation de groupe par générateurs et relations il est naturel de se poser le problème suivant:

Problème 2.1.1 *Soient données deux tresses* $\beta_1\ \beta_2 \in \mathcal{B}_n$
Existe t-il une méthode pour décider si $\beta_1 = \beta_2$ *?*

Définition 2.1.1 *Un mot de tresse w est mot formé à partir des générateurs $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ et de leurs inverses:*
Soient w_1, w_2 deux mots de tresses. On dit que w_1 est équivalent à w_2 si on peut transformer w_2 à w_1 par application des opérations suivantes:

$$T_1 : x_{i_1}^{\varepsilon_1}...x_{i_j}^{\varepsilon_j}x_{i_{j+1}}^{\varepsilon_{j+1}}...x_{i_m}^{\varepsilon_m} \to x_{i_1}^{\varepsilon_1}... \left[x_p^{\varepsilon_p}x_p^{-\varepsilon_p}\right] ...x_{i_m}^{\varepsilon_m} \tag{2.1.1}$$

$$T_2 : x_{i_1}^{\varepsilon_1}...x_{i_j}^{\varepsilon_j} \left[x_p^{\varepsilon_p}x_p^{-\varepsilon_p}\right] x_{i_{j+1}}^{\varepsilon_{j+1}}...x_{i_m}^{\varepsilon_m} \to x_{i_1}^{\varepsilon_1}...x_{i_m}^{\varepsilon_m} \tag{2.1.2}$$

T_1 est appelée insertion et T_2 est appelée suppression.

Théorème 2.1.1 *Le problème du mot est résoluble pour les groupes libres.*

Preuve. voir [21] ■

Solution 2.1.1 *du problème du mot pour le groupe des tresses.*

Pour résoudre ce problème on suit les étapes suivantes:

La première étape: Est-ce-que la tresse en question est une tresse pure ou non ?.

Pour cela on considère sa tresse de permutation $\pi(\beta) \in \Sigma_n$. Si $\pi(\beta) = (1)$ alors β est une tresse pure, si $\pi(\beta) \neq (1)$ alors β ne l'est pas.

Donc on détermine la tresse de permutation $\pi(\beta)$.
Si β est une tresse pure, alors on passe à la seconde étape.

La deuxieme étape Puisque β est une $n-$tresse pure, alors chaque courbe d_i joint A_i avec B_i pour tout $i = 1, 2, ..., n$, puis on remplace le dernier brin d_n par un segment et on note la nouvelle tresse par γ, aprés on fait le produit de β et γ^{-1} et on pose

$$\alpha = \beta\gamma^{-1}$$

Si on supprime le brin final de α alors la tresse obtenue est la tresse triviale.

Définition 2.1.2 *La tresse α est appelée tresse peignée*

Soit maintenant $\alpha = \alpha_1$, $\gamma = \gamma_1$ donc

$$\beta = \alpha_1\gamma_1$$

On s'intéresse maintenant à γ_1, puisque le dernier brin de γ_1 est un segment. On applique le processus précédent à γ_1 en commençant avec les $(n-1)^{\grave{e}me}$ brins.

Soit γ_2 la tresse γ_1 ou on supprime le $(n-1)^{\overset{ème}{=}}$ brin et on le remplace par un segment, donc on obtient une tresse peignée α_2 , alors on a

$$\gamma_1 = \alpha_2\gamma_2$$

et

$$\beta = \alpha_1\alpha_2\gamma_2$$

On repète ce processus et on arrive à la décomposition de β sous la forme

$$\beta = \alpha_1\alpha_2...\alpha_{n-1} \tag{2.1.3}$$

tel que chaque n tresse α_i est une tresse peignée pour $i = 1, 2, ..., n-1$.

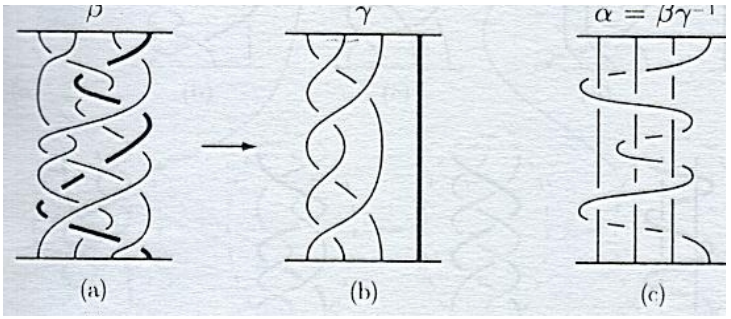

Figure 2.1.1 : Décomposition d'une tresse pure en produit des tresses peignées

Proposition 2.1.1 *Soit β une tresse pure alors β est une tresse triviale si et seulement si chaque α_i dans la décomposition (2.1.3) est une tresse triviale.*

Preuve. $\Longleftarrow$ / Si chaque α_i est une tresse triviale alors β aussi est une tresse triviale.
$\Longrightarrow$ / On suppose que β est une tresse triviale et soit ξ_i la $(n-i)^{\overset{ème}{=}}$ tresse obtenue de β en supprimant son dernier $i^{\overset{ème}{=}}$ brin.
Par construction : $\xi_0 = \beta$ et ξ_{n-1} est une tresses a un brin et ξ_n est la tresse triviale.

Puisque β est une tresse triviale alors pour chaque $i = 0, 1, ..., n-1$ les tresses $\xi_0, \xi_1, ..., \xi_{n-1}$ sont des tresses triviales .

De la même façons on définit $\alpha_{j,i}$ comme étant la $(n-i)^{ème}-$tresse obtenue de α_j en supprimant le dernier brin, alors on a la construction :

$$\begin{aligned}
\beta &= \xi_0 = \alpha_1 ... \alpha_{n-1} \\
\xi_1 &= \alpha_{1,1}\alpha_{2,1} ... \alpha_{n-1,1} \\
\xi_2 &= \alpha_{1,2}\alpha_{2,2} ... \alpha_{n-1,2} \\
&... \\
\xi_{n-2} &= \alpha_{1,n-2}\alpha_{2,n-2} ... \alpha_{n-1,n-2}
\end{aligned}$$

telle que $\alpha_{1,1}$ est la $(n-1)-$tresse triviale , $\alpha_{1,2}$ et $\alpha_{2,2}$ sont les tresses triviales a $(n-2)$ brins.

En général $\alpha_{1,i}$, $\alpha_{2,i}$, ..., $\alpha_{i,i}$ pour $i = 1, 2, ..., n-2$ sont tous des $(n-i)-$tresses triviales.

Maintenant $\alpha_{1,n-2}$, $\alpha_{2,n-2}$, ..., $\alpha_{n-2,n-2}$ sont tous des $2-$tresses triviales et α_{n-1} est une $n-$tresse obtenue de la tresse $\alpha_{n-1,n-2}$ a deux brins en ajoutant $(n-2)$ segments de plus la trivialité de $\xi_{n-2} = \alpha_{n-1,n-2}$ implique que α_{n-1} est une $n-$tresse triviale.

Par ce processus on montre que chaque α_i est triviale. ■

La troisième étape On détermine si chaque tresse α_i est triviale ou non ?

Donc si on peut démontrer que chaque α_i est un élément d'un groupe libre, alors on peut déterminer si chaque tresse α_i est triviale ou non de la $3^{ème}=$ et le finale étape de l'algorithme.

On déduit à partir des trois étapes précédentes la solution du problème du mot pour le groupe des tresses $\mathcal{B}_n$.

Notre but ici est de démontrer que les tresses peignées sont des éléments d'un groupe libre.

Soit A_n l'ensemble des tresses peignées α tel que si on supprime le dernier brin on obtient la tresse triviale.

Proposition 2.1.2 *A_n est un sous groupe normal de $\mathcal{P}_n$.*

Preuve. A_n n'est pas vide car $1_n \in A_n$

Soient a_1, $a_2 \in A_n$

$a_1 (a_2)^{-1} \in A_n$ car $\pi\left(a_1 (a_2)^{-1}\right) = \pi(a_1)\,\pi\left((a_2)^{-1}\right) = \pi(a_1)\,\pi(a_2)^{-1} = (1)$

Alors A_n est un sous groupe de $\mathcal{P}_n$.

A_n est normal dans $\mathcal{P}_n$

Soient $\alpha \in \mathcal{P}_n$ et $\beta \in A_n$: $\alpha\beta\alpha^{-1} \in A_n$

$\pi(\alpha\beta\alpha^{-1}) = \pi(\alpha)\,\pi(\beta)\,\pi(\alpha)^{-1} \in A_n$

Donc A_n est normal dans $\mathcal{P}_n$. ■

Proposition 2.1.3 *le groupe A_n est engendré par les $(n-1)-$éléments*

$$\begin{aligned} a_1 &= (\sigma_{n-1}\sigma_{n-2}...\sigma_2)\,\sigma_1^2\left(\sigma_2^{-1}...\sigma_{n-2}^{-1}\sigma_{n-1}^{-1}\right) \\ a_2 &= (\sigma_{n-1}\sigma_{n-2}...\sigma_3)\,\sigma_2^2\left(\sigma_3^{-1}...\sigma_{n-2}^{-1}\sigma_{n-1}^{-1}\right) \\ &... \\ a_{n-2} &= \sigma_{n-1}\sigma_{n-2}^2\sigma_{n-1}^{-1} \\ a_{n-1} &= \sigma_{n-1}^2 \end{aligned}$$

Preuve. voir [21] ■

Proposition 2.1.4 *Les éléments $a_1, a_2, ..., a_{n-1}$ définis dans la proposition* (2.1.3) *engendrent librement le groupe A_n.*

Preuve. On considère le sous-ensemble H_n de $\mathcal{B}_n$, tel que

$$H_n = \{n \text{ tresses } \beta \text{ avec } \pi(\beta)(n) = n\}$$

c'est à dire la tresse de permutation qui laisse n fixé.

H_n est un sous groupe de $\mathcal{B}_n$.

Les éléments β_1, β_2 appartiennent à la même classe à droite si et seulement si $\beta_1\beta_2^{-1} \in H_n$ et donc

$$\pi(\beta_1)(n) = \pi(\beta_2)(n)$$

Chaque classe à droite $H_n\beta$ de H_n dans $\mathcal{B}_n$ est l'ensemble des tresses β avec $\pi(\beta)(n) = k$ pour un certain $1 \leq k \leq n$. Donc on a de plus n classes à droite distinctes de H_n dans $\mathcal{B}_n$ et donc

$$[\mathcal{B}_n : H_n] = n$$

En particulier chaque classe à droite est représentée par

$$M_i = \sigma_{n-1}, ..., \sigma_{n-i+1}$$

Pour $i = 1, 2, ..., n$ et $M_1 = 1$, on note que

$$\begin{aligned} \pi(M_i) &= \pi(\sigma_{n-1}, ..., \sigma_{n-i+1}) \\ &= (n, n-1)...(n-i+2, n-i+1) \end{aligned}$$

et alors on a $\pi(M_i) = n - i + 1$ ■

Proposition 2.1.5 *1-pour tout élément $g \in G, Mi \in M$.pour $i = 1, 2.....$*
$\rho(M_i, g) = M_i g \overline{Mg}^{-1} \in H$ *tel que* $M_i = \sigma_{n-1}\sigma_{n-2}...\sigma_{n-i+1}$
2- pour $j = 1, 2, ..., n$ *et* $k = 1, 2, ..., [G : H]$
On pose $y_{j,k} = \rho(M_k, x_j)$ *alors* H *est engendré par les* $y_{j,k}$ *est ses inverses*

Preuve. 1- puisque $M_i g, \overline{M_i g}$ ont le même representant des classes à droités de H alors $M_i g, \overline{M_i g} \in H$
2-$\rho(M_k, x_j) = y_{j,l}^{-1}$ pour un certain l tel que $M_k = \overline{M_l x_j}$
Soit $h \in H$ $h = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}$ $\overline{h} = \overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}}$ on transforme h comme suit:
$h = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}$
$= \left(1 x_{i_1}^{\epsilon_1} \overline{x_{i_1}^{\epsilon_1}}^{-1}\right)\left(\overline{x_{i_1}^{\epsilon_1}} x_{i_2}^{\epsilon_2} \overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}}^{-1}\right)...\left(\overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_{p-1}}^{\epsilon p-1}}^{-1} x_{i_p}^{\epsilon_p}\right)$
$= \rho\left(1, x_{i_1}^{\epsilon_1}\right) \rho\left(\overline{x_{i_1}^{\epsilon_1}}, x_{i_2}^{\epsilon_2}\right)...\rho\left(\overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_{p-1}}^{\epsilon p-1}}, x_{i_p}^{\epsilon_p}\right)$
On note cette transformation par τ alors
$\tau\left(x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_p}^{\epsilon_p}...\right) = \rho\left(1, x_{i_1}^{\epsilon_1}\right)\rho\left(\overline{x_{i_1}^{\epsilon_1}}, x_{i_2}^{\epsilon_2}\right)...\rho\left(\overline{x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2}...x_{i_{p-1}}^{\epsilon p-1}}, x_{i_p}^{\epsilon_p}\right) = y_{i_1,\lambda_1}^{\varepsilon_1} y_{i_2,\lambda_2}^{\epsilon_2}...y_{i_p,\lambda_p}^{\epsilon_p}$ alors chaque facteur est $y_{j,k}$ ou bien son inverse pour un certain j et k ■

Proposition 2.1.6 *Soient G un groupe qui a la présentation suivante $G =< x_1, x_2, ..., x_n. / R_1 = 1, R_2 = 1, ..., R_m = 1 >$ et H un sous groupe de G et $M = \{M_1, M_2, ..., M_n\}$ un système de Schreier alors H a la présentation suivante:*

$$H = \langle y_{j,k} / R_{l,k} \text{ pour } j = 1, 2, ..., n, l = 1, 2, ..., m \text{ et } k = 1, 2, ..., [G : H] \rangle$$

avec $R_{l,k} = \tau\left(M_k R_l M_K^{-1}\right)$

Preuve. $M = \{M_1, M_2, ..., M_n\}$ un système de *Schreier* des classes à droite.

On utilise ce système pour trouver une présentation de H_n et puisque ce processus est une application de la méthode de Reidemeister-Schreier on va déterminer explicitement les génerateurs de H_n .

Alors on a:

$$\begin{aligned}
M_i &= \sigma_{n-1}, ..., \sigma_{n-i+1} \\
&\Longrightarrow M_i\sigma_j = \sigma_{n-1}, ..., \sigma_{n-i+1}\sigma_j \\
\overline{M_i\sigma_j} &= \overline{\sigma_{n-1}, ..., \sigma_{n-i+1}\sigma_j} \\
&= \sigma_{n-1}, ..., \sigma_{n-i+1} \text{ si } n-i > j \text{ on } n-i < j-1 \\
&= \sigma_{n-1}, \sigma_{n-2}, ..., \sigma_j + 1\sigma_j \text{ si } n-1 = j \\
&\quad \sigma_{n-1}, \sigma_{n-2}, ..., \sigma_j + \sigma_{j+1} \text{ si } n-i = j-1
\end{aligned}$$

Maintenant on va calculer

$$\pi\left(\overline{M_i\sigma_j}\right) = \overline{\pi\left(M_i\sigma_j\right)}$$

Le groupe H_n est engendré par

$$\sigma_1, \sigma_2, ..., \sigma_{n-2} \text{ pour } j = 1, 2, ...n-1$$

et par

$$a_j = \left(\sigma_{n-1}\sigma_{n-2}, ...\sigma_{j+1}\right)\sigma_j^2\left(\sigma_{j+1}^{-1}...\sigma_{n-2}^{-1}\sigma_{n-1}^{-1}\right)$$

On a déja établi la nature des générateurs donc il reste à trouver l'ensemble des relations de définition
Le premier type des relations devient

$$\tau\left(M_i\sigma_k\sigma_l\sigma_k^{-1}\sigma_l^{-1}M_i^{-1}\right) = 1 \text{ pour } \begin{array}{c} i = 1, 2, ..., n \\ \text{et} \\ k, l = 1, 2, ..., n-1 \end{array}$$

Mais

$$\begin{aligned} \tau\left(M_i\sigma_k\sigma_l\sigma_k^{-1}\sigma_l^{-1}M_i^{-1}\right) &= \tau\left[\left(\sigma_{n-1}\sigma_{n-2}...\sigma_{n-i}\right)\sigma_k\sigma_l\sigma_k^{-1}\sigma_l^{-1}\left(\sigma_{n-i}^{-1}...\sigma_{n-2}^{-1}\sigma_{n-1}^{-1}\right)\right] \quad (2.1.4) \\ &= M_i\sigma_k\overline{M_i\sigma_k}^{-1}.M_i\sigma_k\sigma_l\overline{M_i\sigma_k\sigma_l}^{-1}.\overline{M_i\sigma_k\sigma_l}\sigma_k^{-1}.\overline{M_i\sigma_k\sigma_l\sigma_k^{-1}}^{-1} \\ &\quad .\overline{M_i\sigma_k\sigma_l\sigma_k^{-1}}\sigma_l^{-1}\overline{M_i\sigma_k\sigma_l\sigma_k^{-1}\sigma_l^{-1}}^{-1} \end{aligned}$$

Puisque M est un système de Schreier *et* les facteurs qui restent sont tous identiques, l'argument qui apparait dans (2.1.4) détermine explicitement les relations. ■

Proposition 2.1.7 *Le groupe H_n a une présentation de la forme*

$$< \sigma_1, \sigma_2, ..., \sigma_{n-2}, a_1, ..., a_{n-1} / \quad \begin{array}{c} \sigma_i\sigma_k = \sigma_k\sigma_i \text{ pour } |i-k| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ pour } i = 1, ..., n-3. \\ \sigma_i a_k\sigma_i^{-1} = a_k \text{ pour } k \neq i, i+1 \\ \sigma_i a_i\sigma_i^{-1} = a_{i+1} \\ \sigma_i a_{i+1}\sigma_i^{-1} = a_{i+1}^{-1}a_i a_{i+1} \end{array}$$

On considère maintenant le groupe libre F engendré par les éléments $\mu_1, \mu_2, ..., \mu_{n-1}$ et on va établir un morphisme entre H_n et le groupe des automorphisme $Aut\,(F)$. Définissons cette application pour démontrer que A_n est un groupe libre engendré par $a_1, a_2, ..., a_{n-1}$.

Pour cela soit $\phi : H_n \to Aut(F)$ pour $k = 1, 2, ..., n-2$

$$\phi(\sigma_k) : \begin{cases} \mu_i \longmapsto \mu_i \text{ si } i \neq k, k+1 \text{ et } 1 \leq i \leq n-1 \\ \mu_k \longmapsto \mu_{k+1} \\ \mu_{k+1} \longmapsto \mu_{k+1}^{-1}\mu_k\mu_{k+1} \end{cases}$$

et pour $j = 1, 2, ..., n-1$ par

$$\phi(a_j) : \mu_i \to \mu_j^{-1}\mu_i\mu_j \text{ avec } i = 1, 2, ..., n-1$$

l'application ϕ définie précédement est un morphisme de H_n dans $Aut(F)$.

