

Mémoire de stage de M1

Introduction à la théorie des tresses

Baptiste Dugué
Encadré par Bert Wiest

2023

Introduction

L'objectif de ce mémoire est de présenter les bases de la théorie des tresses, domaine mathématique que j'ai eu le plaisir de découvrir au cours d'un stage réalisé durant les mois d'avril et mai 2023 sous la direction de Bert Wiest, que je remercie chaleureusement pour sa bienveillance, sa patience et son enthousiasme indéfectibles. La source principale de ce travail a été le livre de Patrick Dehornoy, Le calcul des tresses [Deh19], dont je recommande vivement la lecture à toute personne souhaitant approfondir les idées présentées ici. À quelques exceptions près, les notations de ce document seront celles de ce livre, et le point de vue généralement adopté doit beaucoup à l'angle particulier choisi par P. Dehornoy pour son ouvrage.

Nous partirons de l'idée intuitive et tangible de tresses en tant qu'objets du quotidien et de la question naturelle qui émerge de leur manipulation : "Puis-je démêler ce tas de nœuds et, si oui, comment ?". La réponse exhaustive à cette interrogation passera par une mathématisation du problème et des concepts mis en jeu ; on associera les tresses à des groupes présentés dans lesquels on cherchera à construire une forme normale déterminant complètement si deux tresses a priori distinctes sont en fait identiques à déformation près. À l'aide des outils que nous aurons construits, nous aborderons également le problème de conjugaison des tresses, problème dont la résolubilité en un temps polynomial est à ce jour encore une question ouverte.

Table des matières

1	Les groupes de tresses	2
1.1	Intuition et mathématisation	2
1.2	Les groupes B_n	4
2	Le monoïde des tresses positives	5
2.1	Le Théorème de Ore	5
2.2	La tresse fondamentale	7
2.3	La forme normale gloutonne	9
3	La forme Δ-normale, applications	11
3.1	La forme Δ -normale et le problème d'isotopie des tresses	11
3.2	Le problème de conjugaison	12
3.3	L'ensemble super-sommital	14
3.4	Borne sur le nombre de cyclages et décyclages	16

1 Les groupes de tresses

1.1 Intuition et mathématisation

Comme dit en introduction, les tresses sont avant tout des objets tangibles et connus de toutes et tous. On peut s'amuser à en manipuler enfant, apprendre à tresser ses cheveux ou chercher la meilleure façon de démêler une paire d'écouteurs. Il s'agit d'ailleurs du premier problème que nous nous proposons de traiter : étant donnée une tresse, déterminer s'il est possible de la démêler (comprendre la ramener dans un état dans lequel les brins qui la composent ne se croisent pas) et comment s'y prendre. Notons que les tresses que nous considérons sont "fixées" à leurs extrémités, à la différence de la majorité des tresses que l'on rencontre habituellement. On peut par exemple penser à une natte de cheveux fixée à l'extrémité basse par un élastique.

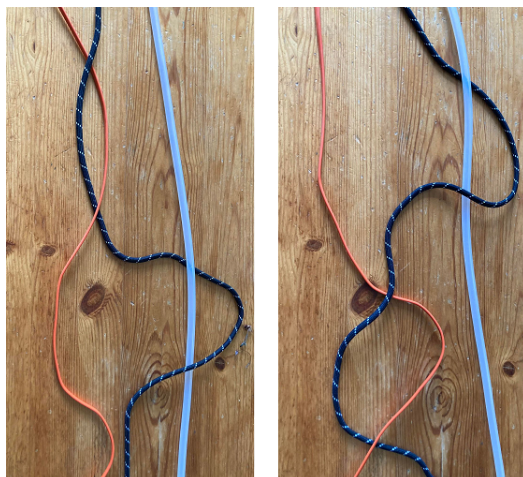


FIGURE 1 – Premiers exemples de tresses

Tout d'abord, il convient de fixer un système de représentation et de notations algébriques permettant de manipuler mathématiquement ces objets. Les diagrammes ci-dessous sont des exemples des représentations standardisées que nous adopterons par la suite. Ils représentent les tresses réelles des deux photos ci-dessus. Noter qu'à chaque croisement, on met en évidence le brin passant au-dessus et celui passant en-dessous.



FIGURE 2 – Diagramme associé à la première tresse

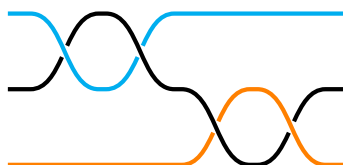


FIGURE 3 – Diagramme associé à la seconde tresse

On se convainc facilement qu'au fond, tout ce qui importe pour identifier une tresse, ce sont ses croisements entre ses brins et leur ordre. On définit donc une notation permettant de coder une tresse par une suite de lettres (appelée *mot*) représentant un croisement entre deux brins.

Définition 1.1.1. Le mot de tresse d'un diagramme de tresse est la suite de lettres σ_i et $\overline{\sigma}_i$ définie de la façon suivante :

Chaque lettre correspond à un croisement du diagramme, et on code les croisements de gauche à droite. Localement, les brins sont numérotés en partant du bas, et le croisement entre le brin i et le brin $i + 1$ est codé σ_i si le brin i passe en-dessous du brin $i + 1$, et $\overline{\sigma}_i$ sinon.

Le mot vide, décrivant une tresse sans aucun croisement, sera noté ϵ .

Exemples. Le mot de tresse de la première tresse (fig.2) est $\sigma_1\sigma_1\sigma_2\sigma_2$ et celui de la deuxième (fig.3) est $\sigma_2\sigma_2\sigma_1\sigma_1$. Le mot $\overline{\sigma}_1\sigma_2\overline{\sigma}_1\sigma_2\overline{\sigma}_1\sigma_2$ représente le diagramme suivant (fig.4) :



FIGURE 4 – Diagramme de tresse associé au mot $\overline{\sigma}_1\sigma_2\overline{\sigma}_1\sigma_2\overline{\sigma}_1\sigma_2$.

Définition 1.1.2. Deux mots de tresses w_1 et w_2 seront dits *équivalents* si l'on peut déformer continûment la tresse représentée par l'un en la tresse représentée par l'autre. On notera $w_1 \equiv w_2$.

Exemples.

- Faire passer un brin au-dessus d'un autre puis immédiatement refaire la même chose revient à ne rien faire du tout, autrement dit il est évident qu'une tresse représentée par un mot $\sigma_i\overline{\sigma}_i$ se démêle sans difficulté, c'est-à-dire que pour tout entier i , $\sigma_i\overline{\sigma}_i \equiv \overline{\sigma}_i\sigma_i \equiv \epsilon$.

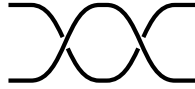


FIGURE 5 – Diagramme de tresse associé au mot $\overline{\sigma}_1\sigma_1$

- Pourvu qu'ils se produisent sur des brins assez éloignés, deux croisements consécutifs peuvent se réaliser dans n'importe quel ordre. On peut donc passer facilement d'une tresse représentée par le mot $\sigma_i\sigma_j$ à une tresse représentée par le mot $\sigma_j\sigma_i$ dès lors que $|i - j| \geq 2$. Dans un tel cas, on a donc l'équivalence de mots $\sigma_i\sigma_j \equiv \sigma_j\sigma_i$.

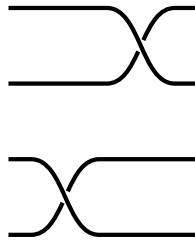


FIGURE 6 – Diagramme de tresse associé au mot $\sigma_1\sigma_3$.

- Comme cela se voit aisément sur le diagramme suivant, on a aussi, pour tout entiers i, j tels que $|i - j| = 1$, $\sigma_i\sigma_j\sigma_i \equiv \sigma_j\sigma_i\sigma_j$. Concrètement, il suffit de faire coulisser le brin central du bas vers le haut, ou inversement.

La conséquence de cette façon de présenter le problème est que pour décider si une tresse est démêlable, il suffit de déterminer si son mot de tresse est équivalent au mot vide. En fait, nous allons faire mieux, en mettant en place une méthode permettant de déterminer pour tout couple de mots si ceux-ci sont ou non équivalents. La structure mathématique toute indiquée pour traiter ce type de problème est celle de groupe présenté.

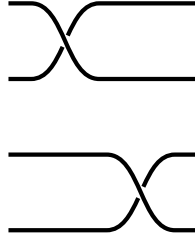


FIGURE 7 – Diagramme de tresse associé au mot $\sigma_3\sigma_1$.

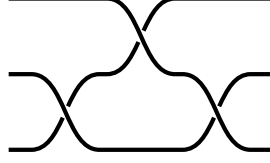


FIGURE 8 – Diagramme de tresse associé au mot $\sigma_1\sigma_2\sigma_1$.

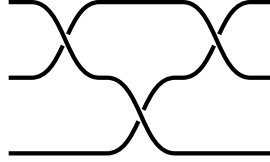


FIGURE 9 – Diagramme de tresse associé au mot $\sigma_2\sigma_1\sigma_2$.

1.2 Les groupes B_n

Fort de ces observations, nous allons maintenant associer aux ensembles de tresses des structures de groupes. Pour cela, on commence par introduire une loi de composition interne.

Définition 1.2.1. Si g_1 et g_2 sont deux tresses à n brins représentées par des mots w_1 et w_2 , on définit leur *produit* $g_1 \cdot g_2$ comme la tresse dont le diagramme associé est celui représenté par la *concaténation* des mots w_1 et w_2 , à savoir $w_1 w_2$.

Remarque. La loi $\cdot$ est évidemment associative, mais pas commutative.

Définition 1.2.2. Pour tout entier $n \in \mathbb{N}^*$, le *groupe de tresses à n brins* est le groupe (muni de la loi $\cdot$) admettant la présentation

$$B_n := \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{si } |i - j| \geq 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{si } |i - j| = 1 \end{array} \right\rangle$$

Remarques. — Les éléments de B_n sont donc les tresses vues à déformation près. Si jusqu'à maintenant on parlait de deux tresses différentes lorsque celles-ci étaient équivalentes, désormais on désignera informellement par *tresse* n'importe quelle forme qu'une tresse donnée puisse prendre. Formellement, on peut montrer que B_n est le quotient du groupe des mots de tresses par la relation d'équivalence induite par la notion d'*équivalence* de la définition 1.1.2.

- L'exemple explicité précédemment par la figure 5 fournit immédiatement la formule pour l'inverse de tout élément de B_n : Pour tout $i \in \{1, \dots, n-1\}$, $\sigma_i^{-1} = \overline{\sigma_i}$. Le fait de disposer de l'inverse de chacun des générateurs du groupe donne directement la formule générale de l'inverse d'un élément quelconque.
- Pour tout $n \leq m$, le groupe B_n se plonge naturellement dans le groupe B_m , l'image de B_n dans B_m étant l'ensemble des tresses à m brins dont aucun des $m - n$ derniers brins n'en croise un autre. Concrètement, B_n est isomorphe au sous-groupe de B_m engendré par les éléments $\sigma_1, \dots, \sigma_n$.