Preuve. Il suffit de démontrer que l'image de chaque relation dans la présentation de H_n est l'élément neutre dans $Aut(F)$ .On commence par une des relations

$$\sigma_i a_i \sigma_i^{-1} = a_{i+1}$$

Si $j \neq i, i+1$ on a

$$\begin{aligned} \phi\left(\sigma_i a_i \sigma_i^{-1}\right) &: \mu_i \overset{\sigma_i^{-1}}{\longmapsto} \mu_j \overset{a_i}{\longmapsto} \mu_i^{-1}\mu_j\mu_i \overset{\sigma_i}{\longmapsto} \mu_{j+1}^{-1}\mu_j\mu_{j+1} \\ \phi(a_{i+1}) &: \mu_j \longmapsto \mu_{j+1}^{-1}\mu_i\mu_{j+1} \end{aligned}$$

alors

$$\phi\left(\sigma_i a_i \sigma_i^{-1}\right) = \phi(a_{i+1})$$

et

$$\phi\left(\sigma_i a_i \sigma_i^{-1}\right) : \mu_{i+1} \overset{\sigma_i^{-1}}{\longmapsto} \mu_i \overset{a_i}{\longmapsto} \mu_i \overset{\sigma_i}{\longmapsto} \mu_{i+1}$$

donc

$$\left(\sigma_i a_i \sigma_i^{-1}\right)(\mu_i) = \mu_{i+1}$$

et

$$\phi(a_{i+1}) : \mu_{i+1} \longmapsto \mu_{i+1} = \mu_{i+1}^{-1}\mu_{i+1}\mu_{i+1}$$

Notre but est de démontrer que $a_1, a_2, ..., a_{n-1}$ sont des générateurs libres.

Si $n = 2$: a_1 engendre un groupe libre de rang 1 puisque $a_l^k \neq 1$ pour tout $k \neq 0$. On suppose que $n \geq 3$.

Supposons que $a_1, a_2, ..., a_{n-1}$ ne sont pas des générateurs libres de H_n , donc il existe une relation non triviale dans H_n en termes des $a_1, a_2, ..., a_{n-1}$ c'est à dire

$$w(a_1, a_2, ..., a_{n-1}) = 1 \tag{2.1.5}$$

Si on applique le morphisme précédent à la relation (2.1.5) on obtient

$$\phi(w)(a_1, a_2, ..., a_{n-1}) = w(\phi(a_1), \phi(a_2), ..., \phi(a_{n-1})) = id_{Aut(F)}$$

On suppose que

$$w(a_1, a_2, ..., a_{n-1}) = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} ... a_{i_k}^{\varepsilon_k}$$

donc pour $j = 1, 2, ..., n-1$

$$\phi(w)(u_j) = \left(u_{i_1}^{-\varepsilon_1} ... u_{i_{k-1}}^{-\varepsilon_{k-1}} u_{i_k}^{-\varepsilon_k}\right) u_j \left(u_{i_k}^{\varepsilon_k} u_{i_{k-1}}^{\varepsilon_{k-1}} ... u_{i_1}^{\varepsilon_1}\right)$$

d'autre façon puisque $u_1, u_2, ..., u_{n-1}$ sont des générateurs libres de F et $\phi(w) = id_{Aut(F)}$ implique

$$u_j = \left(u_{i_1}^{-\varepsilon_1} ... u_{i_{k-1}}^{-\varepsilon_{k-1}} u_{i_k}^{-\varepsilon_k}\right) u_j \left(u_{i_k}^{\varepsilon_k} u_{i_{k-1}}^{\varepsilon_{k-1}} ... u_{i_1}^{\varepsilon_1}\right) \tag{2.1.6}$$

pour $j = 1, 2, ..., n-1$

On pose $u_{i_k}^{\varepsilon_k} u_{i_{k-1}}^{\varepsilon_{k-1}} ... u_{i_1}^{\varepsilon_1} = g$ alors (2.1.6) implique que g commute avec les u_j pour chaque $j = 1, 2, ..., n-1$

Alors il existe un entier λ_j tel que $g = u_j^{\lambda_j}$ pour $j = 1, 2, ..., n-1$ ce qui implique aussi que si $j \neq l$ alors

$$u_j^{\lambda_j} = u_l^{\lambda_l}$$

mais $u_1, u_2, ..., u_{n-1}$ sont des générateurs libres de F ce qui donne

$$\lambda_j = \lambda_l = 0 \text{ ce qui implique que } g = 1$$

Donc aprés un nombre fini d'opérations T_1 ou T_2 , g réduit au mot vide, donc la relation $w = 1$ est la relation triviale ce qui contredit la relation (2.1.5) Alors $a_1, a_2, ..., a_{n-1}$ forment un ensemble de générateurs libres d'ou la preuve de la proposition (2.1.4) . Alors on peut affirmer si la tresse β est triviale ou non et écrit β sous la forme

$$\beta = \alpha_1 \alpha_2 ... \alpha_{n-1}$$

tel que les α_i sont des tresses peignées.

Puisque α_1 est un élément du groupe libre A_n engendré par $a_1, a_2, ..., a_{n-1}$ on peut determiner si $\alpha_1 = 1$ ou non. Si $\alpha_1 \neq 1$ alors la proposition (2.1.1) implique que β n'est pas triviale.

On suppose que $\alpha_1 = 1_n$ et on considère α_2. On a $\alpha_2 = 1$ si et seulement si la $\alpha_{2,1} = 1_{n-1}$, mais par définition cette $(n-1)$ tresse est un élément d'un sous-groupe constitué par des

tresses peignées dans le groupe des $(n-1)$ tresses pures telles que seulement le $(n-1)^{eme}$ brin est lié avec les autres brins.

Donc $\alpha_{2,1} = 1_{n-1}$ est un élément du groupe libre de rang $(n-2)$ et on peut déterminer si $\alpha_{2,1} = 1_{n-1}$ ou non.
L'argument se répète pour déterminer si chaque $\alpha_i = 1$ ou non pour $i = 1, 2, ..., n-1$ ce qui est la solution du problème du mot pour $\mathcal{B}_n$. ■

2.2 Le problème de conjugaison pour le groupe des tresses

Problème 2.2.1 *Soient donnés* $\beta, \gamma \in \mathcal{B}_n$
Existe t-il un élément δ *tel que* $\beta = \delta\gamma\delta^{-1}$ *?*

Ce problème a été démontré en 1969 par Garside [15]. Sa méthode consiste à associer à chaque tresse $\beta \in \mathcal{B}_n$ l'ensemble de ses conjuguées appelé ensemble sommet.

Remarque 2.2.1 *La solution qu'on va présenter ici est basée sur une forme dite forme normale de Garside.*

Solution 2.2.1 *La solution est de la façon suivante:*

Rappellons que

$$\mathcal{B}_n = \langle \sigma_1, \sigma_2 ... \sigma_{n-1} / \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ si } |i-j| = 1 \text{ et } \sigma_i\sigma_j = \sigma_j\sigma_i \text{ si } |i-j| > 1 \rangle$$

Les générateurs de $\mathcal{B}_n$ dont les deus relations n'apparaissent qu'avec des puissances positives; alors il existe un semigroupe S_n tel que:

$$S_n = \langle s_1, s_2 ..., s_{n-1} / s_i s_j s_i = s_j s_i s_j \text{ si } |i-j| = 1 \text{ et } s_i s_j = s_j s_i \text{ si } |i-j| > 1 \rangle$$

Notation 2.2.1 *Soient* X, V, W *des mots de* S_n
$V = W$ *ségnifie que* $V; W$ *définissent le même élément dans* S_n *:*
$V \equiv W$ *ségnifie que* $V; W$ *sont deux mots identiques:*

Définition 2.2.1 *Soit* W *un mot de* S_n *tel que* $W = s_{i_1} s_{i_2} ... s_{i_k}$
l'entier k *est appelé longueur de* W *qu'on note* $L(W)$
Soit $V = V_0 = ... = V_r = W$ *si chaque* V_i *peut etre obtenu à partir de* V_{i-1} *par une seule*

application de l'une des relations de définition de S_n ; on dit dans ce cas que W est obtenu à partir de V par une chaine de transformation de longueur r.
Soit $D_1(W)$ l'ensemble de mots obtenus à partir de W par une chaine de transformation de longueur 0 ou 1, et $D_i(W)$ est l'ensemble de mots obtenus à partir de $D_{i-1}(W)$ par une chaine de transformation de longueur 0 ou 1, et puisque tous les mots de $D_i(W)$ sont de longueur $L(W)$ alors pour un certain i
$W \in D_1(W) \subset ... \subset D_i(W) = D_{i+1}(W)$.
Donc $D_i(W') = D_j(W)$ pour tout $j > i$.
$D_i(W)$ est appelé diagramme de W.

On considère les deux mots de tresse positif

$$\Delta = (\sigma_1\sigma_2...\sigma_{n-1})\,(\sigma_1\sigma_2...\sigma_{n-2})\,...\,(\sigma_1\sigma_2)\,(\sigma_1) \in \mathcal{B}_n$$

$$\Delta^{\#} = (s_1s_2...s_{n-1})\,(s_1s_2...s_{n-2})\,...\,(s_1s_2)\,(s_1) \in S_n$$

Notation 2.2.2 *Si $w = s_{i_1}...s_{i_k}$ on désigne par $\widehat{w}$ le mot $s_{n-i_1}...s_{n-i_k}$:*

Lemme 2.2.1 *Le mot $\Delta^{\#}$ a les propriétés.*
1-pour chaque mot $V \in S_n$

$$\Delta^{\#}V = \widehat{V}\Delta^{\#}$$

2-Pour chaque j , $(1 \leq j \leq n-1)$
$D(\Delta^{\#})$ contient un mot qui commence par s_j et un mot qui se termine par s_j

Preuve. [15] ■

Théorème 2.2.1 *L'application $\Psi : S_n \longrightarrow \mathcal{B}_n$*
$s_i \longmapsto \sigma_i$
est injective

Preuve. voir [4] ■

Lemme 2.2.2 *Pour chaque j $(1 \leq j \leq n-1)$ il existe un mot de tresse positif $\exists X_j$ tel que: $\sigma_j^{-1} = \Delta^{-1}X_j$ aussi $\Delta\sigma_j^{-1} = \sigma_{n-j}^{-1}\Delta$.*

Preuve. Conséquence du lemme (2.2.1) propriété 1 ■

Remarque 2.2.2 *Le lemme (2.2.1) et le lemme (2.2.2) impliquent que* $\Delta_n^{-1}V = \widehat{V}\Delta_n^{-1}$ *pour tout mot de tresses V.*

Définition 2.2.2 *Un mot positif P est dit premier à* Δ *s'il n y a pas de mots dans* $D(P)$ *de la forme* ΔQ *.*
Deux mots de tresses positifs P_1 *,* P_2 *du même longueur k , tels que:*

$$P_1 = \sigma_{\mu_1}....\sigma_{\mu_k}$$

$$P_2 = \sigma_{\lambda_1}....\sigma_{\lambda_k}$$

P_1 *est plus petit que* P_2 *si le nombre* $\mu_1\mu_2...\mu_k <$ *au nombre* $\lambda_1\lambda_2..\lambda_k$
$D(P)$ *possède un plus petit élément qu'on appelle base de* $D(P)$ *.*

Garside a démontré que chaque tresse $\beta \in \mathcal{B}_n$ peut etre représenté par un unique mot de la forme $\Delta^m\overline{P}$ tels que m et $\overline{P}$ se calculent comme suit:

Théorème 2.2.2 *Soit* $\sigma_{u_1}^{\varepsilon_1}\sigma_{u_2}^{\varepsilon_2}...\sigma_{u_r}^{\varepsilon_r}$ *un représentant de* β
1-Trouver tous les mots positifs $X_1, X_2, ..., X_{n-1}$
2-Remplacer chaque $\sigma_{u_i}^{-1}$ *qui apparait dans* $\sigma_{u_1}^{\varepsilon_1}\sigma_{u_2}^{\varepsilon_2}...\sigma_{u_r}^{\varepsilon_r}$ *par* $\Delta^{-1}X_{u_i}$
3-Regrouper les Δ^{-1} *à gauche en utilisant la propriété* $\Delta^{-1}V = \widehat{V}\Delta^{-1}$ *; donc* β *est représentée par un mot de la forme* $\Delta^k P_0$ *, tel que* P_0 *est un mot positif et* $k \leq 0$
4-Construire $D(P_0)$
5-Dans $D(P_0)$ *choisir un mot* $\Delta^h P$ *tel que h est maximal, puis on pose* $m = h + k$ *tel que* $h \geq 0$.
6-Dans $D(P)$ *en posant* $\overline{P}$ *la base de* $D(P)$ *.*

Définition 2.2.3 *Le mot* $\Delta^m\overline{P}$ *est appelé la forme normale de Garside pour* β *, l'entier m est appelé puissance de* β *et le mot* $\overline{P}$ *est appelé queue de* β *Si* $P \in D\left(\overline{P}\right)$ *alors le mot* $\Delta^m P$ *est appelé forme standard de Garside pour* β *.*

Lemme 2.2.3 *Soient s, m deux entiers. Alors le nombre de mots dans* $\mathcal{B}_n$.
(*dont la forme standard est de puissance* $\geq m$ *et la somme des exposants est s) est fini.*

Preuve. Soit la forme $\Delta^l A$ on suppose que $\Delta^l A$ satisfait les conditions:

$(i) : l \geq m.$

$(ii) : S = lL(\Delta) + L(A)$

$(iii) : S \diagup L(\Delta) \geq l.$

Alors il existe un nombre fini d'entiers vérifiants (i) et (iii).la condition (ii) montre que $L(A)$ est déterminée par l et par la suite il existe un nombre fini de mots de longueur donné.

■

Lemme 2.2.4 *Soit $\beta = \delta^{-1}\gamma\delta \in \mathcal{B}_n$ tel que γ, δ sont deux mots de tresse, alors il existe un mot positif B tel que $\beta = B^{-1}\gamma B \in \mathcal{B}_n$*

Preuve. Supposons que $\gamma = \Delta_n^q Q$, tel que Q est un mot positif

Si q est pair, on pose $B = Q$ alors $B^{-1}\gamma B = Q^{-1}\gamma Q = Q^{-1}\Delta^{-q}\Delta^q\gamma Q = Q^{-1}\Delta^{-q}\gamma\Delta^q Q = \delta^{-1}\gamma\delta$

Si q est impair, on pose $B = \Delta Q$ alors $B^{-1}\gamma B = Q^{-1}\Delta^{-1}\gamma\Delta Q = Q^{-1}\Delta^{-1}(\Delta^{1-q}\Delta^{q-1})\gamma\Delta Q$ $= Q^{-1}\Delta^{-q}\Delta^{q-1}\gamma\Delta Q = Q^{-1}\Delta^{-q}\gamma\Delta^q Q = \delta^{-1}\gamma\delta = \beta.$

Définition 2.2.4 *1-Si β est un mot positif, l'élément $\beta^{-1}\gamma\beta$ est appelé un conjugué positif de γ*

■

Si $\Delta = IF$ tel que: $1 \leq L(I) \leq L(\Delta)$

I est appelé la route initiale de Δ , et F est appelé la route finale associée

On définit l'ensemble sommet $S(\beta)$ d'un élément $\beta \in \mathcal{B}_n$ comme suit:

(i)-On construit la liste des routes intiales $\{I_1, I_2, ..., I_k\}$ du mot fondamental Δ dans $\mathcal{B}_n$

(ii)-Soit $S_1(\beta)$ l'ensemble de mots dont la forme standard a une puissance au moins plus grande que celle de β et tel que $S_1(\beta)$ est obtenu à partir de β par conjugaison par une seule route initiale I_j $(1 \leq j \leq k)$

Itérativement soit $S_i(\beta)$ l'ensemble de mots qui ont une puissance au moins plus grande que celle de β, et obtenu à partir des mots de $S_{i-1}(\beta)$ par conjugaison par une seule route intiale de Δ

(iii)-Le lemme (2.2.3) implique que le nombre de mots obtenus par ce processus est fini, alors pour un certain j

$$S_j(\beta) = S_{j+1}(\beta)$$

est le sous ensemble de $S_j(\beta)$ constitué par les éléments qui ont des puissances maximales dans $S_j(\beta)$.

Définition 2.2.5 *La puissance sommet t de $\beta \in \mathcal{B}_n$ est la puissances commune des éléments de $S(\beta)$, la queue sommet T de β est la queue de l'unique élément dans $S(\beta)$ avec la plus petite queue et la forme sommet de β est le mot $\Delta^t T \in \mathcal{B}_n$.*

Théorème 2.2.3 *Deux éléments $\beta_1, \beta_2 \in \mathcal{B}_n$ sont conjugués si et seulement s'ils ont la même forme sommet .*

Pour démontrer ce théorème on a besoin des lemmes suivants .

Définition 2.2.6 *Un mot de tresse V est commencé avec σ_i , si $D(V)$ contient un mot de la forme $\sigma_i A$. Il se termine par σ_i si $D(V)$ contient un mot de la forme $A\sigma_i$*

Lemme 2.2.5 *1-Si $i \in \{1, 2, ..., n-1\}$ alors $\Delta\sigma_i = \sigma_{n-i}\Delta$*
donc si V est un mot positif alors $\Delta V = \widehat{V}\Delta$
2-Si $i \in \{1, 2, ..., n-1\}$, il existe X_i, Y_i deux mots positifs tels que
$\Delta = \sigma_i X_i = Y_i\ \sigma_i$
3-Si $\Delta = IF$ alors soit I se termine par σ_i soit F commence par σ_i
pour chaque $i \in \{1, 2, ..., n\}$ mais pas les deux
4-Si $w = \Delta V$ et $w = AB$ alors soit A se termine par σ_i ou B commence en σ_i pour chaque $i \in \{1, 2, ..., n-1\}$
5-Si w est un mot positif dans $\mathcal{B}_n$,et si w commence en σ_i ou se termine en σ_i pour chaque $i \in \{1, 2, ..., n-1\}$
alors $w = \Delta V$ pour un certain mot positif V.

Preuve. voir [15] ■

Notation 2.2.3 *On désigne par $\widetilde{Q}$ les mots positifs Q ou $\widehat{Q}$*

Lemme 2.2.6 *Supposons que $\beta = \Delta^m P$ et on suppose en plus que pour un certain mot Q le mot $Q^{-1}\Delta^m PQ$ a puissance $r > m$ alors PQ contient Δ_n*

Preuve. Par hypothèse $Q^{-1}\Delta^m PQ = \Delta^r R$ avec $r > m$ et lemme (2.2.2)$\Longrightarrow \Delta^m PQ = Q\Delta^r R = \Delta^r \widetilde{Q}\ R \implies PQ = \Delta^{r-m}\widetilde{Q}R$, $r - m > 0$ ■

Lemme 2.2.7 *Dans le groupe des tresses $\mathcal{B}_n$ on suppose que.*
(1) $\gamma = \Delta^t T \in S(\beta)$
(2)X est un mot positif tel que $X^{-1}\gamma X = \Delta^t Q$
(3) $X = IY$ tel que I est une route de longueur minimale.
alors $I^{-1}\gamma I$ réduit à la forme standard est dans $S(\beta)$

Preuve. Puisque $\gamma \in S(\gamma) \subset S(\beta)$, $I^{-1}\gamma I$ a une puissance $\leq t$ il reste a démontrer que $I^{-1}\gamma I$ a une puissance $\geq t$

1-Si $X = \Delta Y$ alors $\Delta^{-1}\gamma\Delta = \Delta^{-1}(\Delta^t T)\Delta = \Delta^t \widehat{T}$ a une puissance t

2-Si $L(I) < L(\Delta)$, soit F un mot positif tel que :$IF = \Delta$ il y a une partition des indices $1, 2, ..., n-1$ en deux ensembles Ω et Λ tel que pour chaque $j \in \Omega$ il existe un mot positif U_j tel que :$I = U_j\sigma_j$ et pour chaque :$j \in \Lambda$ il n'existe pas de mot donc $I^{-1}\Delta^t = I^{-1}\Delta\Delta^{t-1} = F\ \Delta^{t-1} = \Delta^{t-1}\widetilde{F}$ et par conséquent $\Delta^t\ Q = X^{-1}\Delta\ X^{-1}\Delta X = Y^{-1}I^{-1}(\Delta^t T)IY = Y^{-1}\left[\Delta^{t-1}\widetilde{F}TI\right]Y$ et lemme (2.2.6) propriété 4 $\Longrightarrow$ $\widehat{F}TIY$ contient Δ.

Lemme (2.2.5) propriété 3 $\Longrightarrow$ soit $\widehat{F}TI = V_j\sigma_j$ pour un certain V_j

soit $V_j = \sigma_j Y_j$ pour un certain Y_j et $j \in \{1, 2, ..., n-1\}$

Mais si le dernier était vrai pour un certain $j \in \Lambda$, alors $X = IY = I\sigma_i Y_j$

et $I\sigma_j$ sera positivement égal à une route initiale de Δ de longueur $> L(I)$

(lemme (2.2.5) propriété 3 ce qui est contredit l'hypothèse .

Ainsi $\widetilde{F}TI = V_j\sigma_j$ pour chaque $j \in \Lambda$ établi par contradiction .

Encors $\widetilde{F}TI = \widetilde{F}TU_j\sigma_j$ pour chaque $j \in \Omega$.par définition de Ω

Donc par lemme (2.2.5) propriété 5 $\widetilde{F}TI$ contient Δ cela montre que

$$I^{-1}\gamma I = \Delta^{t-1}\widetilde{F}TI$$

a une puissance $\geq t$ ■

Revenons à la démonstration du théorème .

Preuve. On va maintenant prouver que β_1 est le conjugué de β_2 si et seulement si $S(\beta_1) = S(\beta_2)$

Si $X \in S(\beta_1) \cap S(\beta_2)$ donc X est le conjugué de β_1 et β_2 alors β_1 et β_2 sont conjugués. Réciproquement supposons que β_1 et β_2 sont conjugués tels que $\Delta^p P \in S(\beta_1)$ et $\Delta^q Q \in S(\beta_2)$ avec $p \leq q$, le lemme (2.2.4) implique qu'il existe un mot positif X tel que $X^{-1}($ $\Delta^p P)X = \Delta^q Q$.

Si $L(X) > 0$, alors $X = IY$ tel que I est une route initiale de Δ de longueur maximale $L(I) > 0$.

On note que $p \leq q$ donc par le lemme (2.2.6) $I^{-1}(\Delta^p P)I \in S(\beta_1)$ quand il est réduit à la forme normale.

Par récurrence sur la longueur de $L(X)$, $\Delta^q Q. = Y^{-1}\left[I^{-1}(\Delta^p P)I\right]Y$ a une forme normale dans $S(\beta_1)$ ainsi $S(\beta_2) \subset S(\beta_1)$ et $p = q$.

Puisque $p = q$ on répète le même argument et montrons que $S(\beta_1) \subset S(\beta_2)$ ce qui termine la démonsration. ■

3

Ordre sur les tresses

Depuis la découverte du caractère ordonnable du groupe des tresses en 1991 par Dehornoy [7], plusieurs méthodes ont été proposées pour résoudre le problème visé.

Le but de ce chapitre est de présenter les approches suivantes: l'algèbre autodistributive, la théorie combinatoire des groupes et le groupe des classes d'isotopie (mapping class group). Ces dernières seront utilisées pour construire l'ordre sur les tresses.

3.1 Ordre de Dehornoy sur les tresses

Une des découverte récentes les plus intéressantes concernant le groupe de tresses est due à Dehornoy qui a démontré fin de 1991 [7] que $\mathcal{B}_n$ a un ordre total invariant par multiplication à gauche. Le but de cette section est de présenter cette approche qui repose sur deux propriétés l'une est appelée propriété d'acyclicité et l'autre dite de comparaison.

Groupes ordonnables.

Définition 3.1.1 *Un groupe G est dit ordonnable s'il possède un ordre total $<$ invariant par multiplication à gauche, c'est à dire vérifiant $a < b \Rightarrow ca < cb$ pour tout $a, b, c \in G$.Si de plus l'ordre est invariant par multiplication à droite on dit que le groupe est biordonnable.*

Pour tout groupe ordonnable G , notons P l'ensemble$\{x \in G / x > 1\}$ de ses éléments positifs.

Le caractère total de l'ordre se traduit par la partition $G = P \amalg \{1\} \amalg P^{-1}$ où $P^{-1} = \{x \in G \ / \ x^{-1} > 1\}$.

L'invariance par multiplication à gauche se traduit par $P^2 \subseteq P$,où P^2 est formé des produits de deux éléments de P dans G.

Réciproquement, s'il existe un sous ensemble P de G vérifiant $G = P \amalg \{1\} \amalg P^{-1}$ et $P^2 \subseteq P$,alors G est ordonnable pour l'ordre défini par $x < y$ si $x^{-1}y \in P$.

L'ordre de Dehornoy sur $\mathcal{B}_n$

Définition 3.1.2 *1-Un mot de tresse w est mot formé à partir des générateurs $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ et de leurs inverses*
2-Pour $i \in \{1, 2, ..., n-1\}$,on dit qu'un mot de la forme $w = w_0\sigma_i w_1 \sigma_i ... \sigma_i w_r$ est σ_i-positif si les sous mots $w_0, w_1, ..., w_r$ sont des mots dans les lettres $\sigma_j^{\pm 1}$ avec $j > i$.S'il n'apparaît qu'avec des puissances négatives,on dit que le mot est σ_i-négatif
3-On dit qu'un mot de tresse w est $\sigma-$positif (respectivement $\sigma-$négatif) s'il existe un entier i tel que w est σ_i-positif (respectivement σ_i-négatif)
Si w n'est σ_i-positif ni σ_i-négatif, w est dit σ_i-libre.

Les deux propriétés suivantes nous assurent le caractère ordonnable de $\mathcal{B}_n$

Propriété d'acyclicité (A)

Toute tresse σ-positive est non triviale.

Propriété de comparaison (C)

Toute tresse est soit σ-positive, σ-négatif ou σ-libre.

Définition 3.1.3 *Soit $2 \leq n \leq \infty$ et soient $\beta_1, \beta_2 \in \mathcal{B}_n$.*
On dit que $\beta_1 < \beta_2$ est vrai si pour un certain i la tresse $\beta_1^{-1}\beta_2$ admet au moins un représentant σ_i-positif.
Un mot de tresse est dit positif si tous les exposants sont positifs

Notation 3.1.1 *$\mathcal{B}_n^+$ désigne l'ensemble des tresses positives ($\mathcal{B}_n^-$ est l'ensemble des tresses négatives respectivement)*

Théorème 3.1.1 *La relation $<$ est un ordre linéaire sur $\mathcal{B}_n$,invariant par multiplication à gauche.*

Preuve. Le fait que $\mathcal{B}_n^+, \{1\}$ et $(\mathcal{B}_n^+)^{-1}$ constituent une partition de $\mathcal{B}_n$ est exactement la propriété (C).

Soit $\beta \in \mathcal{B}_n^+ \cap (\mathcal{B}_n^+)^{-1}$ .Alors β et β^{-1} admettent un représentant σ-positif, donc $1 = \beta\beta^{-1}$ admet un représentant σ-positif ce qui contredit la propriété (A).
Alors $\mathcal{B}_n^+ \amalg \{1\} \amalg (\mathcal{B}_n^+)^{-1} = \mathcal{B}_n$ et $(\mathcal{B}_n^+)^2 \subseteq \mathcal{B}_n^+$

alors $<$ est est un ordre linéaire sur $\mathcal{B}_n$ invariant par multiplication à gauche. ■

3.1.1 Quelques applications de l'ordre sur les tresses

Lemme 3.1.1 *Soit G un groupe ordonnable à gauche et R est un anneau intègre.*
Alors l'anneau de groupe $R(G)$ n'a pas de diviseurs de zéro.
De plus les seuls unités de $R(G)$ sont les monomes rg tels que r est un élément inversible de R.

Preuve. G est ordonnable à gauche par hypothèse ,on considère dans l'anneau de groupe le produit suivant $(r_1g_1 + ... + r_pg_p)(s_1h_1 + ... + s_qh_q) = \sum_{i,j}(r_is_j)(g_ih_j)$ tel que tous les r_i et $s_j \in R - \{0\}$ et g_i , $h_j \in G$.

Si un produit est nul ,alors chaque terme est annulé par un autre dans le produit.

On suppose que $h_1 < h_2 < ... < h_q$,on considère le terme $(r_is_j)(g_ih_j)$ tel que g_ih_j est minimal en particulier $g_ih_j < g_ih_1$ mais puisque G est invariant par multiplication à gauche alors on a:$g_ih_j = g_ih_1$ donc $h_j = h_1$.

Alors on a montrer que si g_kh_l est le produit minimal alors on a:$l = j = 1$,donc $g_k = g_i$ et puisque $r_is_j \neq 0$ alors le produit dans l'anneau de groupe est non nul.Pour la deuxième partie, il y a un élément maximal dans le produit et si p ou $q > 1$ il diffère de l'élément minimal alors le produit est différent de 1 dans l'anneau de groupe $R(G)$. ■

Proposition 3.1.1 *Le groupe des tresses $\mathcal{B}_n$ est sans torsion.*

Preuve. Soit $\beta \in \mathcal{B}_n$

$\mathcal{B}_n$ est ordonné à gauche alors $\beta > 1$ implique $\beta^{-1} < 1$ ce qui donne:

$... < \beta^{-n} < \beta^{-n+1} < ... < \beta^{-1} < 1 < \beta < ...$

Alors $\beta^k \neq 1\ \forall k \in \mathbb{Z}$.

Donc $\mathcal{B}_n$ est sans torsion et par conséquent $\mathcal{B}_n$ est infini. ■

3.2 Ordre sur les tresse (méthode des systèmes autodistributifs)

Dehornoy déduit l'ordre sur les tresses à partir de l'étude générale des systèmes autodistributifs définis comme des ensembles munis d'une loi de composition vérifiant certaines identités et leurs liens avec les tresses est le but de cette section.

3.2.1 Action des tresses sur les systèmes autodistributifs

Définition 3.2.1 *Un système autodistributif qu'on note (AD) est un ensemble S mini d'une loi de composition qui vérifié.*

$$x * (y * z) = (x * y) * (x * z). \tag{3.2.1}$$

On définit une action de $\mathcal{B}_n^+$ sur S^n par la méthode suivante:
$S^n \times \mathcal{B}_n^+ \to S^n$

$$\begin{aligned} \overrightarrow{x}\varepsilon &= \overrightarrow{x} \\ \overrightarrow{x}...\sigma_i w &= (x_1, x_2, ...x_i * x_{i+1}, x_i, x_{i+2}, ..., x_n)w \end{aligned} \tag{3.2.2}$$

ε designe le mot vide

Coloriage des tresses.

Partons d'un mot de tresse w représentant un élément de $\mathcal{B}_n$. Colorions de gauche à droite les extremités supérieures des brins de la configuration plane associée à w avec les éléments $(a_1, ..., a_n) \in S^n$.
Si nous propageons les couleurs le long des brins, nous lirons en bas de la configuration une suite de couleurs qui est une permutation de $a_1, ..., a_n$.
On autorise les couleurs à interagir à chaque croisement de brins, decidons qu'a chaque croisement la couleur a reste inchangée taudis que la couleur b s'amalgame avec a et donne une nouvelle couleur $a * b$.

Proposition 3.2.1 *L'action définie dans (3.2.2) est compatible avec les relations des tresses si et seulement si $(S, *)$ est un système (AD)*

Preuve. Compatibilité avec la relation
$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ si $|i-j| > 1$
Cette compatibilité est assuré si $x*(y*z) = (x*y)*(y*z)$ est saisfaite
(voir figure (3.2.1)).

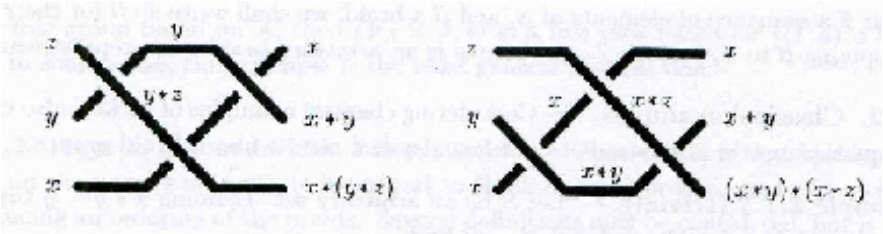

Figure 3.2.1 : Compatibilité de l'action avec les relations de définition.

Compatibilité avec la relation
$\sigma_i\sigma_j = \sigma_j\sigma_i$ si $\mid i-j\mid > 1$
$(x_1, x_2, ..., x_n)\sigma_i\sigma_j = (x_1, x_2, ...x_i * x_{i+1}, x_i, x_{i+2}, ...x_n)$
$(x_1, x_2, ..., x_n)\sigma_i\sigma_j = (x_1, x_2, ..., x_i * x_{i+1}, x_i, x_j * x_{j+1}, x_j, ..x).$
$(x_1, x_2, ..., x_n)\sigma_j\sigma_i = (x_1, x_2, ..., x_j * x_{j+1}, x_j, ..., x_n)\sigma_i$
$= (x_1, x_2, ..., x_i * x_{i+1}, x_j * x_{j+1}, x_j, ...x_n)$ alors
$(x_1, x_2, ..., x_n)\sigma_i\sigma_j = (x_1, x_2, ..., x_n)\sigma_i\sigma_j$ si $\mid i-j\mid > 1.$.
Soit $(S, o, \overline{*})$.telle que.
C'est l'extension du mot de tresses sur une suite de couleurs par:

$$\overrightarrow{x}.\sigma_i^{-1}w = (x_1, ..., x_i o x_{i+1}, x_{i+1}\overline{*}x_i, x_{i+2}, ..x_n)w \tag{3.2.3}$$

Les action (3.2.2) et (3.2.3) sont compatibles avec les relations
$\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1$
$\overrightarrow{x}.\sigma_i^{-1}(\sigma_i w) = (x_1, x_2, ..., x_i o x_{i+1}, x_{i+1}\overline{*}x_i, x_{i+2}, ..., x_n)\,\sigma_i w$
$= (x_1, x_2, ..., x_i o x_{i+1} * x_{i+1}\overline{*}x_i, x_i o x_{i+1}, x_{i+2}, ..., x_n)\,w$
$\overrightarrow{x}.\sigma_i\left(\sigma_i^{-1}w\right) = (x_1, x_2, ..., x_i * x_{i+1}, x_i, x_{i+2}, ..x_n)\,\sigma_i^{-1}w$
$= (x_1, x_2, ..., x_i * x_{i+1} o x_i, x_i\overline{*}(x_i * x_{i+1}), ..., x_n)\,w$
Alors:

$$x_i o x_{i+1} = x_i\overline{*}x_i * x_{i+1}$$
$$x_i * x_{i+1} o x_i = x_i o x_{i+1} * x_{i+1}\overline{*}x_i$$

si les identités sont satisfaites alors $x_{i+1}ox_i = x_i$

$$x_i * (x_i \overline{*} x_{i+1}) = x_i \overline{*} (x_i * x_{i+1}) = x_{i+1}$$

donc l'operation o est triviale par contre $\overline{*}$ doit être choisit de telle façon que les translations à gauche associées à $\overline{*}$ sont les translations à gauche associées à $*$. Alors $\overline{*}$existe si et seulement si les translations associées à $*$ sont bijectives

on a: $x \overline{*} y =$ l'unique z qui satisfait

$$x * z = y \tag{3.2.4}$$

■

Définition 3.2.2 *Un ensemble automorphe $(S, *)$ est un système (AD) tel que toutes les translations à gauche soient bijectives c'est à dire $(x, y), \exists!.z$.*

$$x * z = y. \tag{3.2.5}$$

Alors pour tout ensemble automophe $(S, *)$ et pour tout n les règles (3.2.2) (3.2.3) et (3.2.5) définissent une action de $\mathcal{B}_n$ sur S^n.

3.2.2 Acyclicité et systèmes (AD) ordonnables

Définition 3.2.3 *On dit qu'un système autodistributif $(S, *)$ est acylique si la relation de divisibilité à gauche dans $(S, *)$ n'a pas de cycles c'est à dire il n'y a pas d'égalité dans S de la forme:*

$$x = (....((x * x_1) * x_2) * ....) * x_p) \tag{3.2.6}$$

On dit dans ce cas que $(S, *, <)$ est un système (AD) ordonné si $(S, *)$ est un système (AD) et $<$ est un ordre sur S telle que $x < x * y$ et toujours vrai et $y < z \implies x * y < x * z$.

Proposition 3.2.2 *Un ensemble automorphe n'est jamais acyclique.*

Preuve. Soit $(S, *)$ un ensemble automorphe

On montre que l'identité $(x * x) * y = x * y$ est verifiée dans S.

On utilise l'operation symétrique $\overline{*}$ de (3.2.4) *on trouve:*

$(x * x) * y = (x * x) * (x * (x \overline{*} y)) = x * (x * (x \overline{*} y)) = x * y.$ ■

3.2.3 Retournement de mots:

On considére la fonction Υ: $\Sigma \times \Sigma \rightarrow L$ telle que L est l'ensemble de mots de tresses positifs définie par $\Upsilon(\sigma_i\ , \sigma_j) = \begin{cases} \sigma_i \ pour\ |i-j| > 1 \\ \sigma_j\sigma_i \ pour\ |i-j| = 1 \\ \varepsilon \ pour i = j \end{cases}$

Donc l'equivalence de mots de tresses est engendrée par les relations pour $i \neq j$

$$\Upsilon(\sigma_j, \sigma_i)\sigma_i = \Upsilon(\sigma_i, \sigma_j)\sigma_i$$

ce qui implique que

$$\sigma_i\sigma_j^{-1} = \Upsilon(\sigma_j, \sigma_i)^{-1}.\Upsilon(\sigma_i, \sigma_j)$$

Notation 3.2.1 *On note par $\Sigma = \{\sigma_1\ \sigma_2.....\}$.l'ensemble de l'alphabet*
On utilise $\equiv$ pour désigner l'equivalence de mots des tresses et ε pour designer l'ensemble vide

Définition 3.2.4 *On dit qu'un mot de tresse w se transforme par retournement de mot à gauche au mot $w^{'}$ si $w^{'}$ s'obtient en remplaçant dans w des facteurs de type $\sigma_i\sigma_j^{-1}$ par des facteurs correspondants $\Upsilon(\sigma_j\ , \sigma_i)^{-1}\Upsilon(\sigma_i, \sigma_j)$.*

Proposition 3.2.3 *Soit w un mot de tresse. Il existe un unique paire de mots de tresse positifs $N\ (w)$ $D(w)$ tel que chaque suite de retournement de mot à partir de w se termine dans un nombre fini d'étapes avec le mot $D\ (w)^{-1}\ N\ (w)$*

Preuve. Par le procédé si dessue

$$w = D\ (w)^{-1}N(w)$$

L'unicité**:** Le diagramme de retournement implique que le retournement de mot d'un mot donné conduit à un mot de la forme $u^{-1}v\ /\ u, v \in \mathcal{B}_n^+$ puisque en remplace $\sigma_i\sigma_j^{-1}$ par $\Upsilon(\sigma_j\ , \sigma_i)^{-1}\Upsilon(\sigma_i, \sigma_j)$.
Alors il reste a démontrer que ce processus est fini, donc il suffit de le faire pour un mot uv^{-1}, tel que $u, v \in \mathcal{B}_n^+$.
Pour $u, v \in \mathcal{B}_n^+$, on note par $\frac{u}{v}$ l'unique mot positif $u^{'}$ tel que uv^{-1} retourne à $(v^{'})^{-1}u^{'}$ pour un certain mot positif $v^{'}$.
Donc $\frac{u}{v}v = \frac{v}{u}u$ est verifié, dans ce cas $\frac{u}{v}v$ représente un commun multiple à gauche des tresses représentées par u et v dans $\mathcal{B}_\infty^+$ dans ce cas le commun multiple est le plus petit.