Le fait de déterminer si deux tresses peuvent se démêler de l'une vers l'autre (en termes savants, on parle du *problème d'isotopie des tresses*) se ramène dès lors à la résolution du problème des mots des groupes B_n . L'objectif va maintenant être de construire une forme normale sur B_n , c'est-à-dire un ensemble d'expressions privilégiées et uniques sous forme de mots de tresse pour chaque élément de B_n , ainsi que des algorithmes pour les calculer en un temps fini (et si possible raisonnable). Pour ce faire, nous allons commencer par nous concentrer sur un sous-ensemble sympathique de l'ensemble des tresses.

2 Le monoïde des tresses positives

Définition 2.0.1. Une tresse $g \in B_n$ est dite *positive* si elle est représentée par un mot de tresse w qui ne s'écrit qu'avec des lettres $\sigma_1, \dots, \sigma_n$ élevées à des puissances positives.

On considère le monoïde présenté

$$B_n^+ := \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{si } |i - j| \geq 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{si } |i - j| = 1 \end{array} \right\rangle^+$$

On va voir que B_n^+ s'identifie à un sous-monoïde de B_n et qu'il s'agit précisément de l'ensemble des tresses positives, ce qui n'est en fait pas aussi évident que ce qu'on pourrait croire à première vue. En effet, le fait que B_n^+ et B_n admettent la même présentation (respectivement en tant que monoïde et que groupe) fournit un morphisme $\iota : B_n^+ \rightarrow B_n$ qui à la classe $[w]_{B_n^+}$ d'un mot w dans le monoïde associe sa classe $[w]_{B_n}$ dans le groupe. Pour conclure à un plongement, il faut encore montrer que le morphisme ι est injectif, ce qui est une question difficile en général.

2.1 Le Théorème de Ore

Heureusement pour nous, le monoïde B_n^+ a de bonnes propriétés qui vont nous faciliter la tâche : il est *simplifiable* et, étant donnés deux de ses éléments, ceux-ci admettent toujours un multiple commun à droite.

Définition 2.1.1. — Un monoïde M est dit *simplifiable à gauche* (resp. *à droite*) si pour tout $a, b, c \in M$, $ab = ac$ (resp. $ba = ca$) implique $b = c$.
Un monoïde *simplifiable* est un monoïde simplifiable à gauche et à droite.
— Soient a, b deux éléments d'un monoïde M . On dit que a *divise* b à gauche ou, de manière équivalente, que b *est un multiple de* a à droite s'il existe $x \in M$ tel que $ax = b$.
Une telle relation de divisibilité induit un ordre partiel sur le monoïde, et l'on écrira $a \preccurlyeq b$ pour signifier que a divise b à gauche.

Remarque. La démonstration du fait que B_n^+ est simplifiable est intéressante en ce qu'elle amène à introduire l'outil des grilles de retournement, mais elle est assez technique et minutieuse dans sa mise en place. Aussi je préfère renvoyer la lectrice au chapitre III de [Deh19] pour les détails de cette preuve, et me concentrer ici sur d'autres aspects.

Pour de tels monoïdes, on dispose du joli théorème suivant qui nous permet de conclure immédiatement pour le cadre des tresses :

Théorème 1 (Ore¹). Si M est un monoïde simplifiable et si deux éléments quelconques de M admettent toujours un multiple (à droite) commun, alors il existe un plongement ι de M vers un groupe G appelé *groupe de fractions de* M dont tout élément peut s'écrire sous la forme $\iota(a)\iota(b)^{-1}$ avec $a, b \in M$. De plus, si M admet la présentation $\langle S | R \rangle^+$, alors le groupe G admet la présentation $\langle S | R \rangle$.

1. Il s'agit de Øystein Ore, connu notamment pour son théorème sur le plongement d'un anneau sans diviseurs de zéro dans un corps. La condition sur l'intersection non-vide de tout couple d'idéaux principaux se trouve traduite dans le monde des monoïdes par l'existence d'un multiple commun.

Démonstration. On introduit sur $M \times M$ la relation binaire $\sim$ définie ainsi :

$$(a, b) \sim (a', b') \Leftrightarrow \exists (x, x') \in M^2, ax = a'x' \text{ et } bx = b'x'.$$

Dans ce cas, on dit que le couple (x, x') *témoigne* pour la relation $(a, b) \sim (a', b')$. Cette relation est une relation

d'équivalence. En effet, elle est réflexive $((1, 1) \text{ témoigne pour toute relation } (a, b) \sim (a, b))$ et symétrique (si (x, x') témoigne pour $(a, b) \sim (a', b')$, alors (x', x) témoigne pour $(a', b') \sim (a, b)$). La démonstration de la transitivité est plus délicate. Tout d'abord, observons que

$$(a, b) \sim (a', b') \Leftrightarrow \forall y, y' \in M, (ay = a'y' \Rightarrow by = b'y').$$

En effet, supposons que (x, x') témoigne pour $(a, b) \sim (a', b')$ et que $ay = a'y'$. Comme x et y admettent un multiple à droite commun, il existe $c, d \in M$ tels que $xd = yc$. Alors $a'x'd = axd = ayc = a'y'c$ donc, comme M est simplifiable, $x'd = y'c$. Ainsi, $b'yc = b'xd = b'x'd = b'y'c$ et donc $b'y = b'y'$.

La réciproque vient du fait que tout couple d'éléments admet un multiple commun à droite. Ainsi il existe $x, x' \in M$ tels que $ax = a'x'$, ce qui implique $bx = b'x'$ et donc $(a, b) \sim (a', b')$.

Dès lors, si l'on a $(a, b) \sim (a', b') \sim (a'', b'')$, en considérant $ax = a'x' = a''x''$ un multiple commun à a, a' et a'' , on a $bx = b'x' = b''x''$ et donc $(a, b) \sim (a'', b'')$, et $\sim$ est donc transitive.

On note G l'espace quotient $M^2 / \sim$ et $\frac{a}{b}$ la classe de (a, b) . On munit G de la loi $\frac{a}{b} \cdot \frac{c}{d} = \frac{ax}{dy}$, où $bx = cy$ est un multiple à droite commun à b et c . La loi ainsi construite est bien définie (on vérifie que $\frac{a}{b} \cdot \frac{c}{d}$ ne dépend pas de x et y) et associative, conférant ainsi à G une structure de groupe, de neutre $\frac{1}{1}$ et dont l'inverse d'un élément $\frac{a}{b}$ est $\frac{b}{a}$. Enfin on pose pour tout a dans M , $\iota(a) := \frac{a}{1}$. Il ne nous reste plus qu'à voir que $\iota : M \rightarrow G$ est un morphisme injectif et que pour tout élément $\frac{a}{b}$ de G , on a $\frac{a}{b} = \iota(a)\iota(b)^{-1}$:

Tout d'abord, pour tous $a, b \in M$, on a $1b = b1$, d'où $\iota(a) \cdot \iota(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{11} = \frac{ab}{1} = \iota(ab)$.

Ensuite, ι est bien injectif : Si $\iota(a) = \iota(a')$, alors $(a, 1) \sim (a', 1)$ et donc il existe $x, x' \in M$ tels que $ax = a'x'$ et $1x = 1x'$. De la deuxième égalité on déduit $x = x'$ puis, en simplifiant à droite, de la première on obtient $a = a'$.

Enfin, pour tous $a, b \in M$, on a $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1} = \iota(a) \cdot \iota(b)^{-1}$.

Pour ce qui est de la deuxième partie du théorème concernant la présentation de G , il y a deux choses à montrer : Premièrement, que l'image de la partie génératrice S par le morphisme ι engendre G en tant que groupe, et deuxièmement que les relations de monoïde R définissent bien le groupe G , cette fois-ci en tant que relations sur un groupe. Pour ne pas alourdir les notations, on se place dans le cas où ι est l'identité et on identifie donc sans danger M et ses éléments avec leurs images dans G .

Le premier point est facile. S engendre M en tant que monoïde, et donc engendre aussi les inverses des éléments de M dans le groupe G . Puisque tout élément de G s'écrit comme produit d'un élément de M et d'un inverse d'un élément de M , S engendre G .

Pour le deuxième point, la subtilité vient de la différence entre une présentation sur un monoïde et une présentation sur un groupe. Concrètement, S est un alphabet auquel on associe un alphabet $\bar{S}$ constitué des mêmes lettres que S mais surmontées d'une barre, et d'un ensemble de relations sur $S \cup \bar{S}$ noté $Sym(S)$ et composé de toutes les relations de la forme $s\bar{s} = 1$ et $\bar{s}s = 1$ pour s lettre de S (on parle des *relations du groupe libre*). On dispose également d'une application $eval_G : (S \cup \bar{S})^* \rightarrow G$, où $(S \cup \bar{S})^*$ désigne l'ensemble des mots composés de lettres dans S et $\bar{S}$, qui au mot vide associe le neutre de G et qui à un mot $s_1 \dots s_n$ associe l'élément $s_1 \cdot s_2 \cdot \dots \cdot s_n \in G$. Si on note $\equiv$ la congruence (relation d'équivalence compatible avec la structure ambiante de monoïde/groupe) sur $(S \cup \bar{S})^*$ engendrée par les relations $(R \cup Sym(S))$, alors dire que G admet la présentation $\langle S | R \rangle$ revient à dire que pour tout mot w dans $(S \cup \bar{S})^*$,

$$w \equiv \epsilon \Leftrightarrow eval_G(w) = 1.$$

La première implication est une conséquence directe des définitions du groupe G et du morphisme d'évaluation. Pour l'implication réciproque, l'idée est de se ramener à un point de vue sur le monoïde $\bar{M}$, dont on sait déjà que $\langle S | R \rangle^+$ est une présentation. Pour ce faire, on montre d'abord que tout mot w de $(S \cup \bar{S})^*$ peut s'écrire sous la forme $u\bar{v}$ avec u et v des mots de S^* . On commence par observer que tout mot w peut s'écrire $u_1\bar{v}_1u_2\bar{v}_2\dots u_p\bar{v}_p$ où les $u_1, \dots, u_p, v_1, \dots, v_p$ sont des mots de S^* avec u_1 et v_p éventuellement vides, puis on procède par récurrence sur p . Pour $p = 1$ il n'y a rien à montrer. Supposons $p \geq 2$ et notons $w' := u_2\bar{v}_2\dots u_p\bar{v}_p$. Par hypothèse de récurrence, il existe $u', v' \in S^*$ tels que $w' = u'\bar{v}'$ et donc $w = u_1\bar{v}_1u'\bar{v}'$. On utilise à nouveau le fait que deux éléments de M admettent toujours un multiple commun à droite pour considérer u'' et v'' dans S^* tels que $v_1u'' \equiv u'v''$ dans le monoïde M et donc également dans le groupe G , ce qui implique $\bar{v}_1u'' \equiv u''\bar{v}'$, et donc $w \equiv u_1u''\bar{v}''v'$, ce qu'on cherchait.

Maintenant, si on suppose $eval_G(w) = 1$, en écrivant $w = u\bar{v}$ il vient $eval_G(u) = eval_G(v)$, et on en déduit donc que u et v sont équivalents dans l'alphabet S^* muni des relations R , puisqu'on sait que M se plonge dans G et admet la présentation $\langle S | R \rangle^+$. Comme M se plonge dans G , cela signifie *a fortiori* que u et v sont équivalents dans l'alphabet $(S \cup \bar{S})^*$ muni des relations $(R \cup Sym(S))$, i.e. $u \equiv v$. Ainsi, on a $u\bar{v} \equiv \epsilon$, c'est-à-dire $w \equiv \epsilon$. $\square$

Si l'on admet que les monoïdes B_n^+ sont simplifiables, on va quand même prendre le temps de démontrer le point sur les multiples communs de toute paire d'éléments, et pour cause, c'est là qu'entre en scène une famille de tresses nommées à juste titre *fondamentales* et qui vont jouer un rôle de première importance dans toute la suite

de l'exposé.

2.2 La tresse fondamentale

On définit les tresses fondamentales sur les ensembles B_n de manière récursive :

Définition 2.2.1 (Tresses fondamentales). On pose $\Delta_1 := \epsilon$ puis, pour tout $n \geq 2$, $\Delta_n := \sigma_1 \sigma_2 \dots \sigma_{n-1} \Delta_{n-1}$.

Chaque tresse Δ_n est donc une tresse positive vivant dans B_n , et on va montrer le résultat suivant, qui en plus de nous permettre d'appliquer le théorème de Ore, va être la base d'une première tentative de création de forme normale :

Proposition 2.2.1. L'élément Δ_n^l est multiple à droite de tout élément de B_n^+ de longueur inférieure à l , c'est-à-dire décrit par un mot $\sigma_{i_1} \dots \sigma_{i_k}$ avec $k \leq l^1$.

1. Remarquons que, sur le monoïde B_n^+ , la *longueur* d'une tresse est en fait un invariant, au sens où elle ne dépend pas de l'expression sous forme de mot choisie. En effet, les relations de la présentation de B_n^+ conservent les longueurs des expressions mises en jeu, et comme les éléments n'admettent pas d'inverse dans le monoïde, une expression ne se "simplifie" jamais. Cela n'est évidemment plus vrai dans le groupe B_n , où par exemple un mot de deux lettres comme $\sigma_1 \bar{\sigma}_1$ se trouve représenter le même objet que le mot vide.

Commençons par fixer une notation qui permettra de condenser les expressions des prochaines démonstrations et de rendre leur lecture plus digeste. Dans la suite, $\underline{\sigma}_{i,j}$ désignera $\sigma_i \sigma_{i+1} \dots \sigma_{j-1}$ si $i < j$, ϵ si $i = j$, et $\sigma_{i-1} \dots \sigma_{j+1} \sigma_j$ si $i > j$. Ainsi, on écrira pour tout entier $n \geq 2$, $\Delta_n = \underline{\sigma}_{1,n} \Delta_{n-1}$. On dispose tout d'abord du lemme suivant :

Lemme 1. Pour tous entiers i, j, k avec $j \geq i + 2$ et $i < k < j$, on a

- (i) $\sigma_k \underline{\sigma}_{i,j} = \underline{\sigma}_{i,j} \sigma_{k-1}$,
- (ii) $\sigma_{k-1} \underline{\sigma}_{j,i} = \underline{\sigma}_{j,i} \sigma_k$.

Démonstration. On se contente de montrer (i), la démonstration de (ii) étant sensiblement identique. On procède par récurrence sur $|i - j|$. Pour $j = i + 2$, on a nécessairement $k = i + 1$, et donc $\sigma_k \underline{\sigma}_{i,j} = \sigma_{i+1} \sigma_i \sigma_{i+1}$ qui est bien égal à $\underline{\sigma}_{i,j} \sigma_{k-1} = \sigma_i \sigma_{i+1} \sigma_i$ par les relations de la présentation du monoïde. Supposons maintenant $j \geq i + 3$ et, dans un premier temps, $k = i + 1$. En appliquant d'abord l'hypothèse de récurrence puis en utilisant le fait que $j - 1 - i \geq 2$, et donc que σ_{j-1} et σ_i commutent, on a

$$\sigma_k \underline{\sigma}_{i,j} = \sigma_{i+1} \underline{\sigma}_{i,j-1} \sigma_{j-1} = \underline{\sigma}_{i,j-1} \sigma_i \sigma_{j-1} = \underline{\sigma}_{i,j-1} \sigma_{j-1} \sigma_i = \underline{\sigma}_{i,j} \sigma_{k-1}.$$

Pour $k \geq i + 2$, on fait essentiellement la même chose, mais en utilisant maintenant le fait que σ_i et σ_k commutent :

$$\sigma_k \underline{\sigma}_{i,j} = \sigma_k \sigma_i \underline{\sigma}_{i+1,j} = \sigma_i \sigma_k \underline{\sigma}_{i+1,j} = \sigma_i \underline{\sigma}_{i+1,j} \sigma_{k-1} = \underline{\sigma}_{i,j} \sigma_{k-1}.$$

□

On continue à jouer avec cette écriture pour préparer le terrain en vue des preuves suivantes.

Lemme 2. Pour tout $n \geq 2$, $\Delta_n = \Delta_{n-1} \underline{\sigma}_{n,1}$.

Démonstration. On procède encore par récurrence, cette fois sur n . Pour $n = 1$ et $n = 2$ le résultat est immédiat, supposons donc $n \geq 3$. Il suffit d'appliquer l'hypothèse de récurrence et le fait que Δ_{n-2} , n'admettant dans son écriture que des lettres σ_i avec $i \leq n - 3$, commute avec σ_{n-1} :

$$\Delta_n = \underline{\sigma}_{1,n} \Delta_{n-1} = \underline{\sigma}_{1,n-1} \sigma_{n-1} \Delta_{n-2} \underline{\sigma}_{n-1,1} = \underline{\sigma}_{1,n-1} \Delta_{n-2} \sigma_{n-1} \underline{\sigma}_{n-1,1} = \Delta_{n-1} \underline{\sigma}_{n,1}.$$

□

On profite de commencer à découvrir plus intimement les tresses fondamentales pour introduire les automorphismes "flips" des monoïdes B_n^+ , notés τ_n , qui envoient une tresse $\sigma_{i_1} \dots \sigma_{i_k}$ dans B_n^+ vers la tresse dont les lettres sont "renversées", à savoir $\sigma_{n-i_1} \dots \sigma_{n-i_k}$. Le principal résultat les concernant est qu'il s'agit en fait des automorphismes intérieurs associés aux tresses fondamentales.

Proposition 2.2.2. Soit $n \in \mathbb{N}^*$. Pour tout $a \in B_n^+$, $a\Delta_n = \Delta_n\tau_n(a)$.

Démonstration. On procède par récurrence sur la longueur du mot a . Pour un mot de longueur 1, c'est-à-dire de la forme σ_i avec $1 \leq i \leq n-1$, on montre le résultat par récurrence sur n . Une fois de plus, le résultat est immédiat pour $n = 1$ et $n = 2$. Supposons $n \geq 3$ et, tout d'abord, $i = 1$. En utilisant successivement le lemme 2, l'hypothèse de récurrence, le point (ii) du lemme 1 et encore le lemme 2, on a :

$$\sigma_1\Delta_n = \sigma_1\Delta_{n-1}\underline{\sigma}_{n,1} = \Delta_{n-1}\sigma_{n-2}\underline{\sigma}_{n,1} = \Delta_{n-1}\underline{\sigma}_{n,1}\sigma_{n-1} = \Delta_n\sigma_{n-1}.$$

Maintenant, pour $2 \leq i \leq n-1$, en utilisant cette fois-ci le point (i) du lemme 1 et l'hypothèse de récurrence, on a :

$$\sigma_i\Delta_n = \sigma_i\underline{\sigma}_{1,n}\Delta_{n-1} = \underline{\sigma}_{1,n}\sigma_{i-1}\Delta_{n-1} = \underline{\sigma}_{1,n}\Delta_{n-1}\sigma_{n-1-(i-1)} = \Delta_n\sigma_{n-i}.$$

Supposons maintenant a de longueur $l \geq 2$, de sorte que l'on puisse écrire $a = b\sigma_i$ pour un certain b non vide dans B_n^+ et un i dans $\{1, \dots, n-1\}$, et la proposition vérifiée pour tous les mots positifs de longueur strictement plus petite que l , donc en particulier pour b . On a alors

$$a\Delta_n = b\sigma_i\Delta_n = b\Delta_n\sigma_{n-i} = \Delta_n\tau_n(b)\sigma_{n-i} = \Delta_n\tau_n(a).$$

□

Remarques. — Lorsque l'on a dit plus haut que les τ_n étaient les "automorphismes intérieurs associés aux tresses fondamentales", on a utilisé un vocabulaire de théorie des groupes, alors que l'on n'a pour l'instant établi un résultat que sur des monoïdes. En fait, en anticipant un peu et en admettant que le monoïde B_n^+ se plonge dans le groupe B_n , on peut considérer dans le groupe l'automorphisme de conjugaison par Δ_n qui, par la démonstration que l'on vient de faire, envoie nécessairement tout σ_i vers σ_{n-i} et coïncide dès lors avec τ_n sur B_n^+ . Les σ_i formant un ensemble de générateurs pour B_n , τ_n s'étend de manière unique en un automorphisme sur le groupe, et il n'y a pas de difficulté : on retiendra que pour toute tresse $a \in B_n$, $\tau_n(a) = \Delta_n^{-1}a\Delta_n$.

— Comme on l'a fait pour la tresse fondamentale, dans les contextes où il n'y a pas d'ambiguïté ou d'intérêt à spécifier l'indice n , celui-ci sera omis et on parlera simplement du morphisme τ , automorphisme intérieur associé à Δ .

Nous avons maintenant entre notre possession tous les outils nécessaires à la démonstration de la proposition 2.2.1.

Démonstration de la proposition 2.2.1. Rappelons que dire qu'un élément a est multiple à droite d'un élément b signifie qu'il existe c tel que $a = bc$. On cherche donc à montrer que pour tout $u \in B_n^+$ de longueur inférieure à l , il existe un élément w de B_n^+ tel que $\Delta_n^l = uw$.