Ce résultat général au sujet de retournement de mot est vrai si la condition

$$((x/y)\diagup(z/y))\diagup((x/z)\diagup\ (y/z) = \varepsilon.$$

est satisfaite pour chaque triple de lettres.
Tous les résultats pour le retournement à gauche restent vrai pour le retournement à droite en remplacant les facteurs $\sigma_i^{-1}\sigma_j$ par des facteurs de la forme uv^{-1}. On obtient donc pour chaque mot de tresses deux mots de tresses positifs $\widetilde{N}\ (w)$ et $\widetilde{D}\ (w)$ tels que w est retourné à droite à $\widetilde{N}\ (w).\widetilde{D}(w)^{-1}$.
Soit w un mot de tresses on définit les applications: $N_{rl}\ (w) = \widetilde{N}\ (D\ (w)^{-1}\ N(w))$
et $D_{rl}(w) = \widetilde{D}\ (D(w)^{-1}N(w))$.

Ces applications sont bien définies car:
$w \equiv w^{'} \Rrightarrow N_{rl}\ (w) \equiv N_{rl}\ (w^{'})$ et $D_{rl}(w) \equiv D_{rl}(w^{'})$.
Ce qui nous permet de résoudre le problème de mots pour les tresses ■

3.2.4 Action des tresses sur les systèmes autodistributifs simplifiables à gauche

- – On va présenter ici l'extension de l'action de $\mathcal{B}_n^+$ sur S^n a $\mathcal{B}_n$.

Définition 3.2.5 *Un système autodistributif simplifiable à gauche est un système pour lequel les multiplications à gauche sont injectives*

Définition 3.2.6 *Soit $(S, *)$ un système AD et w un mot de tresses , $n \leq \infty$.*
On dit que $(\overrightarrow{x}, \overrightarrow{y}) \in S^n$ est une $S-$coloration pour w si les couleurs de S peuvent être attribuer pour chaque segment dans le diagramme associé à w tel que les $\overrightarrow{x}$ sont les couleurs entrées à gauche et les $\overrightarrow{y}$ sont les couleurs sorties à droite telles que les règles sont satisfaites en chaque croisement (voir figure (3.2.2))

Si w est un mot de tresses, pour toute suite $\overrightarrow{x} \in S^n$ le couple $(\overrightarrow{x}, \overrightarrow{x}w)$ est une coloration de w, et si S est automorphe le resultat reste vrai pour tout mot de tresses.

Lemme 3.2.1 *On suppose que $(S, *)$ est un système AD et u, v sont deux mots de tresses positifs alors pour toute suite $\overrightarrow{x} \in S^n$ le pair $(\overrightarrow{x}u, \overrightarrow{x}v)$ est une $S-$coloration pour $u^{-1}v$.*

Preuve. On applique les couleurs $\overrightarrow{x}$ dans la moitiée du diagramme associé à $u^{-1}v$ et on propage à gauche u^{-1} et à droite v comme suit: on obtient à gauche $\overrightarrow{x}u$ et à droite $\overrightarrow{x}v$

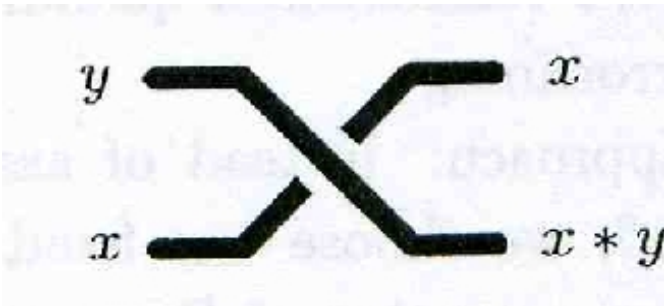

Figure 3.2.2 : Règle de coloriage

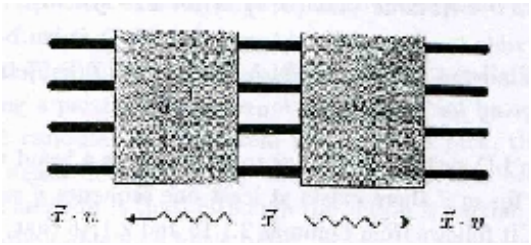

Figure 3.2.3 : compatibilité des règles de coloriage

Les règles de coloriage sont satisfaites dans chaque partie du diagramme (voir figure (3.2.3)) ■

Toute tresse peut être représenter par un mot de la forme $u^{-1}v$ avec u, v sont positifs.

Remarque 3.2.1 *La $S-$coloration d'un mot de tresses w n'est pas une $S-$coloration pour tout mot de tresses w' tel que w' est équivalent à w.*

On va utiliser maintenant le retournement de mots.

Lemme 3.2.2 *On suppose que $(S, *)$ est un système AD et on suppose que le mot de tresses w est retourné à gauche à w' et que $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration bien définie pour w', alors $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration bien définie pour w, en particulier $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration pour $D(w)^{-1}N(w)$.*

Preuve. voir [11] ■

Remarque 3.2.2 *le resultat précedent est vrai pour le retournement à droite de mots.*

Définition 3.2.7 *Si $(S, *)$ est un système AD, $\overrightarrow{x} \in S^n$ et w est un mot de tresses, on dit que $\overrightarrow{x}$ est admissible pour w s'il existe au moins une suite $\overrightarrow{y}$ telle que $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration pour w.*

Lemme 3.2.3 *On suppose que $(S,*)$ est un système AD simplifiable à gauche et $w, w^{'}$ sont deux mots de tresses équivalents.*
Alors pour chaque suite $\overrightarrow{x} \in S^n$ qui est admissible pour les deux mots il existe exactement une suite $\overrightarrow{y}$ telle que $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration pour les deux mots.

Preuve. On suppose que $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration pour w et $\left(\overrightarrow{x}, \overrightarrow{y^{'}}\right)$est une coloration pour $w^{'}$.

w,$w^{'}$ sont équivalents n'implique pas que leurs numérateurs et leurs dénominateurs sont équivalents, mais il existe $v, v^{'}$ tels que:

$$\widetilde{N}(w)v = \widetilde{N}(w^{'})v^{'}$$

$$\widetilde{D}(w)v = \widetilde{D}(w^{'})v^{'}$$

Le lemme (3.2.3) implique $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration pour $\widetilde{N}(w)\widetilde{D}(w)^{-1}$ et donc $(\overrightarrow{x}, \overrightarrow{y})$ est une $S-$coloration pour $\widetilde{N}(w)vv^{-1}\widetilde{D}(w)^{-1}$.
Par construction

$$\overrightarrow{x}.\widetilde{N}(w)v = \overrightarrow{y}.\widetilde{D}(w)v$$

Le même argument nous donne

$$\overrightarrow{x}.\widetilde{N}(w^{'})v^{'} = \overrightarrow{y^{'}}.\widetilde{D}(w^{'})v^{'}$$

et donc on a

$$\overrightarrow{y}.\widetilde{D}(w)v = \overrightarrow{y^{'}}.\widetilde{D}(w^{'})v^{'} = \overrightarrow{y^{'}}.\widetilde{D}(w)v$$

cela implique que

$$\overrightarrow{y} = \overrightarrow{y^{'}}$$

En effet on démontre par recurrence que $\overrightarrow{x}\sigma_i = \overrightarrow{x^{'}}\sigma_i$ implique que $\overrightarrow{x} = \overrightarrow{x^{'}}$.

L'hypothèse implique que

$$\overrightarrow{x_i} = \overrightarrow{x_i^{'}}$$

et

$$x_i * x_{i+1} = x_i^{'} * x_{i+1}^{'}$$

alors $x_{i+1} = x_{i+1}^{'}$ ce qui montre que $(S,*)$ est simplifiable à gauche ■

On admet la proposition suivante.

Proposition 3.2.4 *On suppose que $(S,*)$ est un système AD simplifiable à gauche .Alors pour toute famille finie de tresses $\beta_1, \beta_2, ..., \beta_m \in \mathcal{B}_n$, il existe au moins une suite $\overrightarrow{x} \in S^n$ telle que la suite $\overrightarrow{x}\beta_i$ est définie pour tout i.*

3.2.5 Tresses spéciales

Définition 3.2.8 *Pour $\beta_1, \beta_2, \in \mathcal{B}_n$, on pose*

$$\beta_1 * \beta_2 = \beta_1 sh(\beta_2)\, \sigma sh\left(\beta_1^{-1}\right) \tag{3.2.7}$$

on dit qu'une tresse est spéciale si elle est obtenue à partir de la tresse triviale 1 *on utilisant l'opération* $*$ *recursivement et sh est l'endomorphisme shift.*

Notation 3.2.2 *On note l'ensemble des tresses spéciale par $\mathcal{B}_{sp}$*

Lemme 3.2.4 *Les systèmes $(\mathcal{B}_\infty, *)$ et $(\mathcal{B}_{sp}, *)$ sont des systèmes (AD) simplifiable à gauche.*

Lemme 3.2.5 *Soit $\overrightarrow{x}$ une suite de tresses spéciales*
pour $\overrightarrow{x} \in \mathcal{B}_n^{\mathbb{N}}$ avec un nombre fini de termes $\neq 1$ on définit

$$\Pi^{sh}\left(\overrightarrow{x}\right) = \Pi_{k=1}^{\infty} sh^{k-1}(x_k) = x_1 sh(x_2)\, sh^2(x_3) \ldots \tag{3.2.8}$$

alors si $\beta \in \mathcal{B}_\infty$ et $\overrightarrow{x}.\beta$ existe, on a

$$\Pi^{sh}\left(\overrightarrow{x}.\beta\right) = \Pi^{sh}\left(\overrightarrow{x}\right).\beta \tag{3.2.9}$$

Preuve. On fait un raisonnement par recurrence sur la longueur minimal d'un mot de tresses représentant β et telle que $\overrightarrow{x}.w$ existe

le résultat est vrai si w est vide

On suppose que $w = \sigma_i w'$ si β est une tresse représentée par w' donc $\overrightarrow{x}.\sigma_i$ et $\left(\overrightarrow{x}\,\sigma_i\right).\beta'$ existent.

On trouve:
$\Pi^{sh}\left(\overrightarrow{x}.\sigma_i\right) = \Pi^{sh}\left((x_1, ..., x_i * x_{i+1}, x_{i...})\right)$
$= x_1 sh(x_2) ... sh^{i-1}(x_i * x_{i+1})\, sh^i(x_i)\, sh^{i+1}(x_{i+2}) ...$
$= x_1 sh(x_2) ... sh^{i-1}(x_i)\, sh^i(x_{i+1})\, \sigma_i sh^i(x_i)^{-1}\, sh^i(x_i)\, sh^{i+1}(x_{i+2}) ...$
$= x_1 sh(x_2) ... sh^{i-1}(x_i)\, sh^i(x_{i+1})\, \sigma_i sh^{i+1}(x_{i+2})..$
$= x_1 sh(x_2) ... sh^{i-1}(x_i)\, sh^i(x_{i+1})\, sh^{i+1}(x_{i+2}) ... \sigma_i$
$= \Pi^{sh}\left(\overrightarrow{x}\right) x_i$
comme σ_i commute avec $sh^k(x)$ pour $k \geq i+1$ on applique l'hypothèse de recurrence en déduire
$\Pi^{sh}\left(\overrightarrow{x}.\beta\right) = \Pi^{sh}\left(\overrightarrow{x}.\sigma_i\right)\beta'$
$= \Pi^{sh}\left(\overrightarrow{x}\right) x_i \beta'$
$= \Pi^{sh}\left(\overrightarrow{x}\right)\beta'$ ■

Proposition 3.2.5 *Toute tresse peut être écrite sous la forme*

$$sh^{i-1}(\beta_i^{'})^{-1}...sh(\beta_2^{'})^{-1}(\beta_1^{'})^{-1}\beta_1 sh(\beta_2)...sh^{i-1}(\beta_i) \tag{3.2.10}$$

telles que: $\beta_1^{'}, \beta_2^{'}, ..., \beta_1, \beta_2 \in \mathcal{B}_{sp}$

Preuve. On suppose que $\beta \in \mathcal{B}_\infty^+$ alors la suite $(1, 1, ...)\,\beta$ est définie puisque l'obstruction apparait seulement avec des croisements négatives elle consiste des tresses spéciales et comme les tresses spéciales sont stables par l'opération $(*)$ on suppose que $(1, 1, ...)\,\beta = (\beta_1, \beta_2, ...)$ $\Pi^{sh}((\beta, \beta, ...)) = \Pi^{sh}((1, 1, ...)\,\beta)$ c'est à dire $\beta = \beta_1 sh(\beta_2) sh^2(\beta_3)...$
et le fait que toute tresse est le quotient de deux tresses positives alors le résultat est démontré. ■

Remarque 3.2.3 *L'ensemble des tresses spéciales forme un système (AD) monogène engendré par la tresse* 1.

Définition 3.2.9 *Pour $(S, *)$ est un système binaire $x, y \in S$, on dit que x est un diviseur à gauche itérré de y et en écrit $x \sqsubset y$ s'il éxiste un certain entier p et certains éléments $z_1, z_2, ..., z_p \in S$ satisfaisont*

$$y = (...((x * z_1) * z_2) * ...) * z_p \tag{3.2.11}$$

Propriété de comparaison C_{AD}

Définition 3.2.10 *On suppose que $(S, *)$ est un système (AD) monogène, alors deux éléments x, y de S verifient au moins l'une des trois propositions $x = y$, $x \sqsubset y$, $y \sqsubset x$*

Lemme 3.2.6 *Soient β_1, $\beta_2 \in \mathcal{B}_{sp}$ telles que $\beta_1 \sqsubset \beta_2$; alors la tresse $\beta_1^{-1}\beta_2$ admet un représentant σ_1-positif.*

Preuve. Par construction il existe $\beta_1^{'}$,..., $\beta_P^{'}$ satisfaisants
$\beta_2 = (...((\beta_1 * \beta_1^{'}) * \beta_2^{'})*...) * \beta_P^{'}$ étendre le dernier produit pour donner
$\beta_{_2} = \beta_1 sh(\beta_1^{'})\sigma_1 sh(\beta_1^{"})\sigma_1...\sigma_1 sh(\beta_P^{"})$ avec
$\beta_1^{"} = \beta_1^{'}\beta_2^{'}$,$\beta_k^{"} = (...((\beta_1 * \beta_1^{'}) * \beta_2^{'})...) * \beta_k^{'})_{k+1}^{-1\beta'}$ pour $2 \leq k < p$ et $\beta_p^{"} = ((...((\beta_1 * \beta_1^{'}) * \beta_2^{'}) * ...) * \beta_p^{'})^{-1}$.
Donc la tresse $\beta_1^{-1}\beta_2$ admet un représentant qui contient p lettres en σ_1 mais pas en σ_1^{-1}. ■

Proposition 3.2.6 *La propriété C_{AD} implique la propriété C_∞ c'est à dire elle implique que toute tresse dans $\mathcal{B}_\infty$ admet un représentant σ_1-positif , σ_1-négatif ou σ_1-libre.*

Preuve. Soit $\beta \in \mathcal{B}_\infty$

La proposition (3.2.4) implique que β admet la décomposition

$sh^{i-1}(\beta_i^{'})^{-1}...sh(\beta_2^{'})^{-1}(\beta_1^{'})_1^{-1}\beta sh(\beta_2)...sh^{i-1}(\beta_i)$

telles que: $\beta_1, \beta_2, ..., \beta_1^{'}, \beta_2^{'}, ... \in \mathcal{B}_{sp}$ et propriété de comparaison (C_{AD}) un des trois cas apparait

1-$\beta_1^{'} \sqsubset \beta_1$ ce qui implique que $\left(\beta_1^{'}\right)^{-1}\beta_1$ admet un représentant σ_1-positif donc β l'admet aussi.

2-$\beta_1^{'} = \beta_1$ alors $\beta \in \mathrm{Im}\,(sh)$, donc elle a un représentant σ_1-libre.

3-$\beta_1^{'} \sqsupset \beta_1$, alors comme dans (1) β admet un représentant σ_1-négatif

Ainsi la propriété C_∞ est démontrée. ■

On démontre maintenant la propriété (C_{AD})

Preuve. Soit $\overrightarrow{I}$ une famille des identités algébriques et X un ensemble non vide, alors il existe un système algébrique S constitué d'un ensemble muni des opérations satisfaisant $\overrightarrow{I}$ tel que X engendre S et tout système $\overrightarrow{I}$ engendré par X est l'image de S par le morphisme sh en particulier il existe pour tout n un système (AD) libre de rang n qu'on note F_n ■

Les systèmes (AD) libres peuvent être décrits à partir des systèmes libres absolus ou (magam libre).

Notation 3.2.3 *Pour $1 \leq n \leq \infty$, on note par T_n le magma libre engendré par $x_1, x_2, ..., x_n$*

les éléments de T_n sont appelés parenthésages.

Définition 3.2.11 *Pour $t, t^{'} \in T_\infty$ on dit que $t^{'}$ est une $AD-$ expansion de t,respectivement $t^{'}$ est $AD-$ équivalent à t et on note $t^{'} =_{AD} t$ si on peut aller de t à $t^{'}$ par application de transformations finies en remplaçant les parenthéssages de la forme $t_1 * (t_2 * t_3)$ par les parenthésages de la forme $(t_1 * t_2) * (t_1 * t_3)$ et vice versa*

Pout tout n l'équivalence (AD) est une congruence sur T_n et $T_n/ =_{AD}$ est un système (AD) libre de rang n

Définition 3.2.12 *Soit t un parenthésage et k un entier suffisamment petit, on note par $left^k(t)$ le k^{eme} sous terme gauche de t et on a:*

$$left^0(t) = t$$

pour tout t et

$$left^k(t) = left^{k-1}(t_1)$$

pour $t = t_1 * t_2$ *et* $k \geq 1$. *Pour* $t_1, t_2 \in T_\infty$, *on dit que* $t_1 \sqsubset_{AD} t_2$,*est vrai si on a*

$$t_1^{'} = left^k(t_2^{'}) \text{ pour un ceratain } k, t_1^{'}, t_2^{'} \text{ satisfaisont } k \geq 1, t_1^{'} =_{AD} t_1, t_2^{'} =_{AD} t_2$$

Si t *un parenthésage en définit recursivement* $t^{[1]} = t$, $t^{[k+1]} = t * t^{[k]}$

Remarque 3.2.4 *Démontrer la propriété* (C_{AD}) *est équivalent à démontrer que l'une au moins des trois assertions est vrai* $t_1 \sqsubset_{AD} t_2, t_1 =_{AD} t_2$ *ou* $t_1 \sqsupset_{AD} t_2$ *pour tout parenthésages* $t_1, t_2 \in T_1$.