Commençons par montrer le résultat pour les mots d'une seule lettre, c'est-à-dire que pour tout $1 \leq i \leq n-1$, il existe $\partial_n(\sigma_i) \in B_n^+$ tel que $\Delta_n = \sigma_i\partial_n(\sigma_i)$. Raisonnons par récurrence sur n . Le cas $n = 1$ est trivial et le cas $n = 2$ se ramène à voir que $\sigma_1\epsilon = \Delta_2$. Supposons $n \geq 3$. Si $i < n-1$, il suffit d'appliquer l'hypothèse de récurrence au rang $n-1$, auquel on se ramène à l'aide du lemme 2 :

$$\Delta_n = \Delta_{n-1}\underline{\sigma}_{n,1} = \sigma_i(\partial_{n-1}(\sigma_i)\underline{\sigma}_{n,1}).$$

Pour σ_{n-1} , on utilise le point (ii) du lemme 1. En effet, Δ_{n-1} s'écrit entièrement à l'aide des lettres $\sigma_1, \dots, \sigma_{n-2}$ qui vérifient toutes $\sigma_i\underline{\sigma}_{n,1} = \underline{\sigma}_{n,1}\sigma_{i+1}$. Ainsi, si on note Γ_{n-1} la tresse composée des mêmes lettres que Δ_{n-1} mais avec leur indice augmenté de 1 (σ_i est remplacé par σ_{i+1}), alors on a :

$$\Delta_n = \Delta_{n-1}\underline{\sigma}_{n,1} = \underline{\sigma}_{n,1}\Gamma_{n-1} = \sigma_{n-1}(\underline{\sigma}_{n-1,1}\Gamma_{n-1}).$$

Pour étendre la démonstration aux mots de longueur supérieure ou égale à deux, on procède par récurrence. Soit donc u un mot de longueur $l \geq 2$, et u' un mot de longueur $l-1$ tel que u s'écrive $u = u'\sigma_i$ pour un certain i dans $\{1, \dots, n-1\}$. Par hypothèse de récurrence, il existe $v' \in B_n^+$ tel que $\Delta_n^{l-1} = u'v'$. On pose $w = \partial_n(\sigma_i)\tau_n(v')$, et on a alors :

$$uw = u'\sigma_i\partial_n(\sigma_i)\tau_n(v') = u'\Delta_n\tau_n(v') = u'v'\Delta_n = \Delta_n^l,$$

ce qui achève la démonstration. □

Ce résultat, qui implique l'existence d'un multiple à droite commun pour toute paire de tresses positives, associé au fait que les monoïdes B_n^+ sont simplifiables (admis) permet d'appliquer le théorème de Ore : Non seulement le monoïde B_n^+ se plonge dans B_n (ce qui justifie, a posteriori, l'abus dont on a fait preuve jusqu'ici dans la désignation des objets du monoïde que l'on appelait déjà "tresses positives"), mais en plus B_n est le groupe de fractions à droite de B_n^+ , ce qui implique que toute tresse $g \in B_n$ peut s'écrire comme produit d'une tresse positive et d'une tresse "négative", autrement dit il existe $a, b \in B_n^+$ telles que $g = ab^{-1}$.

Avant d'étendre cette première forme normale sur le monoïde en une forme normale sur le groupe, opération pour laquelle on a déjà démontré tous les résultats nécessaires, on termine cette section sur les tresses fondamentales par une proposition centrale (sans mauvais jeu de mot) les concernant.

Lemme 3. Les puissances paires de la tresse fondamentale sont toutes dans le centre de B_n , i.e.

$$\forall k \in \mathbb{N}, \forall g \in B_n, \Delta^{2k} g = g \Delta^{2k}.$$

Démonstration. D'après la proposition 2.2.2, pour tout $i \in \{1, \dots, n-1\}$,

$$\sigma_i \Delta_n^2 = \Delta_n \sigma_{n-i} \Delta_n = \Delta_n^2 \sigma_{n-(n-i)} = \Delta_n^2 \sigma_i.$$

Ainsi Δ_n^2 commute avec tous les σ_i , donc avec tous les éléments de B_n^+ , et donc avec tous les éléments de son groupe de fractions, à savoir B_n . $\square$

Remarque. Avec plus de travail on peut en fait même montrer que pour tout $n \in \mathbb{N}$, $Z(B_n) = \{\Delta_n^{2k} | k \in \mathbb{N}\}$, voir par exemple [GAR69].

2.3 La forme normale gloutonne

On poursuit nos efforts en gardant en tête notre objectif de construction d'une forme normale sur B_n . Avant de nous attaquer directement à cette tâche, nous allons terminer notre travail sur les monoïdes B_n^+ en mettant en place une forme normale qui leur sera spécifique. Notre point de départ sera un résultat que l'on se contentera d'admettre, la démonstration reposant essentiellement sur des outils développés dans le cadre de la preuve de la simplifiabilité de B_n^+ , non présentée dans ce document.

Proposition 2.3.1. Pour tout $n \in \mathbb{N}^*$, le monoïde B_n^+ muni de la relation de divisibilité à gauche $\preceq$ est un *treillis*.

Cela signifie que, pour tous $a, b \in B_n^+$, il existe deux éléments $\text{pgcd}_{\text{gauche}}(a, b)$ et $\text{ppcm}_{\text{droite}}(a, b)$ dans B_n^+ tels que, pour tous $x, y \in B_n^+$,

- $x \preceq a$ et $x \preceq b \Rightarrow x \preceq \text{pgcd}_{\text{gauche}}(a, b)$
- $a \preceq y$ et $b \preceq y \Rightarrow \text{ppcm}_{\text{droite}}(a, b) \preceq y$.

Remarques. — La non-trivialité de cette proposition, que l'on pourrait appeler "existence d'un pgcd et d'un ppcm", provient du fait que $\preceq$ n'est qu'une relation d'ordre partielle. A priori, il n'est donc pas assuré qu'il existe un multiple commun à a et b qui soit ordonné avec (et en particulier plus petit que) tous leurs multiples communs, et il en va de même pour les diviseurs.

- Notons qu'avec l'existence du pgcd et du ppcm vient sans hypothèse supplémentaire leur unicité. Cela découle simplement du fait que $\preceq$, en tant que relation d'ordre, est antisymétrique.

On se sert une fois de plus des décidément bien nommées tresses fondamentales pour définir la notion de *tresses simples*.

Définition 2.3.1. [Tresse simple] Une tresse $a \in B_n^+$ est dite *simple* si elle divise la tresse fondamentale Δ_n .

Remarques. — On ne précise pas de quel côté une tresse doit diviser Δ pour être simple, car dans ce cas précis ces deux notions sont en fait équivalentes.

- Il existe d'autres façons équivalentes de définir les tresses simples :
 - On peut considérer le morphisme $\text{perm}: B_n \rightarrow \mathfrak{S}_n$ qui à une tresse g associe la permutation ω telle que dans tout diagramme de tresse représentant g , le brin en i -ème position à la gauche du diagramme se retrouve en position $\omega(i)$ à droite, et considérer une certaine section ensembliste de ce morphisme qui se trouvera être exactement l'ensemble des tresses simples. Cela signifie notamment que B_n comporte exactement $n!$ tresses simples.
 - On peut aussi montrer que les tresses simples sont exactement les tresses positives qui sont représentées par un diagramme dans lequel deux brins distincts se croisent au plus une fois (ou, de façon équivalente, telle que dans tous diagrammes les représentant, deux brins distincts se croisent au plus une fois).

Définition 2.3.2 (Tête d'une tresse). Soit $a \in B_n^+$ une tresse positive. La *tête* de a est la tresse $T(a) := \text{pgcd}_{\text{gauche}}(a, \Delta_n)$.

Empressons-nous de démontrer tout de suite un petit lemme dont on se servira plus tard concernant ce nouvel objet.

Lemme 4. Pour tout $a, b \in B_n^+$, $T(ab) = T(aT(b))$.

Démonstration. Pour montrer cette égalité, on va montrer que $T(aT(b))$ divise $T(ab)$ et inversement.

Tout d'abord, la tête de b divise b par définition, donc on a $aT(b) \preceq ab$. Or, la tête d'une tresse positive $g \in B_n^+$ est, en tant que pgcd entre g et Δ , l'unique tresse simple "maximale" divisant cette tresse, autrement dit $T(g)$ est l'unique tresse simple vérifiant $T(g) \preceq g$ et, pour toute tresse s simple, $s \preceq g \Rightarrow s \preceq T(g)$. La tresse $T(aT(b))$ étant par ailleurs elle-même simple et divisant ab , il vient $T(aT(b)) \preceq T(ab)$.

Considérons maintenant s une tresse simple telle que $s \preceq ab$, et montrons qu'alors $s \preceq aT(b)$. Soit s' telle que $as' = \text{ppcm}(a, s)$ (tous les ppcm considérés dans cette preuve sont des ppcm à droite). Premièrement, $s' \preceq b$. En effet, comme s et a divisent ab , leur ppcm as' divise aussi ab , et donc en simplifiant par a on a $s' \preceq b$.

La tresse s' est de plus simple. Montrons ce point par récurrence sur p le nombre de tresses simples dont a est le produit (en tant que tresse simple, a s'écrit nécessairement comme produit de tresses simples, par exemple comme produit de σ_i). Si $p = 0$, alors $b = 1$ et $s' = a$. Supposons $p \geq 1$, et écrivons $a = a't$ où a' s'écrit comme un produit d'au plus $p - 1$ tresses simples et t est simple. Si on note t' la tresse telle que $a't' = \text{ppcm}(a', s)$, alors par propriété du ppcm on a $t's' = \text{ppcm}(t', t)$. Par hypothèse de récurrence, t' se trouve être simple, et t l'est par construction. Or le ppcm de deux tresses simples étant lui-même simple (cela vient de la définition d'une tresse simple comme diviseur de Δ), on a $t's'$ simple. De plus, si un produit de tresses est simple, alors chaque terme du produit est également simple, et on en déduit que s' est aussi simple. Ainsi, par définition de la tête d'une tresse, le fait que s' divise b est équivalent au fait que s' divise la tête de b . Ce dernier point montre en particulier que $s \preceq aT(b)$. En effet, $s' \preceq T(b)$ implique $as' \preceq aT(b)$, et comme as' est multiple de s (c'est le ppcm de a et s), s divise nécessairement $aT(b)$. Enfin, puisque s est simple, cela entraîne $s \preceq T(aT(b))$. Pour finir, si on considère pour s la tresse $T(ab)$ qui est bien une tresse positive divisant ab , on a bien $T(ab) \preceq T(aT(b))$, d'où finalement l'égalité recherchée. $\square$

La tête d'une tresse est donc par définition toujours une tresse simple, ce qui justifie la définition suivante :

Définition 2.3.3 (Suite normale). Une suite $(s_1, \dots, s_d)$ de tresses simples est dite *normale* si pour tout $k \leq d$, $s_k = T(s_k \dots s_d)$.

On sent qu'on approche du but, à savoir dégager pour chaque tresse une expression privilégiée et dont le calcul se réalise par un même algorithme pour toutes les tresses. Pour pouvoir légitimement parler de forme normale, il nous reste à démontrer une propriété d'existence et d'unicité.