Lemme 3.2.7 *Pour tout parenthésage* $t_1 \in T_1$*on a* $x^{[k+1]} =_{AD} t * x^{[k]}$ *pour tout* k *suffisamment grand*

Preuve. On fait un raisonnement par recurrence sur la longueur de t.
Si $t = x$ alors par définition $x^{[k+1]} = t * x^{[k]}$.Si $t = t_1 * t_2$ et si $x^{[k+1]} =_{AD} t_1 * x^{[k]}$ et $x^{[k+1]} =_{AD} t_2 * x^{[k]}$ pour tout k suffisamment grand, alors $x^{[k+2]} =_{AD} t_1 * x^{[k+1]} =_{AD} t_1 * (t_2 * x^{[k]}) =_{AD} (t_1 * t_2) * (t_1 * x^{[k]}) =_{AD} t * x^{[k+1]}$ ■

Lemme 3.2.8 *Si* $t \in T_\infty$ *est un parenthésage tel que* $left^k(t)$ *est défini ,alors il il existe* $k^{'} \geq k$ *tel que* $left^{k^{'}}(t^{'})$ *est une AD-expansion de* $left^k(t)$

Preuve. Il suffit de démontrer le resultat quand $t^{'}$ est obtenu en remplaçant exactement un sous terme t_0 de t de la forme $t_1 * (t_2 * t_3)$ par $(t_1 * t_2) * (t_1 * t_3)$.

Si t_0 est $left^j(t)$ avec $j \leq k$ alors $left^{k+1}(t^{'})$ est égale à $left^k(t)$.

Si t_0 est $left^j(t)$ avec $j > k$ alors $left^k(t^{'})$ est une $AD-$expansion de $left^k(t)$ ■

Lemme 3.2.9 *Si* t_1 *et* t_2 *sont des parenthésages tels que* $t_1 =_{AD} t_2$, *alors ils ont une expansion commune*

Preuve. On démontre que si $t^{'}$, $t^{"}$ sont deux expansions d'un parenthésages t donc $t^{'}$, $t^{"}$ admettent une expansion AD commune.
Soit $t^{'}$ est une $k-$expansion de t si $t^{'}$ est obtenu à partir de t on applique l'identité AD au plus k fois.

Donc pour tout parenthésage t on peut définir explicitement une expansion ∂t de t qui est une expansion commune de toutes les 1-expansion de t .

Si $t^{'}$ est une expansion AD de t alors $\partial t^{'}$ est une expansion AD de ∂t. La définition du parenthésage ∂t est inductive .$\partial t = t$ si t est une variable et $\partial(t_1 * t_2)$ est obtenu en

remplaçant le variable x_i dans ∂t_2 avec le parenthésage $\partial t_1 * x_i$. Alors on montre en utilisant une recurrence qui, pour chaque k, le parenthésage $\partial^k t$ est une $AD-$expansion de toutes les k expansions du parenthésage t.

Si $t^{'}$ et $t^{"}$ sont deux AD-expansions d'un parenthésage t, alors $t^{'}$, $t^{"}$ admettent une AD-expansions, à savoir tous les parenthésages $\partial^k t$ avec k suffisamment grand. ■

Proposition 3.2.7 *(Propriété C_{AD}).*
Si $(S, *)$ est un AD -système monogène, alors deux éléments de S sont comparables par rapport à la division à gauche répétée.

Preuve. Soient t_1, $t_2 \in T_1$ deux parenthésages d'aprés le lemme (3.2.5) on a

$$x^{[k+1]} =_{AD} t_1 * x^{[k]}$$

et

$$x^{[k+1]} =_{AD} t_2 * x^{[k]}$$

Pour k suffisamment grand on fixe un k, d'aprés le lemme (3.2.7) les parenthésages $t_1 * x^{[k]}$ et $t_2 * x^{[k]}$ admettent une expansion commune t et par le lemme (3.2.6) il existe des entiers non négatifs k_1, k_2 tels que pour $i = 1, 2$ le parenrhésage $left^{k_i}(t)$ est une expansion de t_i .
Ainsi on a $t_1 =_{AD} left^{k_1}(t)$ et $t_2 =_{AD} left^{k_2}(t)$.
Alors jusqu'à échanger les indices 1et 2

$$left^{k_1}(t) \sqsubseteq left^{k_2}(t)$$

Donc $t_1 \sqsubset_{AD} t_2$ ou $t_1 =_{AD} t_2$. ■

Propriété (C_∞)

Toute tresse $\beta \in \mathcal{B}_\infty$ admet un représentant σ_1-positif σ_1-négatif ou σ_1-libre.

3.2.6 Le groupe de l'autodistributivité

Le but de cette section est de démontrer la propriété d'acyclicité.

Propriété (A_{AD}) : Il existe un système (AD) acyclique et simplifiable à gauche

Proposition 3.2.8 *Les deux assertions suivantes sont équivalentes*
1-la propriété A_{AD} implique la propriété A
2-la propriété A implique la propriété A_{AD}

Preuve. $1 \Rightarrow 2$: On suppose que $(S, *)$ est un système AD acyclique et simplifiable à gauche et soit w un mot de tresse σ_1-positif, la proposition (2.1.19) implique qu'il existe une suite de couleurs $\overrightarrow{x} \in S$ telle que $\overrightarrow{x}w$ est définie, on désigne par z_0 la couleur initiale à gauche, z_1 la couleur du brin aprés le premier croisement σ_1 (voir figure (3.2.4))

Figure 3.2.4 : Un mot σ_1-positif

Par construction z_i est le i^{eme} diviseur de z_{i+1} pour chaque i, par hypothèse la division à gauche dans $(S, *)$ n'a pas de cycle ce qui implique que $z_n \neq z_0$ et lemme (2.1.18) implique que w ne représente jamais la tresse triviale.

$2 \Rightarrow 1$: $(\mathcal{B}_\infty, *)$ est un système AD simplifiable à gauche, le lemme (2.2.6) implique que $(\beta')^{-1}\beta$ admet un représentant σ_1-positif, donc $\beta' \sqsubset \beta$ est vérifiée.
Si la relation A est vrai alors $\beta' \sqsubset \beta$ implique que $\beta' \neq \beta$ donc la division à gauche dans $(\mathcal{B}_\infty, *)$ n'a pas de cycle donc $(\mathcal{B}_\infty, *)$ est un système (AD) acyclique et simplifiable à gauche. ■

3.2.7 Géométrie de l'identité AD

Notre but ici est de démontrer que les systèmes AD sont acycliques et simplifiables à gauche ce qui montre que ses systèmes sont ordonnables, pour cela on considère les systèmes AD libres. Pour cela on considère le système monogène F_1, pour montrer que F_1 est acyclique on a besoin de démontrer la proposition suivante.

Proposition 3.2.9 *Pour $t, t' \in T_1$ les relations $t \sqsubset_{AD} t'$ et $t =_{AD} t'$ l'une exclus l'autre.*

Pour étudier le système F_1 ,on va représenter les parenthésages par des arbres binaires avec racines on représente la variable x par l'arbre réduit à sa racine, si $t_1$et t_2 sont deux parenthésages on représente $t_1 * t_2$ par l'arbre obtenu en greffant l'arbre associé à t_1 à gauche d'une nouvelle racine, et l'arbre associé à t_2 à droite.

Tout sommet d'un arbre binaire à une adresse qui est une suite finie de 0 et de 1, l'adresse de la racine est la suite vide et en s'éloignant de la racine, on passe de l'adresse d'un sommet à celui de son "succeseur" gauche en ajoutant 0 et a celle de son "successeur" droit enajoutant

1 nous avons définis la notion d'expansion d'un parenthésage cette définition se transpose aux arbres binaires.

Pour décrire la situation en considère le cas ou l'identité AD est appliqué une seule fois toujours de la gauche vers la droite, et en prenant en compte l'adresse ou elle l'est dans l'arbre correspondant.

Notation 3.2.4 *L'opération* $(AD)_\alpha$ *consiste à appliquer l'identité AD à l'adresse* α *et* g_{AD} *le monoide engendré par* $(AD)_\alpha$ *et ses inverses .*

Le lemme admet suivant nous établit les relations entre les $(AD)_\alpha$:

Lemme 3.2.10 *Pour toute adresse* α, β, γ *les relations suivantes sont vérifiées dans* g_{AD}
1-$(AD)_{\alpha 0\beta}(AD)_{\alpha 1\gamma} = (AD)_{\alpha 1\gamma}(AD)_{\alpha 0\beta}$
2-$(AD)_{\alpha 0\beta}(AD)_\alpha = (AD)_\alpha (AD)_{\alpha 00\beta}(AD)_{\alpha 10\beta}$
3-$(AD)_{\alpha 10\beta}(AD)_\alpha (AD)_\alpha = (AD)_\alpha (AD)_{\alpha 01\beta}$
4-$(AD)_{\alpha 11\beta}(AD)_\alpha = (AD)_\alpha (AD)_{\alpha 11\beta}$
5-$(AD)_{\alpha 1}(AD)_\alpha (AD)_{\alpha 1}(AD)_{\alpha 0} = (AD)_\alpha (AD)_{\alpha 1}(AD)_\alpha$.

Notation 3.2.5 *On note par* G_{AD} *le groupe engendré par une suite infinie de générateurs* τ_α *indexés par les adresses telle que les relations du lemme précédent sont satisfaites.*

Remarque 3.2.5 *Le groupe des tresses* $\mathcal{B}_\infty$ *est le groupe quotient du groupe* G_{AD}*. En effet, appliquons* τ_{1^n} *à* σ_{n-1} *et s'écrouler tous les générateurs* τ_α *tel que l'adresse* α *contient au moins un* 0 *définit un morphisme surjectif, comme peut être vu en comparant les relations dans lemme (3.2.8) avec les relations de la tresse. L'existence de cet morphisme exprime le lien entre les tresses et les systèmes AD.*

Soit g^+_{AD} (respectivement G^+_{AD}) le monoide de g_{AD} (respectivement G_{AD}) engendré par les éléments $(AD)_\alpha$ (respectivement τ_α) le lemme (3.2.8) implique que g^+_{AD} est le quotient de G^+_{AD}, donc l'action de g^+_{AD} sur les parenthésages induit une action de G^+_{AD}.

Les modèles des parenthésages.

Définition 3.2.13 *Pour* $t \in T_1$*, le modèle de* t *est l'élément* $[t]$ *de* G_{AD} *défini inductivement par* $[x] = 1$ *et* $[t_1 * t_2] = [t_1]\, sh_1([t_2])\, \tau_\varepsilon sh_1\left([t_1]^{-1}\right)$ *.Notre but est de démontrer que les relations* $t \sqsubset_{AD} t'$ *et* $t =_{AD} t'$ *l'une exclus l'autre , pour cela en va travailler dans* G_{AD} *en utilisant* $[t]$ *en tant que contre partie de* t *.Cet argument nous permet de démontrer la propriété AD . Le lemme (3.2.5) implique que pour tout* $t \in T_1$ *la relation* $x^{[k+1]} =_{AD}$

$t * x^{[k]}$ pour k suffisamment grand .Par construction il existe un élément f de G_{AD} tel que $f\left(x^{[k+1]}\right) = t * x^{[k]}$ et la preuve du lemme (3.2.5) nous donne une définition explicite de f .En effet on suppose que $t = t_1 * t_2$ et que $f_1\left(x^{[k+1]}\right) = t_1 * x^{[k]}$ et $f_2\left(x^{[k+1]}\right) = t_2 * x^{[k]}$.
Pour $g \in g_{AD}$, $sh_1(g)$ est la version shift de g qui consiste à appliquer g à droite au sous terme, donc on a une suite:

$$x^{[k+1]} \longrightarrow t_1 * x^{[k]} \longrightarrow t_1 * \left(t_2 * x^{[k-1]}\right) \longrightarrow (t_1 * t_2) * \left(t_1 * x^{[k-1]}\right) \longrightarrow t * x^{[k]}$$

Alors l'opérateur $\left(f_1.sh_1(f_2).AD_\varepsilon sh_1\left(f_1^{-1}\right)\right)\left(x^{[k+1]}\right) = t * x^{[k]}$.

On obtient le resultat admet suivant:

Lemme 3.2.11 *Pour $t \in T_1$, on définit χ_t dans g_{AD} inductivement par $\chi_x = 1$ et*

$$\chi_{t_1 * t_2} = \chi_{t_1}.sh_1\left(\chi_{t_2}\right).AD_\varepsilon sh_1\left(\chi_{t_1}^{-1}\right)$$

Alors pour tout t et pour k suffisamment grand

$$\chi_t\left(x^{[k+1]}\right) = t * x^{[k]}$$

Notation 3.2.6 *On note par sh_1 (respectivement sh_0) l'endomorphisme à gauche de G_{AD} tel que :$sh_1(\tau_\alpha) = \tau_{1\alpha}$ (respectivement $sh_0(\tau_{0\alpha}) = \tau_{1\alpha}$) pour tout α.*

Lemme 3.2.12 *1-Si $t =_{AD} t'$ est satisfaite alors $[t]^{-1}.\left[t'\right]$ appartient au sous groupe de G_{AD} engendré par les $\tau_{0\alpha}$.*
2-Si $t \sqsubset_{AD} t'$ est satisfaite ,alors $[t]^{-1}.\left[t'\right]$ admet une expansion ou τ_ε apparait mais τ_ε^{-1} n'apparait pas.

Preuve. 1-Si $t =_{AD} t'$ est satisfaite alors il existe $f \in g_{AD}$ / $f(t) = t'$ donc $sh_0(f)\left(t * x^{[k]}\right) = t' * x^{[k]}$.
Alors l'opérateur $\chi_t^{-1}.\chi_{t'}\left(t * x^{[k]}\right) = t' * x^{[k]}$ et cela qui implique que $\chi_t^{-1}.\chi_{t'}$ coincide avec $sh_0(f)$ en au moins un parenthésage qui coincide avec $sh_0(f)$ en tout parenthésage ou il est défini.
Si cette axiomatisation est vrai alors l'élément $[t]^{-1}.\left[t'\right]$ de G_{AD} coincide avec un certain élément de la forme $sh_0(a)$, donc $[t]^{-1}.\left[t'\right]$ appartient au sous groupe $sh_0(G_{AD})$ de G_{AD}.
La verification correspondant à $f = AD_\varepsilon$ est $sh_0(AD_\varepsilon) = 1$ puisque $AD_\varepsilon(t) = t$.

2-On applique (1) pour demontrer la relation pour $t \sqsubset t'$, et on fait la même pour $t' = t * t_0$, comme une énumération alors on a le résultat recherché:
$[t]^{-1}.\left[t'\right] = [t]^{-1}.[t * t_0] = [t]^{-1}.[t].sh_1([t_0])\tau_0 sh_1\left([t]^{-1}\right) = sh_1([t_0])\tau_0 sh_1\left([t]^{-1}\right)$ ■

Construction d'un préordre sur G_{AD}

Par définition un parenthésage $t^{'} \in T_{\infty}$ est une expansion AD d'un autre parenthésage t si $t^{'}$ est l'image de t dans g_{AD}^{+} on peut dire que tout élément dans g_{AD} est écrit sous la forme fg^{-1} avec $f, g \in g_{AD}^{+}$ .Ce resultat est vrai le groupe G_{AD} c'est à dire tout élément du groupe G_{AD} s'écrit sous la forme ab^{-1} avec a, $b \in G_{AD}^{+}$

Alors le lemme (2.2.12) nous assure que si $t^{'}$ est une expansion AD de t alors pour tout k tel que t a un $left^{k}(t)$, il existe $k^{'}$ tel que $left^{k^{'}}(t)$ de $t^{'}$ est une expansion AD de $left^{k}(t)$ de plus il existe deux applications

$$\delta : \mathbb{N} \times g_{AD}^{+} \to \mathbb{N}$$

et

$$\pi : g_{AD}^{+} \times \mathbb{N} \to g_{AD}^{+}$$

telles que pour tout $f \in g_{AD}^{+}$ tout parenthésage et tout k suffisamment petit on a

$$left^{\delta(k,f)}(t.f) = left^{k}(t).\pi(f,k)$$

Le lemme suivant est une conséquence de ce qui précede

Lemme 3.2.13 *Il existe deux applications*

$$d : \mathbb{N} \times G_{AD}^{+} \to \mathbb{N}$$

et

$$p : G_{AD}^{+} \times \mathbb{N} \to G_{AD}^{+}$$

telles que: $\forall\ a \in G_{AD}^{+}$*, pout tout terme* t*, et pour tout* k *suffisamment petit on a*

$$left^{d(k,a)}(t.a) = left^{k}(t).p(a,k)$$

Preuve. de la proposition (3.2.9)

On va introduire deux sous ensembles de G_{AD} comme suit :Soit c un élément de G_{AD} appartient à $P_{<}$ (respectivement à $P_{=}$) s'il existe une décoposition $c = ab^{-1}$ avec $a, b \in G_{AD}^{+}$ qui satisfait $d(1,b) < d(1,a)$ (respectivement $d(1,b) = d(1,a)$), les deux sous ensembles sont disjoints et stable par le produit, il est nécessaire de démontrer que si un élément $c \in G_{AD}$ se décompose $c = ab^{-1} = a^{'}(,)^{-1}$ avec $a, b, a^{'}, b^{'} \in G_{AD}^{+}$ et on a $d(1,b) < d(1,a)$, alors on a $d(1,b^{'}) < d(1,a^{'})$.

Sous les mêmes hypothèses on a $ag = a^{'}g^{'}$ et $bg = b^{'}g^{'}$ pour certains $g, g^{'} \in G_{AD}^{+}$ ce qui

implique que $d(1,ag) = d(1,a^{'}g^{'})$ .Comme les applications $d(.,g)$ et $d(.,g^{'})$ sont croissantes $d(1,b) < d(1,a)$ implique que $d(1,b^{'}) < d(1,a^{'})$,alors on peut démontrer que $P_{=}$ est stable par les inverses, et on démontre les inclusions

$$P_{=}.P_{<} \subseteq P_{<}$$

et

$$P_{<}.P_{=} \subseteq P_{<}$$

Ainsi la relation $c^{-1}c^{'} \in P_{<} \cup P$ définit un un préordre sur G_{AD} .On considère maintenant les générateurs τ_{α} , premièrement on décompose τ_{ε} comme suit $\tau_{\varepsilon} = \tau_{\varepsilon}.1^{-1}$ et on trouve $d(1,1) = 1 < d(1,\tau_{\varepsilon}) = 2$, donc $\tau_{\varepsilon} \in P_{<}$ d'autre part on a pour tout chaque α.

$$d(1,1) = 1 = d(1,\tau_{0\alpha}) = d(1,\tau_{1\alpha})$$

Alors

$$\tau_{0\alpha}, \tau_{1\alpha} \in P_{=}$$

maintenant si $c \in sh_0(G_{AD}) \subset G_{AD}$ et par le calcul précédent $c \in P_{=}$ c'est à dire si c admet une expression tel que τ_{ε} apparait mais τ_{ε}^{-1} n'apparait pas, alors $c \in P_{<}$ alors on conclut que les deux cas l'un est exclus l'autre. ■

Proposition 3.2.10 *Le système libre F_1 est acyclique et simplifiable à gauche.*

Preuve. La proposition (2.2.3) implique que F_1 est acyclique ,il reste à démontrer que F_1 est simplifiable à gauche c'est à dire que pour t_1,$t_2 \in T_1$.$t*t_1 =_{AD} t*t_2$ implique $t_1 =_{AD} t_2$ pour tout t, mais la propriété C_{AD} est vrai, alors $t_1 \neq t_2$ implique qu'au moins l'une des

$$t_1 \sqsubset_{AD} t_2$$

ou

$$t_2 \sqsubset_{AD} t_1$$

est vrai, donc

$$t * t_1 \sqsubset_{AD} t * t_2$$

ou

$$t * t_2 \sqsubset_{AD} t * t_1$$

ce qui contredit la proposition (2.2.3) . ■

Corollaire 3.2.1 *Il existe un système libre AD acyclique et simplifiable à gauche*

Caractérisation des tresses ordonnables.

On a vu que les systèmes AD libres sont acycliques, la proposition suivante nous assure que ces systèmes sont aussi ordonnables .

Proposition 3.2.11 *Tout système AD libre est ordonnable et réciproquement tout système AD ordonnable est libre.*

Preuve. On va traiter le cas de F_1, la propriété AD nous assure que la relation $\sqsubset_{AD}$ sur T_1 induit une relation d'ordre $<$ sur F_1 qui est transitive , donc est un ordre pariel , de plus par définition $x < x * y$ est vrai et on utilise l'identité AD on a $y < z$ implique $x < x * z$, la propriété C_{AD} assure que l'ordre partiel $<$ est linéaire donc $(F_1, <)$ est un système AD ordonnable .Réciproquement supposons que $(S, <)$ est un système AD monogène ordonnable. Par définition il existe une surjection canonique $\pi : F_1 \longrightarrow S$ et la relation $x < y$ est vrai dans F_1 si et seulement si $y = (...((x * z_1) * z_2) * ...z_p))$ pour un certain p et $z_1, ..., z_p \in F_1$ implique que $\pi(y) = (...((\pi(x) * \pi(z_1)) * \pi(z_2)) * ...\pi(z_p))$ alors: $\pi(x) < \pi(y)$ dans S est vrai ce qui montre que π est croissant car $x < y$ implique $\pi(x) < \pi(y)$ donc π est un isomorphisme. ■

Alors les deux propriété C_{AD} et A_{AD} nous assurent l'existence d'un ordre sur les tresses.

3.3 Ordre sur les tresses (méthode de la réduction des poignées)

Dans cette section nous présentons une autre technique différente au autres techniques due à Dehornoy c'est une méthode combinatoire et qui mène aussi à une autre solution du problème de mots.

Soit w un mot de tresse non vide qui n'est pas ni σ-positif ni σ-négatif si i est le plus petit indice tel que $\sigma_i^{\pm}$ apparait dans w alors σ_i et σ_i^{-1} apparaient dans w alors w contient un mot de la forme

$$\sigma_i^e sh^i(\mu)\,\sigma_i^{-e} \text{ avec } e = \pm 1 \tag{3.3.1}$$

sh est l'endomorphisme shift $/sh(\sigma_i) = \sigma_{i+1}$

Définition 3.3.1 *Le mot defini dans 3.3.1 est appelé σ_i-poignée. Ainsi chaque mot de tresse qui n'est σ_i-positif ni σ_i-négatif; doit contenir une σ_i-poignée (voir figure (3.3.1))*

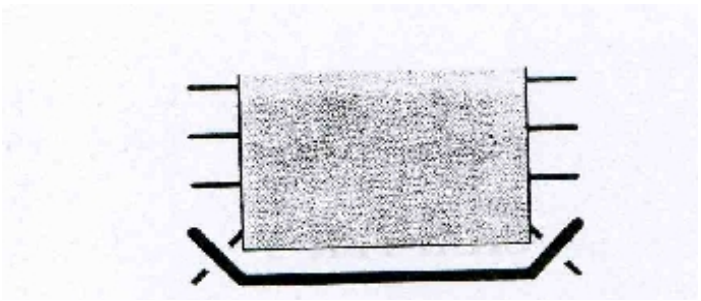

Figure 3.3.1 : Une σ_1 poignée

3.3.1 Réduction de poignées

La réduction d'une poignée est le remplacement de la poignée par un autre sous mot représentant le même élément de $\mathcal{B}_n$, par exemple reduire une σ_1 poignée $\sigma_1^e w \sigma_1^{-e}$

- Détruire les $\sigma_1^{\pm}$ du début et de la fin,

-Remplacer chaque $\sigma_2^{\pm}$ de w par $\sigma_2^{-e}\sigma_1^{\pm}\sigma_2^e$

(voir figure (3.3.2))

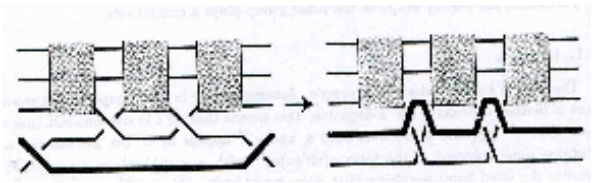

Figure 3.3.2 : Réduction de poignée

On appelle cette transformation la réduction de poignée on peut itérer la réduction de poignée jusqu'il y a pas de poignée si ce processus converge, alors par construction le mot final ne contient aucune poignée.

Donc il est soit σ-positif soit σ-négatif ou σ-libre .

Définition 3.3.2 *1- Une poignée $\sigma^e \upsilon \sigma_i^{-e}$ est dit permise si le mot υ ne contient pas de σ_{i+1}-poignée.*

2- On dit que le mot w' est obtenu à partir de w par réduction de poignée par une seule étape si:

w est une σ_i-poignée permise $w = \sigma_i^l \upsilon \sigma_i^{-l}$

et w' est obtenu à partir de w par l'homomorphisme au dernière poignée.

$\sigma_i^{\pm 1} \to \varepsilon$,$\sigma_{i+1}^{\pm 1} \to \sigma_{i+1}^{-e}\sigma_i^{\pm 1}\sigma_{i+1}^e$

$\sigma_k^{\pm 1} \to \sigma_k^{\pm 1}$ *pour* $k \geq i+2$

3- On dit que $w^{'}$ *est obtunable de* w *par* m*-étapes de réduction de poignée s'il existe une suite de longueur* $(m+1)$ *de* w *par* m*-étapes de réduction de poignée de* w *à* $w^{'}$ *tel que chaque terme est obtunable du terme précédent par une seule étape de réduction de poignée.*

La forme générale d'une σ_i*-poignée est*

$\sigma_i^e \upsilon_0 \sigma_{i+1}^{d_1} \upsilon_1 \sigma_{i+1}^{d_2} ... \sigma_{i+1}^{d_k} \upsilon_k \sigma_i^{-e}$ / $d_j = \pm 1$ $\upsilon_j \in sh^{i+1}(\mathcal{B}_\infty)$

dire que cette poignée permise une quantité équivaux tous les exposants d_j *ont une valeure commune* d.

Alors réduire la poignée $\Longleftrightarrow$ *remplcer cette poignée par*

$\upsilon_0 \sigma_{i+1}^{-e} \sigma_i^d \sigma_{i+1}^e \upsilon_1 \sigma_{i+1}^{-e} \sigma_i^d \sigma_{i+1}^e ... \sigma_{i+1}^{-e} \sigma_i^d \sigma_{i+1}^e \upsilon_k$

On fait bouger le premier et le dernier $\sigma_i^{\pm 1}$ *et on remplace chaque* σ_{i+1}^d *par* $\sigma_{i+1}^{-e} \sigma_i^d \sigma_{i+1}^e$.

Lemme 3.3.1 *1- La réduction de poignée transforme un mot* w *à un mot* $w^{'}$ *équivalent.*
2- Si w *ne contient pas de poignée alors* w *est soit* σ*-positif ou soit* σ*-négatif.*

Preuve. voir la définition ■

3.3.2 Convergence de la méthode de réduction de poignée.

Définition 3.3.3 *On dit qu'un mot de tresse* w *admet un largeur* n *si la différence entre le plus petit et le plus grand indice* i *tel que* σ_i *ou* σ_i^{-1} *se présente dans* w *est* $(n-2)$. *Le largeur de* w *est la taille du plus petit interval qui contient les idices de tous les brins tressés dans* w.

La proposition suivante nous assure la convergence de la réduction

Proposition 3.3.1 *Soit* w *un mot de tresse de longueur* l *et de largeur* n. *Alors toute suite de réduction de poignée de* w *converge au plus en* $2^{n^4 l}$ *étapes.*

On va démontrer cette proposition au plus tard

Corollaire 3.3.1 *Chaque mot de tresse* w *est équivalent à certain mot* $w^{'}$ *qui est soit* σ*-négatif, soit* σ*-positif ou* σ*-libre.*

Preuve. 1- Si w n'est une σ-poignée, alors d'après le théorème de Dehornoy w est soit σ-positif , σ-négatif ou σ-libre .
2- Si w est une σ-poignée comme la méthode de réduction de poignée converge
Alors après un nombre fini d'étapes on n'a pas de poignée donc w est soit σ-positif, σ-négatif ou σ-libre . ■

Proposition 3.3.2 *Soit w un mot de tresse $\beta \in \mathcal{B}_\infty$ est représentée par w alors*
1- $\beta = 1 \Longleftrightarrow w = \varepsilon$
2- $\beta > 1 \Longleftrightarrow w$ *est σ-positif.*

Preuve. Voir définition ■

Corollaire 3.3.2 *Soient* $\beta_1, \beta_2 \in \mathcal{B}_n$.
$\beta_1 < \beta_2$ *est vrai* $\Longleftrightarrow$ *chaque suite de réduction de poignée d'une expression* $\beta_1^{-1}\beta_2$ *se termine avec un mot σ-positif.*

Définition 3.3.4 ***Valeure absolue d'une tresse***
Soit $\Sigma = \{\sigma_1, \sigma_2, ...\}$
Υ *une fonction telle que :*
$\Upsilon : \Sigma \times \Sigma \rightarrow \{$*mot de tresse positif*$\}$
telle que :

$$\Upsilon(\sigma_i, \sigma_j) = \begin{array}{c} \sigma_i \ Pour \ |i-j| > 1 \\ \sigma_j\sigma_i \ Pour \ |i-j| = 1 \\ \varepsilon \ Pour \ i = j \end{array} \tag{3.3.2}$$

L'équivalence de mot de tresse est engendré par les relations

$$\Upsilon(\sigma_j\ ,\ \sigma_i)\,\sigma_i = f(\sigma_i,\ \sigma_j)\,\sigma_j \tag{3.3.3}$$

On pose

$$\begin{aligned} \Upsilon(\sigma_j,\ \sigma_i) &= D(\omega) \\ \Upsilon(\sigma_i,\ \sigma_j) &= N(\omega) \end{aligned} \tag{3.3.4}$$

Pour tout mot de tresse w , $\exists!\,(D(w), N(w))$ *de mots de tresse tel que w est retourné à gauche à* $D(w)^{-1} N(w)$
L'équivalence:

$$w \equiv D(w)^{-1} N(w) \equiv \tilde{N}(w)\,\tilde{D}(w)^{-1} \tag{3.3.5}$$

implique

$$N(w)\,\tilde{D}(w) \equiv D(w)\,\tilde{N}(w) \tag{3.3.6}$$

tel que $\tilde{N}(w)\,\tilde{D}(w)^{-1}$ *est le retournement à droite de w*
1-Soit w un mot de tresse la valeur absolue $|w|$ de w est la tresse positive représenté par $D(w)\,\tilde{N}(w)$.

2-β une tresse positive le graphe de Cayley de β est le graphe fini orienté indexé $\Gamma(\beta)$ défini comme suit
Les sommets sont les diviseurs à gauche de β, et il existe une arète σ_i qui commence de β_1 et qui se termine en β_2 si $\beta_2 = \beta_1\sigma_i$ est vérifiée.
3- On suppose que Γ est un fragment du graphe de Cayley de $\mathcal{B}_\infty$ et β_0 est un sommet de Γ , w un mot de tresse; on dit que w est tracé dans Γ à partir de β_0 si ω soit vide; $w = \sigma_i\upsilon$ ou $w = \sigma_i^{-1}\upsilon$ et il y a une arète indexé σ_i de β_0 à un autre sommet $\beta_0^{'}$ (resp de $\beta_0^{'}$ à β_0) dans Γ et υ est tracé à partir de β_0 dans Γ

Lemme 3.3.2 *.Soit β une tresse positive alors l'ensemble de tous les mots tracés dans $\Gamma(\beta)$ à partir d'un point donné est stable par le retournement de mots à gauche et à droite.*

Preuve. On considère le retournement à gauche on suppose qu'un certain mot $v\ \sigma_i\sigma_j^{-1}v'$ est tracé de β_0 dans $\Gamma(\beta)$ et on va démontrer que le mot : $\upsilon\Upsilon(\sigma_j,\sigma_i)^{-1}\Upsilon(\sigma_i,\sigma_j)\upsilon'$ est tracé de β_0 dans $\Gamma(\beta)$. Alors soit μ un mot de tresse positif qui representé β_0 par hypothèse il existe $\mu, \mu^{'}$ deux mots de tresse positifs tels que $\mu\sigma_i$ et $\mu^{'}\sigma_j$ sont tracés de 1 dans $\Gamma(\beta)$, l'équivalence $\mu\sigma_i \equiv \mu^{'}\sigma_j$ est satisfaite et on a de plus $\mu \equiv \mu_0\upsilon$.
Le plus petit commun multiple existe dans $\mathcal{B}_\infty^+$ [15]
$\mu\sigma_i \equiv \mu^{'}\sigma_j$ implique $\exists\mu^{"}$ un mot de tresse positif qui satisfait:

$$\begin{gathered}\mu \equiv \mu^{"}\Upsilon(\sigma_j,\sigma_i)\\ \text{et}\\ \mu^{'} \equiv \mu^{"}\Upsilon(\sigma_i,\sigma_j)\end{gathered} \tag{3.3.7}$$

Par définition du graphe de Cayley de β les mots $\mu^{"}\Upsilon(\sigma_j,\sigma_i)\sigma_i$ et $\mu^{"}\Upsilon(\sigma_i,\sigma_j)\sigma_j$ sont tracés dans $\Gamma(\beta)$ et puisqu'ils sont équivalents à $\mu\sigma_i$, cela montre que les arètes $\Upsilon(\sigma_j,\sigma_i)^{-1}$ et $\Upsilon(\sigma_i,\sigma_j)$ ont besoin pour completer leurs chemins indexés $v\Upsilon(\sigma_j,\sigma_i)^{-1}\Upsilon(\sigma_i,\sigma_j)\upsilon'$ de β_0 sont dans $\Gamma(\beta)$.
L'argement et lui même pour le retournement à droite (voir figure (3.3.3))

Définition 3.3.5 *On dit que deux mots de tresse w et $w^{'}$ sont positivement (respectivement négativement) équivalents si en peut transformer w à $w^{'}$ en utilisant les relations :*

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \ \textit{Pour}\ |i-j| = 1 \tag{3.3.8}$$

ou $\sigma_i^{-1}\sigma_j^{-1}\sigma_i^{-1} = \sigma_j^{-1}\sigma_i^{-1}\sigma_i^{-1}$ mais pas de relations de type $\sigma_i\sigma_i^{-1} = 1$.

■

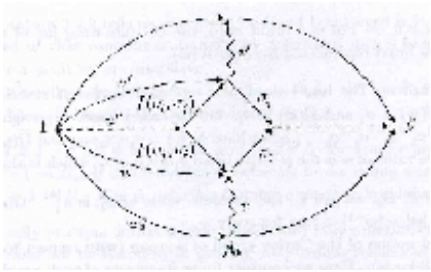

Figure 3.3.3 : Stabilité des mots sous le retournement à gauche

Lemme 3.3.3 *Soit β une tresse positive; l'ensemble de tous les mots tracés dans $\Gamma(\beta)$ à partir d'un point donné est stable sous l'équivalence positive (respectivement négative).*

Preuve. On suppose que $\upsilon\sigma_i\sigma_{i+1}\sigma_i\upsilon'$ est tracé dans $\Gamma(\beta)$ d'un point β_0, soit μ_0 un mot positif qui représente β_0

Par définition il existe un mot positif μ tel que $\mu\sigma_i\sigma_{i+1}\sigma_i$ est tracé de 1 dans $\Gamma(\beta)$.
et $\mu_0\upsilon \equiv \mu$ soit vérifiée.
On a:$\mu\sigma_i\sigma_{i+1}\sigma_i$ est positivement égal à $\mu\sigma_{i+1}\sigma_i\sigma_{i+1}$ donc, il est tracé de 1 dans $\Gamma(\beta)$ et par conséquent $\upsilon\sigma_{i+1}\sigma_i\sigma_{i+1}$ est tracé de β_0 dans $\Gamma(\beta)$

Dans le cas négatif (équivalence négative) il suffit d'inverser l'orientation. ■

Lemme 3.3.4 *Soit w un mot de tresse tout mot peut être obtenir à partir de w en utilisant le retournement à droite (à gauche). ou l'équivalence positive (négative) est tracé dans $\Gamma(|w|)$ à partir de $\overline{D(w)}$.*

Preuve. Les deux lemmes précédents assurent que tout mot obtenu à partir de w par le retournement à gauche (à droite) ou l'équivalence positive (négative) est tracé dans $\Gamma(|w|)$ à partir de $\overline{D(w)}$.Il reste à montré que w lui même est tracé dans $\Gamma(|w|)$ à partir de $\overline{D(w)}$; pour cela on utilise un raisonnement par recurrence sur la longueur de w.On suppose que le résultat est vrai pour w et on considère les mots $w\sigma_i$ et $w\sigma_i^{-1}$ succéssivement

1- $D(w\sigma_i) = D(w)$
2- $N(w\sigma_i) = N(w)\,\sigma_i$
3- $\tilde{N}(w\sigma_i) = \tilde{N}(w)\,\tilde{N}\left(\tilde{D}(w)^{-1}\,\sigma_i\right)$
4- $\tilde{D}(w\sigma_i) = \tilde{D}\left(\tilde{D}(w)^{-1}\,\sigma_i\right)$

Donc:

$$\begin{aligned} |w\sigma_i| &= D(w\sigma_i)\,\tilde{N}(w\sigma_i) \\ &= \underline{D(w).\tilde{N}(w)}.\tilde{N}\left(\tilde{D}(w)^{-1}\sigma_i\right) \\ &= |w|\,\tilde{N}\left(\tilde{D}(w)^{-1}\sigma_i\right) \end{aligned} \tag{3.3.9}$$