Proposition 2.3.2. Pour toute tresse positive $a \in B_n^+$, il existe une unique suite normale $(s_1, \dots, s_d)$ telle que $a = s_1 \dots s_d$ et $s_d \neq 1$, où 1 désigne la tresse triviale représentée par le mot vide ϵ .

Démonstration. Soit $a \in B_n^+$. On montre l'existence d'une telle expression par récurrence sur la longueur de a (notée $|a|$), ce qui est légitime par la remarque de la proposition 2.2.1. L'initialisation pour $|a| = 0$ correspond au cas où la tresse est nécessairement décrite par le mot vide, ce qui est bien une écriture sous forme de suite normale (vide). Supposons $|a| \geq 1$. Dans ce cas a est différent de 1, donc est divisible à gauche par au moins un σ_{i_0} avec i_0 dans $\{1, \dots, n - 1\}$. En particulier on a donc $\sigma_{i_0} \preceq T(a)$, et donc $T(a) \neq 1$. Ainsi, en écrivant $a = T(a)a'$, on a nécessairement $|a'| < |a|$. Si $a' = 1$ alors $a = T(a)$ et il s'agit déjà d'une écriture sous forme de suite normale, sinon on applique l'hypothèse de récurrence à a' en écrivant $a' = s_2 \dots s_d$ et dans ce cas $(T(a), s_2, \dots, s_d)$ est une suite normale convenable pour décrire a .

L'unicité de cette écriture est une conséquence immédiate de la définition de la tête d'une tresse comme un pgcd et de l'unicité d'un tel élément (cf. proposition 2.3.1). $\square$

Ça y est, nous sommes enfin légitimes à parler de "forme normale"! Celle-ci sera qualifiée de *gloutonne*, en référence au fait que lors de son calcul on cherche toujours à déterminer la plus grande tresse simple possible divisant la tresse considérée.

Définition 2.3.4 (Forme normale gloutonne). Soit $a \in B_n^+$ une tresse positive. La *forme normale gloutonne* de a est la suite normale $(s_1, \dots, s_d)$ telle que $a = s_1 \dots s_d$ et $s_d \neq 1$.

Remarque. On peut montrer que le calcul de la forme normale gloutonne d'un mot positif de longueur l s'effectue en $O(l^2)$ étapes.

Pour conclure sur le problème d'isotopie des tresses, il ne nous reste plus qu'à étendre la forme normale gloutonne en une forme normale définie sur le groupe de tresses tout entier. Il existe plusieurs façons de procéder, nous n'en présentons ici qu'une, mais par laquelle on arrivera à obtenir des informations supplémentaires concernant la structure des groupes de tresses.

3 La forme Δ -normale, applications

La forme que l'on se propose d'étudier se base une fois de plus sur les propriétés des tresses fondamentales. Encore une fois, l'intérêt d'une telle forme normale repose sur une propriété d'existence et d'unicité d'écriture.

3.1 La forme Δ -normale et le problème d'isotopie des tresses

Proposition 3.1.1. Toute tresse $g \in B_n$ s'écrit de manière unique $g = \Delta_n^m s_1 \dots s_d$ avec $m \in \mathbb{Z}$ et $(s_1, \dots, s_d)$ une suite normale telle que $s_1 \neq \Delta_n$ et $s_d \neq 1$.

Démonstration. Commençons par montrer que toute tresse $g \in B_n$ possédant une expression avec p lettres négatives peut s'écrire de manière unique $g = \Delta_n^m b$ avec $m \in \mathbb{Z}$, $m \leq p$, $b \in B_n^+$ et $\Delta_n \not\leq b$. Pour ce faire, on montre d'abord par récurrence sur le nombre de lettres négatives du mot g que $\Delta_n^p g \in B_n^+$.

Si $p = 0$, il n'y a rien à montrer puisque le mot est déjà positif. Supposons $p \geq 1$ et considérons $u \in B_n$ dont une écriture comporte moins de $p - 1$ lettres négatives, $i \in \{1, \dots, n - 1\}$ et $v \in B_n^+$ tels que $g = u \bar{\sigma}_i v$. Par hypothèse de récurrence, $\Delta_n^{p-1} g \in B_n^+$, et par une application directe de la proposition 2.2.1 à un mot de longueur 1, $\Delta_n \bar{\sigma}_i \in B_n^+$, d'où en utilisant la proposition 2.2.2 :

$$\Delta_n^p g = \Delta_n \Delta_n^{p-1} u \bar{\sigma}_i v = \tau_n(\Delta_n^{p-1} u)(\Delta_n \bar{\sigma}_i) v \in B_n^+,$$

puisque cette dernière expression s'écrit comme produit d'éléments de B_n^+ .

Considérons maintenant l'ensemble $P := \{k \in \mathbb{Z} \mid \Delta_n^k g \in B_n^+\}$, dont on vient de montrer qu'il contient p . Un mot de tresse comportant plus de lettres négatives que de lettres positives ne pouvant représenter une tresse positive (car il serait alors équivalent à un mot comportant uniquement des lettres positives via les relations de la présentation de B_n , et que la seule façon de faire "disparaître" une lettre négative est de l'accoler à son inverse positif), si on considère une expression de g comportant q lettres positives, alors pour tout $k < -q$, on a nécessairement $\Delta_n^k g \notin B_n^+$, et donc $k \notin P$. L'ensemble P est donc non-vide et minoré, et admet ainsi un plus petit élément $m \in \mathbb{Z}$. Posons $b := \Delta_n^m g \in B_n^+$, de sorte que $g = \Delta_n^{-m} b$. Alors Δ_n ne divise pas b (à gauche), sinon on pourrait écrire $g = \Delta_n^{-(m-1)}(\Delta_n^{-1} b)$ avec $\Delta_n^{-1} b \in B_n^+$, ce qui contredirait la minimalité de m dans P . Enfin, ce couple $(m, b) \in \mathbb{Z} \times B_n^+$ est bien unique, puisque si on considère un autre tel couple $(m', b') \in \mathbb{Z} \times B_n^+$ vérifiant $g = \Delta_n^{m'} b'$ et $\Delta_n \not\leq b'$, alors on a, par minimalité de m , $m \leq m'$, donc $\Delta_n^m b = g = \Delta_n^m \Delta_n^{m'-m} b'$, d'où $b = \Delta_n^{m'-m} b'$, et donc $m' = m$ puisque $\Delta_n \not\leq b$, ce qui implique aussi $b = b'$.

Pour conclure et obtenir la condition de l'énoncé de la proposition, il suffit d'observer que si la forme normale gloutonne de la tresse b que l'on vient d'introduire est $(s_1, \dots, s_d)$, alors la condition $\Delta_n \not\leq b$ est équivalente à $s_1 \neq \Delta_n$. En effet, d'une part $s_1 = \Delta_n$ implique $\Delta_n \leq b$, et d'autre part, comme Δ_n est une tresse simple, le fait que Δ_n divise b implique que Δ_n divise sa tête, c'est-à-dire s_1 , et donc que $s_1 = \Delta_n$ puisque s_1 est simple. $\square$

On dispose enfin de la tant convoitée forme normale sur les groupes B_n :

Définition 3.1.1 (Forme Δ -normale). L'écriture unique d'une tresse $g \in B_n$ introduite par le lemme précédent est appelée *forme Δ_n -normale* de g . On écrira $(\Delta_n^m \mid s_1, \dots, s_d)$ pour parler d'une telle forme normale.

La plupart du temps, lorsqu'il n'y aura aucun risque d'ambiguïté, on omettra l'indice n et on parlera plus simplement de *forme Δ -normale*.

Remarque. Bien que l'on simplifie l'écriture en supprimant l'indice n , il est important de noter que la forme Δ -normale est unique dans un groupe B_n donné, puisque l'expression de la tresse fondamentale Δ_n dépend du groupe

ambiant. Par exemple, une tresse à 3 brins n'aura a priori pas la même forme Δ -normale suivant que l'on la voie comme une tresse de B_3 ou comme une tresse de B_n avec $n > 3$.

Par la suite, nous allons étudier et utiliser à profit les propriétés de cette écriture, et il est donc commode de nommer les différentes caractéristique d'une forme Δ -normale.

Définition 3.1.2. Soit g une tresse de forme Δ -normale $\Delta^m s_1 \dots s_d$. On appelle *borne inférieure* de g l'entier $\inf_n(g) := m$, *borne supérieure* de g l'entier $\sup_n(g) := m + d$, et *longueur canonique* de g l'entier $\text{lc}_n(g) := d$.

L'intérêt de ces entiers va notamment résulter d'une caractérisation les reliant à la tresse fondamentale dont on se servira par la suite pour définir des ensembles de tresses permettant d'apporter une solution au problème de conjugaison.

Proposition 3.1.2. Pour toute tresse $g \in B_n$, on a pour tous p, q entiers :

- (i) $p \leq \inf(g) \Leftrightarrow \Delta^p \preceq g$,
- (ii) $\sup(g) \leq q \Leftrightarrow g \preceq \Delta^q$.

Démonstration. Montrons d'abord le premier point. Soit $(\Delta^m \mid s_1, \dots, s_d)$ la forme Δ -normale de g . Si $p \leq \inf(g)$ alors $g = \Delta^p \Delta^{m-p} s_1 \dots s_d$, et donc $\Delta^p \preceq g$. Réciproquement, si $\Delta^p \preceq g$, il existe $b \in B_n^+$ tel que $\Delta^p b = g$. Soit $(\Delta^r \mid s'_1 \dots s'_e)$ la forme Δ -normale de b , avec donc $r \geq 0$ puisque b est positive. La forme Δ -normale de g est alors nécessairement $(\Delta^{p+r} \mid s'_1 \dots s'_e)$, et on a donc $\inf(g) = p + r \geq p$.

Passons au deuxième point. Supposons $\sup(g) \leq q$ c'est-à-dire, en reprenant la même écriture sous forme Δ -normale que pour le point (i), $m + d \leq q$. Tout d'abord, $a := s_1 \dots s_d \preceq \Delta^d$. En effet, si on raisonne par récurrence sur d (le cas $d = 1$ étant simplement une application de la définition de tresse simple), et qu'on pose $a' = s_1 \dots s_{d-1}$, alors il existe par hypothèse b' dans B_n^+ tel que $a'b' = \Delta^{d-1}$, et on a alors :

$$\Delta^d = \Delta^{d-1} \Delta = a'b' \Delta = a' \Delta \tau(b') = a' s_d \partial(s_d) \tau(b'),$$

où $\partial(s_d)$ est la tresse positive telle que $s_d \partial(s_d) = \Delta$, dont l'existence est assurée par la définition de tresse simple. Si on pose $b := \partial(s_d) \tau(b')$, on a bien d'une part que b est positive en tant que produit de tresses positives, et d'autre part $\Delta^d = ab$, et donc $a \preceq \Delta^d$. Dès lors, $g = \Delta^m s_1 \dots s_d \preceq \Delta^{m+d} \preceq \Delta^q$.