Alors :$\Gamma(|w|)$ est un sous graphe initial de $\Gamma(|w\sigma_i|)$
donc l'hypothèse de récurrence implique que w est encore tracé de $\overline{D(w)}$ dans $\Gamma(|w\sigma_i|)$ .Pour démontrer que $w\sigma_i$ est tracé dans $\Gamma(|w\sigma_i|)$, il reste à vérifier que l'arète final σ_i est tracé dans le graphe $\overline{N(w)}$.c'est à dire le bord final σ_i est tracé dans le graphe du point final du chemin w de $\overline{D}(w)$ qui est $\overline{D(w)\,w}$.et puisque la méthode de réduction du poigné converge alors $|w\sigma_i|$ est representée par $N(w)\,\sigma_i.\overline{D(w\sigma_i)}$ qui est le résultat recherché, pour le cas de $w\sigma_i^{-1}$ on utilise la figure à droite. ■

Lemme 3.3.5 *Soient w, w' deux mots de tresses. On suppose que w' est obtenu de w par réduction du poigné, donc on peut transformer w à w' en utilisant le retournement de mot à gauche, à droite ou l'équivalence négative, positive.*

Preuve. On va montrer que pour $\upsilon_0, ..., \upsilon_k \in sh^{i+1}(\mathcal{B}_\infty)$ on peut aller de

$$\sigma_i^l \upsilon_0 \sigma_{i+1}^d \upsilon_1 ... \sigma_{i+1}^d \upsilon_k \sigma_i^{-l} \tag{3.3.10}$$

à

$$\upsilon_0 \sigma_{i+1}^{-l} \sigma_i^d \sigma_{i+1}^l \upsilon_1 \sigma_{i+1}^{-l} ... \sigma_{i+1}^{-l} \sigma_i^d \sigma_{i+1}^l \upsilon_k \tag{3.3.11}$$

en utilisant le retournement de mot à gauche, à droite ou l'équivalence positive négative.On suppose que:$e = 1$ et $d = -1$
On peut faire une réduction du poigné en bougeant le dernier σ_i à droite
Premièrement on transforme $\sigma_i \upsilon_0$ à $\upsilon_0 \sigma_i$ par une suite de retournement de mots à gauche (pour le cas des lettres négatives) et l'équivalence positive (pour le cas des lettres positives). Alors, on peut trouver le modèle $\sigma_i \sigma_{i+1}^{-1}$ qui vient de $\sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_{i+1}\sigma_i$ par retournement à gauche, donc on a transformer le mot initial à

$$\upsilon \sigma_{i+1}^{-1} \sigma_i^{-1} \sigma_{i+1} \sigma_i \upsilon_1 ... \upsilon_{k-1} \sigma_{i+1}^{-1} \upsilon_k \sigma_i^{-1} \tag{3.3.12}$$

Après k suite de réduction du poignée, et le dernier retournement à gauche pour supprimer le modèle $\sigma_i \sigma_i^{-1}$, on atteind la forme (3.3.11) .
Dans le cas $e = -1$ et $d = 1$ en utilise le retournement à droite avec l'équivalence négative et dans le cas ou e et d ou le même signe, on utilise la même procédure en bougeant σ_i^{-e} à gauche. ■

Définition 3.3.6 *Soit w un mot de tresses. La hauteur h de w est le nombre maximal sur tous les i des lettres σ_i qui se pésentent dans un mot positif tracé dans $\Gamma(|w|)$*

Lemme 3.3.6 *On suppose que la propriété d'acyclicité est vraie, et soit w un mot de tresse de longueur l et de largeur n.*
Alors la hauteur h de w est majorée par

$$(n-1)^{l\frac{n(n-1)}{2}} \tag{3.3.13}$$

Preuve. Soit μ un mot de tresse tracé dans $\Gamma(|w|)$; tel que σ_i^{-1} ne se présente pas on exige que les différentes lettres σ_i qui se présentent dans μ corresponds au differentes arètes dans $\Gamma(|w|)$.Dire que la même arète est se rencontré deux fois ségnifi que certain chemin dans $\Gamma(|w|)$ contient au moins une arète indexé σ_i; mais pas d'arète indexé σ_i^{-1}.c'est à dire un certain mot qui contient au moins une lettre σ_i mais pas de σ_i^{-1} doit représenter la tresse triviale, ce qui est contraduction avec la propriété d'acyclicité.Ainsi le nombre de lettres σ_i dans μ est majoré par le nombre de lettres σ_i dans μ est majoré par le nombre d'arète dans $\Gamma(|w|)$
Soit S_n l'ensemble de tous les brins du mot de tresse positif qui représente les diviseurs de Δ_n.

$$\Delta_n = (\sigma_1\sigma_2...\sigma_{n-1})...(\sigma_1\sigma_2)(\sigma_1) \tag{3.3.14}$$

Garside a démontré que S_n est stable par le commun multiple à gauche et à droite voir [15] cette propriété est vraie par le retournement de mot à gauche et à droite.c'est à dire $\mu, \upsilon \in S_n$.Le retournement de $\mu\upsilon^{-1}$ à gauche se termine avec un mot $\left(\upsilon'\right)^{-1}\mu'$; tels que : $\mu', \upsilon' \in S_n$ .Par recurence on montre que s'il existe q lettres négatives dans w , alors $D(w)$ peut être décomposer au produit de q mots dans S_n , et de même s'il existe p lettres positives dans w alors $\tilde{N}(w)$ se décompose au produit de p lettres dans S_n, donc $|w| = D(w)\tilde{N}(w)$ est le produit de $p+q=l$ diviseurs de Δ_n.la longueur de Δ_n est majoré par $\frac{n(n-1)}{2}$ et par conséquent, la longueur de $|w|$ est au plus $l.\frac{n(n-1)}{2}$.
Maintenant au plus $(n-1)$ arètes commencent d'une sommet donné dans le graphe de Cayley du mot $\sigma_1^{\pm1}\sigma_2^{\pm1}...\sigma_{n-1}^{\pm1}$.
Alors dans le graphe de Cayley un mot de longueur L il n'y a que $(n-1)^L$ arètes c'est à dire $(n-1)^{l\frac{n(n-1)}{2}}$. ■

On considère maintenant une suite de réduction de poignée $(w_0 = w, w_1, ..., w_k, ...)$ de w le nombre de σ_1-poignée dans w_i n'est plus grand que le nombre de σ_1-poignée dans w_0.comme la réduction d'une σ_1-poignée laisse au plus une nouvelle σ_1-poignée apparaisse

ce qui nous donne une notion de héritage entre les σ_1-poignées tel que chaque σ_1-poignée dans le mot initiale possède au plus un héritier dans chaque mot w_k.Si le nombre de σ_1-poignée n'est pas lui même dans chaque mot w_k.c'est à dire certaine σ_1-poignée se termine sans héritier par exemple de w_k à w_{k+1} en coupe la suite en w_k et en commence au w_{k+1}.

Définition 3.3.7 *Le $P^{ième}$ préfixe critique $\pi_p(w_k)$ de w_k est une tresse représentée par le préfixe de w_k qui se termine à la $1^{ère}$ lettre du $P^{ième}$ σ_1-poignée.*

Remarque 3.3.1 *Il y a deux cas à traiter selon la $1^{ère}$ lettre si c'est σ_1 ou σ_1^{-1}.*
On suppose qu'on va commencer avec σ_1 pour tout p , on a:

$$\pi_p(w_0) \geq \pi_p(w_1) \geq ... \tag{3.3.15}$$

et dans chaque étape où on a une réduction est le $P^{ème}$ σ_1-poignée.

Lemme 3.3.7 *On suppose que le $P^{ème}$ σ_1-poignée est réduit de w_k à w_{k+1} et que la poignée commence par $\sigma_1$alors un certain mot de tresse $\mu_{p,k}$ est tracé de $\pi_p(w_k)$ à $\pi_p(w_{k+1})$ dans $\Gamma(|w|)$ .contient un σ_1^{-1} et ne contient pas σ_1.*

Preuve. On représente les chemins associés à w_k en haut et les chemins associés à w_{k+1} en bas dans le graphe de Cayley.

On suppose que le P$^{\text{ème}}$ σ_1-poignée est réduit le mot $\mu_{p,k}$ apparait avec la couleur grise , et le point est tel que dans tous les cas c'est à dire σ_2 apparaisse positivement ou négativement ou n'apparait pas dans la poignée.Ce mot contient une lettre σ_1^{-1} et ne contient pas σ_1.
(a) Si la réduction de w_k à w_{k+1} n'est pas le P$^{\text{ème}}$ σ_1-poignée, il y a des cas
1- Si la réduction de w_k nécessite une σ_i-poignée avec $i \geq 2$.ou il nécessite le P$^{\text{ème}}$ σ_1-poignée tel que: $q \neq p \pm 1$.
Alors on a: $\pi_p(w_k) = \pi_p(w_{k+1})$ et on complète la définition par $\mu_{p,k} = \varepsilon$.
2- Si la réduction nécessite le $P \pm 1^{\text{ème}}$ σ_1-poignée.
L'équivalence $\pi_p(w_k) \equiv \pi_p(w_{k+1})$ n'est pas vraie en générale mais , certain mot $\mu_{p,k}$ ne contien ni σ_1 ni σ_1^{-1} va de $\pi_p(w_k)$ à $\pi_p(w_{k+1})$ dans $\Gamma(|w|)$. Par construction le mot $\mu_p = \mu_{p,0}\mu_{p,1}...$ est tracé dans le graphe de Cayley de $|w|$ il est σ_1-négative , et le nombre N d'étapes dans la suite $(w_0, w_1, ...)$ tel que le P$^{\text{ème}}$ σ_1-poignée est réduit est égal au nombre de lettres σ_1^{-1} dans μ
le nombre N est majoré par la hauteur h de w.
Dans le cas où le P$^{\text{ème}}$ poignée commence avec σ_1^{-1}.
On utilise la même méthode mais il suffit de voir que:

$$\pi_p(w_0) \leq \pi_p(w_1) \leq ... \tag{3.3.16}$$

et on change σ_1 par σ_1^{-1}, et le mot doit contenir un σ_1 et ne contient pas σ_1^{-1}.
Donc dans chaque cas les héritiers de chaque σ_1-poignée du mot initial w sont nécessite au plus h étapes de réduction. ■

Lemme 3.3.8 *Soit w un mot de tresse on suppose que w a un hauteur h et contient c σ_1-poignée.*
Alors le nombre de σ_1-poignée réduit dans toute suite de reduction de poignée de w est majoré par $c.h$.

Preuve. Voir le lemme (3.3.7) ■

Lemme 3.3.9 *Soit w un mot de tresse de longueur l largeur n et d'hauteur h.*
Alors le nombre de poignées réduites dans toute suite de réduction de poignée de w est majoré par $l\,(2h)^{2n-1}$.

Preuve. La réduction d'une σ_1-poignée peut être crier une σ_2-poignée mais ce nombre est majoré par le nombre de σ_2 ou σ_2^{-1} qui se présente dans la σ_1-poignée qui a été réduite , comme par hypothèse une σ_1-poignée permis ne contient pas de σ_2-poignée et le nombre de σ_2 dans une σ_1-poignée crier au plus $(h+1)$ nouveaux σ_2-poignées.On considère maintenant une suite de réduction de poignée qui commence en w.
N_i est le nombre de σ_i-réduction dans cette suite et c_i le nombre initial de σ_i-poignée dans w alors on obtient :

$$\begin{aligned}
N_1 &\leq c_1 h = lh \\
N_2 &\leq c_2 h = (c_2 + N_1\,(h+1))\,h \leq (l + lh\,(h+1)\,h) \\
N_2 &\leq (1 + h\,(h+1))\,lh = \left(h^2+h+1\right)lh \leq 3lh^3 = (2^2-1)lh^{2\times 2-1} \\
N_3 &\leq 7lh^5 \\
&\vdots \\
N_{i+1} &\leq (c_{i+1} + N_i\,(h+1))\,h
\end{aligned}$$

$$\begin{aligned}
c_i \quad &\leq \quad l \implies N_i \leq \left(2^i-1\right)lh^{2i-1} \qquad (3.3.17) \\
&\implies \quad \sum_{i=1}^{n} N_i \leq \sum_{i=1}^{n} \left(2^i-1\right)lh^{2i-1} = l\,(2h)^{2n-1}
\end{aligned}$$

■

D'aprés la proposition (3.3.6) $h < l(2h)^{2n-1}$ et par ce dernier lemme $\sum_{i=1}^{n} N_i \leq l\,(2h)^{2n-1}$ nous déduisons la proposition (3.3.1).

3.4 Ordre sur les tresses (méthode de diagramme de courbe)

Fenn, Greene, Rolfsen, Rourke et Wiest en 1997 [14] ont donné cette construction géométrique de l'ordre de Dehornoy, leurs techniques ont permis également de mettre des structures d'ordre sur le groupe des classes d'isotopie.

On va présenter dans cette section leurs techniques

Définition 3.4.1 *Soit D^2 le disque unité dans $\mathbb{C}$ centré en zéro et D_n le même disque tel que en supprimant n points distincts sur la droite réelle $P_1, P_2, ..., P_n$ en commençant à gauche.on désigne par $e_0, e_1, ..., e_n$ les segments $(-1, P_1), (P_1, P_2), ..., (P_{n-1}, P_n)$ et $(P_n, 1)$ respectivement.et E est le diamètre du disque D_2.*
Soit $\varphi : D_n \to D_n$ un homéomorphisme qui permute les points supprimés et qui laisse fixe le bord de D_n.
Un diagramme de courbe d'un homéomorphisme $\varphi : D_n \to D_n$ est l'image de E par φ.
Soient β, β' deux tresses dans le cube unite D, on dit que β est isotope à β' s'il existe un homéomorphisme $H : D \times [0,1] \longrightarrow D \times [0,1]$
$(x,t) \longmapsto H(x,t) = (h_t(x), t)$ où h_t est une famille d'homéomorphismes tel que: $h_t : D \longrightarrow D$ qui satisfait:
1-$h_t \mid_{\partial D} = id$
2-$h_0 = id$ et $h_1(\beta) = \beta'$
L'homéomorphisme H est appelé isotopie ambient.
Deux diagrammes de courbes sont dits isotopes s'il existe une isotopie de D_n qui déforme un diagramme à un autre et qui laisse fixe $P_1, P_2, ..., P_n$ et ∂D_n.

Identification de $\mathcal{B}_n$ à $MCG(D_n)$.

Théorème 3.4.1 *Il existe un isomorphisme entre $\mathcal{B}_n$ et $MCG(D_n)$*

Preuve. [14] ■

On a le résultat admis suivant

Proposition 3.4.1 *Deux homéomorphismes φ et $\chi : D_n \to D_n$ sont isotopes si et seulement si leurs diagrammes de courbes sont isotopes.*

Définition de l'ordre

Définition 3.4.2 *Soient $\beta_1, \beta_2 \in \mathcal{B}_n$ ou bien deux éléments de $MCG(D_n)$ représentés par deux homéomorphismes φ et χ ou $MCG(D_n)$ désigne le groupe des difféomorphisme de D_n.*
La $1^{ère}$ étape est de superposer les diagrammes de courbes φ et χ dans D_n.
La $2^{ème}$ étape est de coincider les diagrammes de courbes φ et χ avec les segments $[P_i, P_{i+1}]$ et éléminer les intersections unitiles.
La $3^{ème}$ étape on suppose que les diagrammes de courbes φ et χ ne sont pas isotopes.
Imaginons que nous somme au point (-1) de D_n et on va faire un toure autour des courbes de φ; pour un certain temps les courbes de χ coincident avec celles de φ.
A ce moment l'un est au point (-1) ou il est en un certain point P_i pour $i = 1, 2, ..., n$.Les diagrammes φ et χ divergent et a ce point de divergence χ sera situé hors de la composenter superieure de $(D_n \backslash \varphi)$ c'est à dire qui contient $(0, 1)$ ou dans la composente du bas qui contient $(0, -1)$.(voir figure (3.4.1))
Dans le $1^{ère}$ cas on dit que β_1 va aller à gauche plus que β_2 , et dans la $2^{ème}$ cas; on dit que β_1 va aller à droite plus que β_2.
La relation $<_{DC}$ sur $\mathcal{B}_n$ est définie comme suit: Soient $\beta_1, \beta_2 \in \mathcal{B}_n$ telle que $\beta_1 \neq \beta_2$ on met leurs diagrammes de courbes en position superposer on les coincide et on dit que $\beta_1 >_{DC} \beta_2$ est vrai si φ va aller à gauche plus rapide que χ et $\beta_1 <_{DC} \beta_2$ est vrai si χ va aller à gauche plus rapide que φ

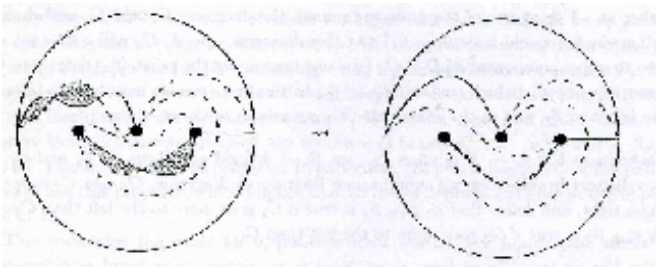

Figure 3.4.1 : Les diagrammes de courbe sont coincidés

Lemme 3.4.1 *.La relation $<_{DC}$ est un ordre linéaire sur $\mathcal{B}_n$ invariant par multiplication à gauche.*

Preuve. 1- $<_{DC}$ est reflexive
Soit φ le diagramme de courbes de β, c'est à dire $\beta <_{DC} \beta$ est vrai si φ va aller à gauche plus rapide que lui même.

Alors $\beta <_{DC} \beta$ est vrai $\Longrightarrow <_{DC}$ est reflexive.

2- $<_{DC}$ est antisymétrique

Soient $\beta_1, \beta_2 \in \mathcal{B}_n$ et φ, χ leurs diagrammes de courbes.

a- $\beta_1 <_{DC} \beta_2$ est vrai puisque χ va aller à gauche plus rapide que φ.

b- $\beta_2 <_{DC} \beta_1$ est vrai puisque φ va aller à gauche plus rapide que χ.

a et b impliquent que $\varphi \equiv \chi \implies \beta_1 = \beta_2$. ■

Pour démontrer la transivité on a besoin du lemme suivant:

Lemme 3.4.2 ***(réduction triple)*** *Soient Σ, Γ, Δ trois diagrammes de courbes tels que: Γ et Δ sont réduit par rapport à Σ.alors il existe un isotopie entre Δ et un diagramme de courbes Δ' qui est une équivalence par rapport à Σ tel que Σ, Δ',et Γ sont réduits deux à deux.*

Preuve. La preuve est faite selon des schémas voir [14] ■

Proposition 3.4.2 *On suppose que la tresse β a au moins un représentant σ-positif alors on a*

$$\beta >_{DC} 1$$

et de même pour une tresse qui admet un représentant σ-négatif , satisfait

$$\beta <_{DC} 1$$

Preuve. Soit w un mot de tresse σ-positif qui représente β avec un diagramme de courbe φ.

On suppose que w est σ_1-positif .

Donc w est de la forme $w_0\sigma_1 w_1\sigma_1 ...\sigma_1 w_k$, tel que les w_i ne contient pas les $\sigma_1^{\pm 1}$.

On considère maintenant les diagrammes de courbes de plusieurs tresses qui commence en (-1); on démontre que le segment initial de la $1^{\text{ère}}$ courbe de φ est liée au demi disque superieur D_n ce qui implique que $\beta >_{DC} 1$.