Réciproquement, si on suppose $g \preceq \Delta^q$, c'est-à-dire $\Delta^m s_1 \dots s_d \preceq \Delta^q$, alors en simplifiant par Δ^m on a $s_1 \dots s_d \preceq \Delta^{q-m}$. Or, par définition de la forme normale gloutonne, d est le plus petit entier tel que Δ^d soit multiple à droite de $s_1 \dots s_d$ lorsque $(s_1, \dots, s_d)$ est une suite normale avec $s_d \neq 1$. On a donc nécessairement $d \leq q - m$, et donc $\sup(g) = m + d \leq q$. $\square$

Avant de nous attaquer au problème de conjugaison, prenons le temps de conclure en ce qui concerne le problème d'isotopie des tresses. Étant donnés deux mots de tresses w_1 et w_2 , pour décider s'ils représentent ou non une même tresse, il suffit par la propriété d'unicité 3.1.1 de calculer leurs formes normales respectives (dans un groupe B_n approprié fixé au préalable), qui sera la même si et seulement si la tresse représentée par w_1 se déforme continûment en celle représentée par w_2 . Concrètement, pour calculer la forme Δ -normale d'un mot $\sigma_{i_1}^{\epsilon_1} \dots \sigma_{i_d}^{\epsilon_d}$ avec pour tout j dans $\{1, \dots, d\}$, $\epsilon_j \in \{-1, 1\}$ et $i_j \in \{1, \dots, n-1\}$, on part des dernières lettres et on remonte le mot : on détermine d'abord la forme normale de σ_d que l'on note a_d , puis celle de $\sigma_{i_{d-1}}^{\epsilon_{d-1}} a_d$, que l'on note a_{d-1} et ainsi de suite¹. Chacune de ces étapes est facile (au sens où elle se réalise en un nombre linéaire d'étapes), et le calcul d'une forme Δ -normale s'effectue donc en un temps polynômial. Plus exactement, la forme Δ -normale d'une tresse de longueur l se calcule en $O(l^2)$ étapes.

3.2 Le problème de conjugaison

Après le problème des mots, un autre problème propre à tout groupe présenté est celui du problème de conjugaison. Il s'agit de déterminer si deux mots représentent des tresses conjuguées dans le groupe. Dans le cadre des groupes de tresses, il est d'autant plus intéressant qu'il permet de construire un lien avec la théorie des entrelacs.

1. On peut donner de façon plus explicite l'allure de ces formes Δ -normales successives. Soit g une tresse de forme normale $(\Delta^m \mid s_1, \dots, s_d)$ et t est une tresse simple. On peut montrer que :

- Si $(s'_1, \dots, s'_d, t_d)$ est la forme normale gloutonne de $\tau^m(t) s_1 \dots s_d$, alors la forme Δ -normale de tg est $(\Delta^m \mid s'_1, \dots, s'_d, t_d)$ si $s'_1 \neq \Delta$ et $(\Delta^{m+1} \mid s'_2, \dots, s'_d, t_d)$ sinon.
- Si $(s'_1, \dots, s'_d, t_d)$ est la forme normale gloutonne de $\tau^m(\partial(t)) s_1 \dots s_d$, alors la forme Δ -normale de $t^{-1}g$ est $(\Delta^{m-1} \mid s'_1, \dots, s'_d, t_d)$ si $s'_1 \neq \Delta$ et $(\Delta^m \mid s'_2, \dots, s'_d, t_d)$ sinon.

En effet, J. W. Alexander montre en 1923 ([Ale23]) que tout entrelacs peut être vu comme une tresse fermée, c'est-à-dire une tresse comme celles que l'on a considérées dans l'introduction, mais dont on a recollé les extrémités des brins. Toutefois, cette correspondance n'est pas bijective, et deux tresses distinctes peuvent donner un même entrelacs une fois refermées. En fait, deux tresses distinctes seront isotopes une fois fermées si elles sont conjuguées en tant qu'éléments d'un groupe B_n .

Définition 3.2.1. Deux tresses g, g' dans B_n sont *conjuguées* s'il existe h dans B_n tel que $g = hg'h^{-1}$. Dans ce cas, on notera $g \simeq g'$.

Le problème de conjugaison est plus général et souvent plus difficile que celui des mots, et on se réjouit de pouvoir mobiliser ici la forme normale que l'on vient de construire pour y apporter une réponse. Commençons par un lemme facile mais primordial pour la suite.

Lemme 5. Deux tresses $g, g' \in B_n$ sont conjuguées si et seulement si elles sont positivement conjuguées, c'est-à-dire si et seulement s'il existe une tresse positive $c \in B_n^+$ telle que $g' = cgc^{-1}$.

Démonstration. Évidemment, si deux tresses sont positivement conjuguées alors elles sont conjuguées, il n'y a donc que le sens direct à traiter. Soient donc g, g' et h des tresses dans B_n telles que $g' = hgh^{-1}$. Par la proposition 2.3.2, il existe $m \in \mathbb{Z}$ et $a \in B_n^+$ tels que $h = \Delta^m a$ et, quitte à remplacer a par Δa , on peut supposer m pair. D'après le lemme 3, Δ^m et Δ^{-m} commutent alors avec tous les éléments de B_n , d'où :

$$g' = hgh^{-1} = a\Delta^m g \Delta^{-m} a^{-1} = aga^{-1},$$

et donc g et g' sont positivement conjuguées. □

Pour résoudre ce problème, on va chercher à être brutal, mais intelligemment. L'idée va être d'effectuer des recherches exhaustives sur des ensembles (très) gros, mais tout de même finis. On cherchera par la suite à raffiner ces ensembles le plus possible pour limiter le temps effectif de calcul d'une solution.

Définition 3.2.2. Pour tous entiers $p, q \in \mathbb{Z}$ avec $p \leq q$, on appellera *intervalle* $[p, q]_n$ le sous ensemble de B_n

$$[p, q]_n := \{g \in B_n \mid \Delta_n^p \preceq g \preceq \Delta_n^q\}.$$

Comme on l'a fait jusqu'à maintenant, on omettra parfois l'indice n lorsque le groupe de référence B_n sera clairement fixé au préalable.

L'objectif va être de montrer que les intervalles ainsi définis sont en quelque sorte "convexes" pour les relations de conjugaison, au sens où l'on va toujours pouvoir trouver un intervalle dans lequel on reste pendant toutes les étapes permettant de passer d'une tresse à une autre par des conjugaisons successives par des tresses simples. Le point crucial réside dans la proposition suivante.

Proposition 3.2.1. Soient $g, g' \in B_n$ et $c \in B_n^+$ tels que $g' = cgc^{-1}$, et soit $s := T(c)$ la tête de c . Alors $\inf(s^{-1}g's) \geq \min(\inf(g), \inf(g'))$.

Démonstration. Notons $m := \min(\inf(g), \inf(g'))$, $b \in B_n^+$ tel que $c = sb$ et t la tresse positive vérifiant $ts = \Delta$ (et donc $t = \Delta s^{-1}$), dont l'existence est assurée par la remarque suivant la définition 2.3.1 d'une tresse simple. Considérons enfin $a, a' \in B_n^+$ telles que $g = \Delta^m a$ et $g' = \Delta^m a'$. La condition de conjugaison reliant g et g' se réécrit $g'c = cg$, donc $\Delta^m a'c = c\Delta^m a$. En multipliant par t à gauche, on obtient $t\Delta^m a'c = tsb\Delta^m a = \Delta b\Delta^m a$. On utilise l'automorphisme flip des deux côtés de l'égalité pour ramener les tresses fondamentales aux extrémités des expressions puis simplifier celles-ci :

$$g'c = cg \Leftrightarrow \Delta^m \tau^m(t)a'c = \Delta^{m+1} \tau^m(b)a \Leftrightarrow \tau^m(t)a'c = \Delta \tau^m(b)a.$$

En particulier, la dernière écriture implique donc que Δ divise $\tau^m(t)a'c$ à gauche. Or, en tant que tresse simple, Δ divise une tresse si et seulement si elle divise sa tête, et par le lemme 4, $T(\tau^m(t)a'c) = T(\tau^m(t)a'T(c)) = T(\tau^m(t)a's)$. Ainsi, $\Delta \preceq \tau^m(t)a's$. En remultipliant des deux côtés par Δ^m , on obtient

$$\Delta^{m+1} \preceq \Delta^m \tau^m(t)a's = t\Delta^m a's = \Delta s^{-1}g's,$$

et donc finalement on a bien $\Delta^m \preceq s^{-1}g's$, et donc $\inf(s^{-1}g's) \geq m$ comme attendu. □

Une démonstration semblable montre un résultat similaire pour la borne supérieure d'une conjugaison par une tresse simple, qui est alors inférieure au maximum des bornes supérieures des deux tresses conjuguées. (En fait on peut prouver que pour toute tresse g , $\inf(g^{-1}) = -\sup(g)$ et $\sup(g^{-1}) = -\inf(g)$, ce qui montre que les deux bornes sont symétriques l'une de l'autre, et donc qu'intuitivement ce qui est valable pour l'une l'est aussi dans une version symétrisée pour l'autre.) Si on écrit la tresse conjugante positive c sous sa forme normale gloutonne $s_1 \dots s_d$, la proposition que l'on vient de démontrer et son équivalent pour la borne supérieure montrent que toutes les tresses $g, s_d g s_d^{-1}, s_{d-1} s_d g s_d^{-1} s_{d-1}^{-1}, \dots, g'$ appartiennent à l'intervalle $[\min(\inf(g), \inf(g')), \max(\sup(g), \sup(g'))]$. Autrement dit, si g et g' sont conjuguées dans B_n , alors elles le sont dans l'intervalle $[\min(\inf(g), \inf(g')), \max(\sup(g), \sup(g'))]$.

Il est commode de donner un nom à l'intervalle que l'on vient de considérer. Si on note $p := \min(\inf(g), \inf(g'))$ et $q := \max(\sup(g), \sup(g'))$, alors on écrira

$$\text{Conj}_{p,q}(g) := \{h \in [p, q] \mid h \simeq g\}.$$

Ainsi, g et g' seront conjuguées si et seulement si g' appartient à l'ensemble $\text{Conj}_{p,q}(g)$. Pour apporter une solution (au moins théorique) au problème de conjugaison, il suffit donc de trouver un algorithme permettant de construire une liste exhaustive des tresses de tels ensembles.

Tout d'abord, les ensembles $\text{Conj}_{p,q}(g)$ sont finis. En effet, d'après la proposition 3.1.2, toute tresse dans $[p, q]$ s'écrit $\Delta^p a$ avec a dans B_n^+ telle que $a \preceq \Delta^{q-p}$. Cela implique que la longueur de a soit inférieure à $|\Delta|(p - q)$, avec $|\Delta| = \frac{n(n-1)}{2}$ si l'on se place dans B_n . Un mot de $[p, q]$ s'écrit donc comme le produit de Δ^p et d'un mot positif d'au plus $\frac{n(n-1)}{2}$ lettres dans $\{\sigma_1, \dots, \sigma_{n-1}\}$, et le cardinal de $[p, q]$ (et par conséquent celui de $\text{Conj}_{p,q}(g)$ qui en est un sous-ensemble) est donc majoré par $(n-1)^{n(n-1)(p-q)/2}$.