La $1^{\text{ère}}$ courbe du diagrammes de courbes représenté par w_k coinside avec la tresse triviale. Il est donc un segment horizontal par ce que le premier brin n'intersecte pas avec les autres brins.On agit σ_1 sur ce diagramme de courbes on obtient le diagramme de courbes $\sigma_1 w_k$.L'image de l'arc e_0 par $\sigma_1 w_k$ est un arc dans le demi disque supérieur D_n joint (-1) au P_2 = le second point supprimé le plus proche à gauche. En particulier cette courbe intersecte premièrement avec la ligne verticale à travers le point supprimé le plus à gauche P_1 lié au demi disque supérieur de D_n, l'application succéssive de toute suite de tresses

$\sigma_2^{\pm}, \sigma_3^{\pm}, ..., \sigma_{n-1}^{\pm}$ et σ_1 (mais pas σ_1^{-1}) ne change pas cette propriété, en particulier φ à cette propriété ce qui implique que le segment initial de φ est lié au demi disque superieur de D_n.

De même pour les mots de tresses σ_i-positifs. ■

Le diagramme de courbes d'un mot σ-positif doit diverger à gauche du diagramme de la courbe triviale et nous déduisons.

Corollaire 3.4.1 ***Propriété d'acyclicité (A)***
Une tresse qui admet au moins un représentant σ_1-positif n'est pas triviale.

Proposition 3.4.3 ***Propriété de comparaison (C)***
Chaque tresse β dans B_n admet un représentant σ-positif, σ-négatif ou σ-libre.

Preuve. Montrons que chaque tresse $\beta >_{DC} 1$ c'est à dire son $1^{\text{ère}}$ diagramme de courbe diverge à partir du diagramme de la courbe triviale vers le demi disque superieur de D_n admet un représentant σ-positif. Pour cela on suppose que le diagramme de la courbe de β diverge à gauche et on conclure que β admet un représentant σ-positif.
Si le diagramme de la courbe coincide avec e_0 seulement et diverge après, dans ce cas β admet un représentant σ-libre.
Si le 1^{er} diagramme de la courbe de β diverge à partir du diagramme de la courbe triviale vers le demi disque inférieur à droite de D_n plus rapide que le diagramme que le diagramme de la courbe triviale. ■

Proposition 3.4.4 *Pour toute tresses $\beta_1, \beta_2 \in \mathcal{B}_n$ la relation $\beta_1 < \beta_2$ est vrai si et seulement si nous avons*

$$\beta_1 <_{CD} \beta_2$$

Propriété S

Toute tresse de la forme $\beta\sigma_i\beta^{-1}$ admet un représentant $\sigma-$positif.

Pour démontrer la propriété **S** on utilise la notion de demi twist de Dehn

Définition 3.4.3 *Soit α un arc joignant deux point distinct P, Q dans le plan.*
Un twist de Dehn autour de α est un homéomorphisme φ du plan tel que $\varphi = 1$ à l'extérieur d'un petit voisinage de α il retourne α et il visse un petit voisinage comme les aiguilles d'une montre (voir figure (3.4.2))

La remarque suivante nous permet de démontrer la proposition.

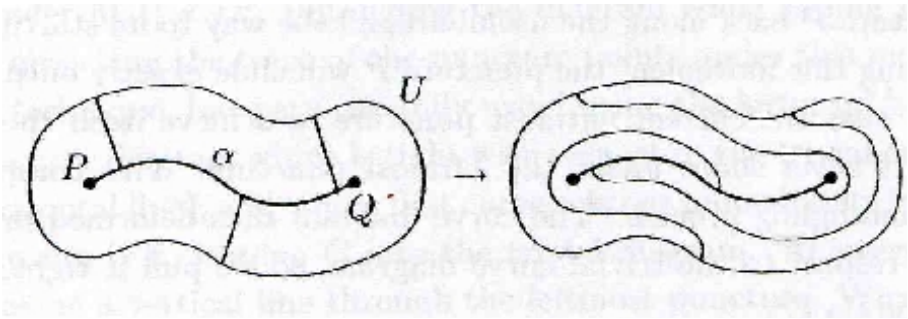

Figure 3.4.2 : Demi twist de Dehn autour d'un arc α

Remarque 3.4.1 *L'élément de $MCG(D)$ a défini par un demi twist de* ***Dehn*** *autour du segment e_i est l'image de la tresse σ_i sous l'isomorphisme de $\mathcal{B}_n$ à $MCG(D)$.*
Soit φ un demi twist de Dehn autour d'un arc α, et γ une courbe qui croise α transversalement à un point dites R.
L'image de γ sous φ se comporte comme suit.
Quand x va le long de γ, l'image $\varphi(x)$ aussi va le long de γ jusqu'à fin future assez à R, alors il tourne à gauche et va au point final de α en restant près de α, en le traversant à un point symétrique à R il retourne dans le sens inverse des aiguilles d'une montre, alors il revient dans un petit voisinage de R qui reste près de α et finalement il continue à avancer vers γ

Proposition 3.4.5 *Pour toute tresse β on a*

$$1 <_{CD} \beta\sigma_i\beta^{-1}$$

Preuve. Soit Ψ l'homéomorphisme de D_n qui correspond à β, et soit α est l'arc$\Psi(e_i)$. Alors un demi twist de Dehn φ autour de α représente la tresse $\beta\sigma_i\beta^{-1}$.

Donc par definition de $<$ l'inégalité $1 <_{CD} \beta\sigma_i\beta^{-1}$ suit de l'observation précitée que $\varphi(E)$ diverge à gauche de E à condition nous nous assurons que ces φ peuvent être choisis afin que $\varphi(E)$ est serré avec E.
Maintenant, nous pouvons supposer cet α est serré avec le diamètre principal E. Alors nous réclamons que le demi twist de Dehn φ peuvent être choisis afin qu'il n'y ait aucun petit disque borné par E et $\varphi(E)$.
En effet en coïncidant les parties de E et $\varphi(E)$, il y a seulement croisements inévitables de E et $\varphi(E)$ cela paraît des croisements proches de E et α. Entre deux tels points la courbe $\varphi(E)$ va parallèle à α. Une petite perturbation est exigée pour que $\varphi(E)$ devenir serré avec E ■

La proposition (3.3.4) implique que $(\mathcal{B}_n, <_{CD})$ est un groupe ordonné**.**

4

Application des tresses à la cryptographie

Le groupe des tresses fournit un cadre adapté à la cryptographie à clé publique car comme nous l'avons vu dans le deuxième chapitre le problème du mot possède des solutions algorithmiques efficaces, tandis que le problème de conjugaison, est difficile.

4.1 Cryptographie basée sur les tresses

La sécurité des échanges de données à distance vise deux qualités complementaires, la confidentialité et l'authenticité.

La confidentialité est la propriété qu'un message ne peut être lu que par les entités qu'on a choisies et l'authenticité est l'assurance de l'identité.

On commence ici par quelques problèmes difficiles dans le groupe des tresses et qui sont intéressants pour la cryptographie.

4.1.1 Problèmes difficiles dans le groupe des tresses

On dit que x et y sont conjugués s'il existe un élément a tel que $y = a.x.a^{-1}$.

On a vu dans le chapitre 2 que le problème de conjugaison est décidable dans le groupe des tresses.

1-**Problème de recherche des conjuguées.**

Soient $(x, y) \in \mathcal{B}_n \times \mathcal{B}_n$ tels que x, y sont conjugués.

Objectif: Trouver $a \in \mathcal{B}_n$ tel que:

$$y = a.x.a^{-1}$$

2-**Généralisation du problème de recherche des conjuguées**.
$\forall\,(x,y) \in \mathcal{B}_n \times \mathcal{B}_n\ \exists b \in \mathcal{B}_m$ avec $m \leq n$ tels que $y = b.x.b^{-1}$
Objectif: Trouver $a \in \mathcal{B}_m$ tel que:

$$y = a.x.a^{-1}$$

3-**Problème de décomposition des conjuguées**.
$\forall\,(x,y) \in \mathcal{B}_n \times \mathcal{B}_n$, $\exists b \in \mathcal{B}_m$ avec $m < n$ tels que $y = b.x.b^{-1}$
Objectif: Trouver $\grave{a}, a^{"} \in \mathcal{B}_m$ tels que:

$$y = \grave{a}.x.a^{"}$$

4.1.2 Le cryptosystème basé sur les tresses

On considère deux sous groupes $L\mathcal{B}_l =< \sigma_1, ..., \sigma_{l-1} >$ et $R\mathcal{B}_r =< \sigma_{l+1}, ..., \sigma_{l+r-1} >$ de $\mathcal{B}_{r+l}$ ces deux sous groupes commutent $ab = ba$, $\forall\,(a,b) \in L\mathcal{B}_l \times R\mathcal{B}_r$.

Définition 4.1.1 *On dit qu'une fonction $f : E \to F$ est à sens unique lorsque, pour $x \in E$ calculer $f(x)$ est facile (polynomial en la longueur de x) et pour tout k, il existe c tel que pour toute machine de Turing probabiliste en temps polynomial M et tout x de longueur $l(x) > c$, on a $P(f(M(f(x)))) = f(x) < l(x)^{-k}$. On dit alors qu'inverser f est difficile.*

Soit $f : L\mathcal{B}_l \times \mathcal{B}_{r+l} \to \mathcal{B}_{r+l} \times \mathcal{B}_{r+l}$, $(a,x) \to (a.x.a^{-1}, x)$ f est une fonction à sens unique , car il est facile de calculer $a.x.a^{-1}$ à partir de la pair (a,x).
Cette fonction est basée sur le problème de recherche des conjugués généralisée.

La sécurité du schéma d'échange de clés et du cryptosystème à clé publique (PKC) est basée sur la difficulté du problème suivant:

Probleme de base: Le triplet (x, y_1, y_2) d'éléments de $\mathcal{B}_{r+l}$ tel que: $y_1 = a.x.a^{-1}$ et $y_2 = b.x.b^{-1}$, pour $a \in L\mathcal{B}_l$ et $b \in R\mathcal{B}_r$.

Trouver: $b.y_1.b^{-1}$ $(= a.y_2.a^{-1} = a.b.x.a^{-1}.b^{-1})$, x doit être suffisamment compliqué.

Exemple 4.1.1 *Si $x = x_1.x_2.z$, avec $x_1 \in L\mathcal{B}_l$, $x_2 \in R\mathcal{B}_r$ et $z \in \mathcal{B}_{r+l}$ qui commute avec $L\mathcal{B}_l$ et $R\mathcal{B}_r$.*

$$b.y_1.b^{-1} = \left(a.x_1.a^{-1}\right)\left(b.x_2.b^{-1}\right)z$$

car $y_1 = a.x.a^{-1} = a.x_1.a^{-1}.x_2.z$ *donc* $b.y_1.b^{-1} = y_1.x^{-1}y_2$.
On a $x = x_1.x_2.z$, $x_1 \in L\mathcal{B}_l$, $x_2 \in R\mathcal{B}_r$ *et* $z \in \mathcal{B}_{r+l}$ *commute avec* $L\mathcal{B}_l$ *et* $R\mathcal{B}_r$ *d'ou*

$$y_1 = a.x.a^{-1} = a.x_1.a^{-1}.x_2.z$$

et

$$y_2 = b.x.b^{-1} = x_1.b.x_2.b^{-1}.z$$

Donc $b.y.b^{-1}$ *pourait être calculé sans connaitre* a *et* b.

Remarque 4.1.1 *1-le problème (3) implique le problème de base car si* $y_1 = à.x.a"$ *alors* $à.y_2.a" = à.b.x.b^{-1}.a" = b.à.x.a"b^{-1} = b.y_1.b^{-1}$ *tels que* $à, a" \in L\mathcal{B}_l$
2- Soit $f : \mathcal{B}_n \longrightarrow \Sigma_n$
Pour éviter que l'adversaire ne puisse calculer $f(a)$ *et* $f(b)$ *d'aprés* $f(x); f(y_1)$ *et* $f(y_2)$ *on choisit* $f(x) = (1)$.

Echange des clés

On choisit une paire d'entiers (l, r) et une tresse $x \in \mathcal{B}_n$ compliqué
a-Alice choisit aléatoirement une tresse $b \in R\mathcal{B}_r$ et envoie $y_1 = a.x.a^{-1}$ à Bob.
b-Bob choisit aléatoirement une tresse $a \in L\mathcal{B}_l$ et envoie $y_2 = b.x.b^{-1}$ à Alice.
c-Alice reçoit y_2 et calcule $k = a.y_2.a^{-1}$.
d-Bob reçoit y_1 et calcule $k = b.y_1.b^{-1}$

Il est suggéré dans [1] de travailler dans $\mathcal{B}_{80}$ $(l = r = 40)$ avec des tresses de longueur 12.

En utilisant le système d'échange des clés décrit ci dessus ; on construit le PKC.

Définition 4.1.2 *On dit qu'une fonction* $h : \mathcal{B}_n \to \{0,1\}^N$ *est une fonction de hachage si la probabilité de trouver* $h(b_2) = h(b_1)$ *pour* $b_2 \neq b_1$ *est négligeable.*

On va maintenant construire le PKC.

Soit $H : \mathcal{B}_{r+l} \to \{0,1\}^k$ une fonction de hachage idéale du groupe des tresses sur l'espace des messages.

1-Génération des clés:
(a) choisir une tresse $x \in \mathcal{B}_{r+l}$ suffisamment compliquée.
(b) choisir une tresse $a \in L\mathcal{B}_l$.
(c) clé publique (x, y) ou $y = a.x.a^{-1}$, a la clé privée.

2-Chiffrement:

Etant donné un message $m \in \{0,1\}^k$ et la clé publique (x, y).

(a) choisir une tresse $b \in R\mathcal{B}_r$ aléatoirement.

(b) texte chiffré: (c, d) ou $c = b.x.b^{-1}$, $d = H\left(b.y.b^{-1}\right) \oplus m$.

3-Déchiffrement:

Etant donné un texte chiffré (c, d) et une clé privée a , calculer $m = H\left(a.c.a^{-1}\right) \oplus d$.

Remarque 4.1.2 *1- Casser le PKC est équivalent à resoudre le problème de base* $(c, d) = \left(b.x.b^{-1}, H\left(a.b.x.a^{-1}.b^{-1}\right) \oplus m\right)$.

Déchiffrer un texte chiffré revient à connaitre $a.b.x.a^{-1}.b^{-1}$.

2- Il est important d'utiliser une clé différente pour chaque session, puisque si la même clé est utilisée pour chiffrer deux messages m_1 *et* m_2 *dont les textes chiffrés sont* (c_1, d_1) *et* (c_2, d_2)*, alors peut être calculé facilement à partir de* (m_1, d_1, d_2) *car* $H\left(b.y.b^{-1}\right) = m_1 \oplus d_1 = m_2 \oplus d_2$

5

Conclusion générale

Nous rappelons l'objectif de notre travail est d'étudier les propriétés du groupe des tresses $\mathcal{B}_n$ en focalisant notre étude sur le groupe des tresses pures $\mathcal{P}_n$, le groupe des commutateurs $\mathcal{B}'_n$ du groupe des tresses sur ce dernier on a trouvé une nouvelle présentation .
Sur le groupe des tresses , deux problèmes algorithmiques ont été traités :
Le premier problème c'est le problème du mot dont la solution est basée sur la technique de E.Artin . Le deuxième problème est le problème de conjugaison où on a donné une solution en basant sur une autre qui est la technique de F.Garside.
Parmi les problèmes qui se posent sur le groupe des tresses on trouve le problème de l'ordre où plusieurs façons de construction ont été présentées.
Nous avons discuter un algorithme éfficace pour décider l'ordre.
On a discuté aussi l'application des tresses à la cryptographie à clé publique puisque comme nous l'avons vu le problème du mot possède une solution algorithmique efficace, tandis que le problème de conjugaison, est difficile.

Bibliographie

[1] **I. Anshel, M. Anshel, B. Fisher &D. Goldfeld**, New key agreement protocols in braid group cryptography,CT-RSA 2001(San Francisco,CA), Springer Lec.Notes in comput.Sci, 2020 (2001) 1-15

[2] **I. Anchel, M. Anchel & D. Goldfeld** An algebraic method for public -key cryptography Math.res.let 6 (1999) 287-291

[3] **E. Artin** Theory of braids Ann of math 48 (1947) 101-126

[4] **J. Birman** Braids, links, and mapping class groups Annals of maths, studies vol 82, princeton univ press (1979)

[5] **J. Birman, K.H. Ko & S.J. Lee**. A new approach to the word problem in the braid groups Advances in maths 109-2 (1998) 322-353

[6] **J. Birman, K.H. Ko & S.J. Lee** The infimum,supremum and geodesic lengh of a braid conjugacy class Advances in math 164 (2001) 41-56

[7] **P. Dehornoy** Braid groups and left distributive operation Trans, Amer .Math soci 345(1994) No 1 p 115-151

[8] **P. Dehornoy** A fast mathed for comparing braids Advanced in math 125 (1997) 200-235

[9] **P. Dehornoy** Braids and Self-Distributivity Progress in Math,Vol 192 Birkhauser (2000)

[10] **P. Dehornoy** Construction of Self-Distributive operations and charged braids Internat, J.Algebra and comput 10 (2000) No 1, p 173-190

[11] **P. Dehornoy, I. Dynikov, D. Rolfsen & B. Wiest** Wy are braids ordrable? Panorama et Synthèse vol 14 soc math France (2002)

[12] **E. A. El Rifai & H.R. Morton** Algorithms for positive braids Quart j math Oxford 45-2 (1994) 479-497

[13] **D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston** Word Processing in groups Jones et Bartlett publ (1992)

[14] **R. Fenn**, **M.T. Greene, D. Rolfsen, C. Rourke & B. Wiest** Ordering the braid groups Pacific j of math 191 (1999) 49-74

[15] **F.A. Garside** The braid groups and other groups Quart. J math Oxford 20 No 78 1969

[16] **N.D. Gilbert & T. Porter** Knots and surfaces oxford science publications 1994

[17] **C. Kassel** L'ordre de Dehornoy sur les tresses Séminaire Bourbaki, exposé 865 (Novembre 1999)

[18] **K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kong & C. Park** New public key cryptosystem using braid groups crypto 2000 Springer lect notes in comput sci 1880 (2000)166-184

[19] **S.J. Lee & E.K. Lee** Overview of the cryptosystems using braid groups ASCDF (2001) p 41-50

[20] **W. Magnus, A. Karas & D. Solitar** Combinatorial group theory presentations of groups in terms of generators and relations Interscience 1966

[21] **K. Murasugi & B. Kurpita** A study of braids Kluwer academic publushers 1999

[22] **D. Rolfsen** Ordered groups and topology Luminy .June 2001

[23] **D. Rolfsen** New developments in the theory of Artin's braid groups Topology and applications 127 (2003) 77-90

[24] **D. Rolfsen & J. Zhu** The braids orderings and zero divirsors: J knot theory and its ramifications (1997)

[25] **C.Rourke & B. Wiest** Order automatic mapping class groups Pacific. J. Math 194 (2000) No 1 p 209-227

[26] **H. Short & B.Wiest** Ordering mapping class groups after Thurston Enseign. Math 46 (2000) p 279-312

[27] **W. Shpilrain** Assessing security of some group based cryptosystems preprint (2003)

[28] **H. Sibert** Algorithmique des groupes des tresses Thèse de doctorat. Univ de caen (2003)