Pour construire $\text{Conj}_{p,q}(g)$ on part de $X_0 := \{g\}$ puis on pose successivement, pour tout entier positif k , $X_{k+1} := \{shs^{-1} \mid h \in X_k, s \text{ simple et } shs^{-1} \in [p, q]\}$. La suite $(X_k)_k \geq 0$ est donc une suite d'ensembles croissante pour l'inclusion, dont tous les éléments ont un cardinal majoré par une même borne. Il existe donc un entier N tel que $X_N = X_{N+1}$, et donc $X_N = \text{Conj}_{p,q}(g)$.

Le problème de conjugaison des groupes de tresses est donc décidable! Malheureusement, cette méthode est absolument désastreuse en pratique, les ensembles mis en jeu devenant très rapidement absolument gargantuesques. À titre indicatif, la taille de l'intervalle $[-3, 3]$ est 234 dans B_3^+ , 45.252 dans B_4^+ , de l'ordre de 29 millions dans B_5^+ et environ $49 \cdot 10^9$ dans B_6^+ .

3.3 L'ensemble super-sommital

Comme dit en introduction, la question de l'existence d'un algorithme résolvant le problème de conjugaison des groupes de tresses en un temps polynomial reste aujourd'hui encore ouverte. Toutefois, cela ne nous empêche pas d'améliorer sensiblement la méthode que l'on vient de voir et qui est, en terme de complexité, tout simplement calamiteuse. Nous allons étudier ici un raffinement de la première méthode, présenté en 1994 par El-Rifai et Morton dans [[EM94]], qui consiste à introduire un sous-ensemble de $\text{Conj}_{p,q}(g)$ le "plus petit possible" en un certain sens, l'*ensemble super-sommital* (en anglais, *super summit set* ou *SSS*).

Définition 3.3.1. Soit g une tresse dans B_n . Posons $\inf^\sim(g) := \max\{\inf(g') \mid g' \simeq g\}$ et $\sup^\sim(g) := \min\{\sup(g') \mid g' \simeq g\}$. L'*ensemble super-sommital* de g est alors l'ensemble des tresses conjuguées à g appartenant à l'intervalle $[\inf^\sim(g), \sup^\sim(g)]$:

$$SSS(g) := \{g' \in [\inf^\sim(g), \sup^\sim(g)] \mid g' \simeq g\}.$$

Deux opérations duales l'une de l'autre vont jouer un rôle clé dans la construction des ensembles super-sommitaux, le *cyclage* et le *décyclage*.

Définition 3.3.2. Soit $g \in B_n$ une tresse de forme Δ -normale $(\Delta^m \mid s_1, \dots, s_d)$. Le *cyclage* et le *décyclage* de g sont alors définis comme

$$\begin{aligned} \text{cycl}(g) &:= \Delta^m s_2 \dots s_d \tau^m(s_1), \\ \text{decycl}(g) &:= \Delta^m \tau^m(s_d) s_1 \dots s_{d-1}. \end{aligned}$$

Remarques. — En général, une tresse à laquelle on vient d'appliquer un cyclage ou décyclage n'est pas sous forme normale. Pour appliquer successivement ces opérations comme on le fera plus loin, il faudra donc veiller à remettre les tresses sous forme Δ -normale entre chaque étape.

— Le cyclage et le décyclage de g sont en fait des conjugaisons de cette tresse, respectivement :

$$\text{cycl}(g) = \tau^{-m}(s_1) g \tau^m(s_1)$$

$$\text{et } \text{decycl}(g) = s_d g s_d^{-1}.$$

- On dispose de plus de la formule suivante, qui relie directement ces deux opérations "duales" (et grâce à laquelle on se permettra de ne détailler les calculs que d'une seule des deux opérations dans les prochaines preuves) :

$$\text{decycl}(g)^{-1} = \tau(\text{cycl}(g^{-1})).$$

Le point le plus délicat à éluder concernant les ensembles super-sommitaux est de montrer que ceux-ci ne sont pas vides et, plus exactement, de réussir à construire une tresse dans de tels ensembles. Une telle construction va être rendue possible par le théorème suivant :

Théorème 2. Soit $g \in B_n$. S'il existe au moins une tresse g' conjuguée à g telle que $\inf(g') > \inf(g)$ (resp. $\sup(g') < \sup(g)$), alors il existe un entier p tel que $\inf(\text{cycl}^p(g)) > \inf(g)$ (resp. $\sup(\text{decycl}^p(g)) < \sup(g)$).

Démonstration. Considérons donc g et g' deux tresses conjuguées avec $\inf(g') > \inf(g)$. Pour tout entier $l \in \mathbb{N}$, on écrira $g \simeq_l g'$ pour signifier que g et g' sont conjuguées via une tresse positive de longueur inférieure ou égale à l (cf. remarque de la proposition 2.2.1). Nous allons montrer par récurrence sur le nombre de lettres d'une tresse positive conjuguante :

$$\forall l \in \mathbb{N}, \exists g' \in B_n, \inf(g') > \inf(g) \text{ et } g \simeq_l g' \Rightarrow \exists p \leq l, \text{ tel que } \inf(\text{cycl}^p(g)) > \inf(g),$$

ce qui est un énoncé parfaitement équivalent à celui formulé pour l'énoncé du théorème.

Tout d'abord, en vertu du lemme 5, il existe une tresse positive $c \in B_n^+$ telle que $g' = cgc^{-1}$. Soit donc c une telle tresse et l sa longueur.

Le cas $l = 0$ est trivial, puisque $g \simeq_0 g'$ implique $g = g'$ et dès lors la condition $\inf(g') > \inf(g)$ n'est jamais satisfaite.

Supposons $l > 0$ et la proposition démontrée pour les conjugaisons par une tresse de longueur strictement inférieure à l . Si en effectuant un seul cyclage on a déjà réussi à "faire monter la borne inférieure", c'est-à-dire si $\inf(\text{cycl}(g)) > \inf(g)$, alors la proposition est d'ores et déjà vérifiée en prenant $p = 1$. Sinon, on va montrer qu'alors il existe $l_1 < l$ tel que $\tau(g') \simeq_{l_1} \text{cycl}(g)$, dans le but d'appliquer l'hypothèse de récurrence à cette relation. Notons $m := \inf(g)$ et considérons $a, a' \in B_n$ telles que $g = \Delta^m a$ et $g' = \Delta^m a'$, avec donc $\Delta \not\preceq a$ et, nécessairement, $\Delta \preceq a'$. On a alors :

$$\Delta^m a' c = c \Delta^m a = \Delta^m \tau^m(c) a,$$

et donc en simplifiant par Δ^m , $a' c = \tau^m(c) a$. Comme Δ divise a' , on déduit de cette dernière égalité que Δ divise $\tau^m(c) a$. Si on note s_1 la tête de a , on obtient à l'aide du lemme 4 et par le fait qu'en tant que tresse simple il est équivalent pour Δ de diviser une tresse ou de diviser sa tête : $\Delta \preceq \tau^m(c) s_1$. En appliquant le flip (qui est l'opérateur de conjugaison par Δ et qui laisse donc cette tresse inchangée) m fois et en tenant compte du fait que τ^{2m} est l'identité (par le lemme 3), on a enfin $\Delta \preceq c \tau^m(s_1)$.

Pour simplifier la lecture (et l'écriture) des dernières lignes de cette preuve, notons $s := \tau^m(s_1)$. On a donc $\Delta \preceq cs$, et on peut donc considérer $c_1 \in B_n^+$ tel que $\Delta c_1 = cs$. Nous allons voir que $|c_1| < l$ et que $\tau(g') = c_1 \text{cycl}(g) c_1^{-1}$; c'est bien ce que l'on cherche à montrer.

Premièrement, on sait que $\Delta \not\preceq a$, et donc que $\Delta \not\preceq s_1$. D'autre part, s_1 étant simple, on a $s_1 \preceq \Delta$. Ces deux points impliquent que la longueur de s_1 , et donc celle de s qui lui est égale, sont inférieures à celle de Δ : $|s| < |\Delta|$. Comme on a en même temps $\Delta c_1 = cs$, et donc $|\Delta c_1| = |cs|$, il vient $|c_1| < |c| = l$.

Le deuxième point résulte simplement de cette suite d'égalités.

$$\Delta \tau(g') c_1 = g' \Delta c_1 = g' cs = cgs = cs \cdot \text{cycl}(g) = \Delta c_1 \text{cycl}(g).$$

On a utilisé successivement la proposition 2.2.2, l'égalité $\Delta c_1 = cs$, le fait que $g'c = cg$, le premier point de la remarque suivant la définition 3.3.2 du (dé)cyclage et enfin encore l'égalité $\Delta c_1 = cs$. En simplifiant les deux termes extrêmes par Δ , on a bien le résultat escompté : $\tau(g') = c_1 \text{cycl}(g) c_1^{-1}$, i.e. $g' \simeq_{l_1} g$.

De plus, appliquer le flip à une tresse ne modifiant sa borne inférieure (on peut s'en convaincre par exemple à l'aide du premier point de la proposition 3.1.2), on a $\inf(\tau(g')) = \inf(g')$ d'une part et, ici, $\inf(\text{cycl}(g)) = \inf(g)$ d'autre part par hypothèse. Comme, toujours par hypothèse, on a $\inf(g') > \inf(g)$, on a donc également $\inf(\tau(g')) > \inf(\text{cycl}(g))$. Les vérifications étant faites, appliquons maintenant l'hypothèse de récurrence à la relation $\text{cycl}(g) \simeq_{l_1} \tau(g')$:

$$\exists p_1 \leq l_1 \text{ tel que } \inf(\text{cycl}^{p_1}(\text{cycl}(g))) > \inf(\text{cycl}(g)).$$

Comme $\inf(\text{cycl}(g)) = \inf(g)$ par hypothèse, en considérant $p := p_1 + 1$, on a finalement :

$$\exists p \leq l \text{ tel que } \inf(\text{cycl}^p(g)) > \inf(g),$$

ce qui achève la démonstration (la contrepartie pour la borne supérieure se déduisant de ce que l'on vient de faire par le fait que $\text{decycl}(g)^{-1} = \tau(\text{cycl}(g^{-1}))$ et que $\sup(g^{-1}) = -\inf(g)$). $\square$

Pour construire l'ensemble super-sommital d'une tresse g , on commence par cycliser g jusqu'à atteindre une tresse g_1 telle que $\inf(g_1) = \inf^\sim(g)$. Puis on décyclise g_1 autant de fois que nécessaire pour obtenir une tresse g_2 , conjuguée à g puisqu'obtenue après des conjugaisons successives de cette dernière, vérifiant $\sup(g_2) = \sup^\sim(g)$. De plus, par définition les opérations de cyclage/décyclage laissent stables les intervalles de tresses, et en particulier pour toute tresse a , $\inf(\text{cycl}(a)) \geq \inf(a)$. Ici, on a donc $\inf(g_2) \geq \inf(g_1) = \inf^\sim(g)$, et donc nécessairement $\inf(g_2) = \inf^\sim(g)$, d'où finalement $g_2 \in SSS(g)$.

Une fois une tresse de l'ensemble super-sommital trouvée, on peut terminer de le construire entièrement en considérant successivement toutes les tresses conjuguées par une tresse simple à g_2 vérifiant encore les hypothèses sur les bornes optimales, puis recommencer en conjugant les nouvelles tresses trouvées par des simples et ainsi de suite, de façon similaire à ce que l'on avait fait pour construire les ensembles $\text{Conj}_{p,q}(g)$.

Par construction, les ensembles super-sommitaux sont des invariants exacts de conjugaison. Ainsi, une fois l'ensemble $SSS(g)$ construit, pour décider si une tresse g' est conjuguée à g , il suffit de déterminer une tresse g'_2 dans $SSS(g')$ (par exemple via des cyclages et décyclages successifs) et de vérifier si elle se trouve dans l'ensemble super-sommital de g .

3.4 Borne sur le nombre de cyclages et décyclages

Une question légitime émerge toutefois à la lecture de la présentation de l'algorithme que l'on vient de donner. Certes, on a montré que s'il était possible de "faire monter" l'infimum dans la classe de conjugaison, alors en cyclant "assez longtemps" on finirait toujours par y arriver, mais pour l'instant on n'a pas d'idée a priori sur combien de fois il faut (dé)cycliser pour atteindre une tresse avec des bornes plus optimales, ni à partir de combien d'étapes on peut affirmer que l'on a atteint la limite de l'ensemble super-sommital.

Une réponse à cette interrogation a été apportée en 2000 par Birman, Ko et Lee dans [BKL01]. Dans cette dernière partie, nous reprenons leur preuve du théorème au cœur de leur article.

Théorème 3. Soit g une tresse dans B_n . Si $\inf(g) \leq \inf^\sim(g)$, alors $\inf(\text{cycl}^{|\Delta_n|-1}(g)) > \inf(g)$.

Remarques. — Un théorème sensiblement identique existe bien sûr pour le décyclage et la borne supérieure, et le nombre maximum d'étapes à réaliser avant d'observer un changement est le même.

- Rappelons que la longueur d'une tresse Δ_n est $|\Delta_n| = \frac{n(n-1)}{2}$. Ce théorème nous assure donc que la partie de l'algorithme consistant à construire une tresse de l'ensemble super-sommital s'effectue en un temps polynomial (plus précisément, quadratique en le nombre de brins par cette borne, et quadratique en la longueur du mot de tresse initial puisqu'il faut recalculer une forme normale après chaque (dé)cyclage).

Lorsque l'on cycle une tresse g écrite sous forme Δ -normale, on n'opère de changements que sur la partie "positive" exprimée comme suite normale de tresses simples. D'après le théorème 2, il existe un entier positif u tel que $\inf(\text{cycl}^u(g)) = \inf(g)$ et $\inf(\text{cycl}^{u+1}(g)) > \inf(g)$. On va considérer une certaine tresse b permettant de relier g à $\text{cycl}^{u+1}(g)$ et étudier son écriture sous forme normale, afin d'en exhiber une liste de facteurs "canoniques" de longueurs strictement décroissantes. On montrera que le nombre de tels facteurs sera à la fois relié au nombre de cyclages d'une part, et majoré par la taille de la tresse fondamentale d'autre part, ce qui nous permettra de conclure.

Commençons par montrer l'existence de la première tresse qui nous intéresse.

Lemme 6. Soit g une tresse dans B_n dont la forme normale s'écrit $g = \Delta^u a$ avec $u = \inf(g)$ et a une tresse positive. Alors

$$\inf^\sim(g) > \inf(g) \Leftrightarrow \exists b \in B_n^+, \Delta \preceq ba\tau^u(b^{-1}).$$

Démonstration. Si $\inf^\sim(g) > \inf(g)$, alors il existe x dans B_n tel que $\inf(xgx^{-1}) > \inf(g)$. Écrivons $x = \Delta^v y$ avec y positive et $v = \inf(x)$. Alors $\Delta^{u+1} \preceq \Delta^v y \Delta^u a y^{-1} \Delta^{-v}$ d'où, en multipliant par Δ^{-v} à gauche et par Δ^v à droite et en simplifiant Δ^u après avoir appliqué le flip,

$$\Delta \preceq \tau^u(y) a y^{-1}.$$

En posant $b := \tau^u(y)$ on a bien le résultat recherché. $\square$

Avant de passer à l'étude de la tresse b en tant que telle, continuons à montrer quelques lemmes préliminaires.

Lemme 7. Si g est une tresse dans B_n et s une tresse simple, alors $\inf(g) \leq \inf(gs) \leq \inf(g) + 1$.

Démonstration. Cela résulte du fait que, par définition de l'infimum, $\inf(g\Delta) = \inf(g) + 1$, que $g \preccurlyeq gs \preccurlyeq g\Delta$ puisque s est simple et que l'infimum préserve l'ordre induit par la divisibilité. $\square$

Dans la suite on notera, pour s simple, $\tilde{s}$ l'unique tresse simple telle que $\tilde{s}s = \Delta$.

Lemme 8. Soit z une tresse positive de forme normale $z = t_l t_{l-1} \dots t_1$. Alors la tresse $z^{-1}\Delta^l$ est positive, de forme normale $z^{-1}\Delta^l = \tau(\tilde{t}_1)\tau^2(\tilde{t}_2) \dots \tau^l(\tilde{t}_l)$.

Démonstration. Observons tout d'abord que l'égalité $\Delta = \tilde{t}_i t_i$ implique pour tout i , $\Delta = \tau^i(\tilde{t}_i = \tau^i(t_i))$. Ainsi, partant de la première égalité, en faisant translater petit-à-petit Δ^l dans le reste de l'expression, puis en utilisant le fait que τ est un morphisme, on a :

$$\begin{aligned} z^{-1}\Delta^l &= t_1^{-1} \dots t_l^{-1} \Delta^l \\ &= (\Delta\tau(t_1^{-1}))(\Delta\tau^2(t_2^{-1})) \dots (\Delta\tau^l(t_l^{-1})) \\ &= \tau(\tilde{t}_1)\tau(t_1)\tau(t_1^{-1})\tau^2(\tilde{t}_2)\tau^2(t_2)\tau^2(t_2^{-1}) \dots \tau^l(\tilde{t}_l)\tau^l(t_l)\tau^l(t_l^{-1}) \\ &= \tau(\tilde{t}_1)\tau^2(\tilde{t}_2) \dots \tau^l(\tilde{t}_l). \end{aligned}$$

$\square$

La combinaison du théorème 2 et du lemme 7 nous permet de considérer un entier positif m tel que $\inf(\text{cycl}^m(g)) = \inf(g)$ et $\inf(\text{cycl}^{m+1}(g)) = \inf(g) + 1$. Pour conclure, il nous reste à montrer que ce m est majoré par $|\Delta| - 1$.

Considérons, par le lemme 6, une tresse positive b de longueur minimale telle que $\Delta \preccurlyeq ba\tau^m(b^{-1})$, où $\Delta^u a$ est l'écriture sous forme normale de g . On va chercher à identifier des facteurs canonique dans l'écriture de b . Observons tout d'abord le fait suivant :

Lemme 9. La borne inférieure de la tresse b considérée est nulle :
 $\inf(b) = 0$.

Démonstration. Si ce n'était pas le cas, on pourrait écrire $b = \Delta b'$ avec b' une tresse positive, et on aurait alors :

$$b' a \tau^u(b'^{-1}) = \Delta^{-1} b a \tau^u(b^{-1}) \Delta = \tau(b a \tau^u(b^{-1})),$$

avec Δ qui divise le dernier terme, ce qui contredit l'hypothèse de longueur minimale de b , puisque $|b'| < |b|$. $\square$

Intéressons nous maintenant plus en détails à l'écriture de b .

Proposition 3.4.1. Notons pour tout i dans $\{0, \dots, m+1\}$, $\text{cycl}^i(g) = \Delta^u s_i a_i$, où s_i est la tête de la partie positive de l'écriture de la forme Δ -normale de $\text{cycl}^i(g)$. Alors la tresse positive b de longueur minimale fournie par le lemme 6 s'écrit

$$b = \tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) \tilde{s}_0.$$

Démonstration. On part de la relation $\Delta \preccurlyeq ba\tau^u(b^{-1})$ qui implique $\Delta \preccurlyeq ba$ puisque $\tau^u(b^{-1})$ est négative. Par le lemme 4, on en déduit $\Delta \preccurlyeq bs_0$, et donc $b = b_1 \tilde{s}_0$ pour une certaine tresse positive b_1 (rappelons que lorsque la tresse fondamentale est en jeu, il y a équivalence entre les notions de division à gauche et à droite). On a alors :

$$\begin{aligned} bs_0 a_0 \tau^u(b^{-1}) &= b_1 \tilde{s}_0 s_0 a_0 \tau^u(\tilde{s}_0^{-1}) \tau^u(b_1^{-1}) \\ &= b_1 \Delta a_0 \tau^u(s_0) \tau^u(s_0^{-1}) \tau^u(\tilde{s}_0^{-1}) \tau^u(b_1^{-1}) \\ &= b_1 \tau(s_1 a_1) \tau^u(b_1^{-1}), \end{aligned}$$

en utilisant, pour la dernière égalité, le fait que $\tau^u(s_0^{-1}) \tau^u(\tilde{s}_0^{-1}) = \Delta^{-1}$, que par définition $a_0 \tau^u(s_0) = \text{cycl}(s_0 a_0) = s_1 a_1$ et que le morphisme τ est l'automorphisme de conjugaison associé à Δ (cf. proposition 2.2.2).

Comme Δ divise le premier membre de cette suite d'égalités, il vient $\Delta \preccurlyeq b_1 \tau(s_1 a_1) \tau^u(b_1^{-1})$, donc $\Delta \preccurlyeq b_1 \tau(s_1 a_1)$

car le dernier élément est négatif, puis par le lemme 4, $\Delta \preccurlyeq b_1 \tau(s_1)$. On en déduit donc l'existence d'une tresse positive b_2 telle que $b_1 = b_2 \tau(\tilde{s}_1)$, puis en répétant les mêmes opérations on écrit $b_2 = b_3 \tau^2(\tilde{s}_2), \dots, b_m = b_{m+1} \tau^m(\tilde{s}_m)$ avec pour tout i , b_i une tresse positive.

En combinant toutes ces écritures, on obtient finalement $b = b_{m+1} \tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) \tilde{s}_0$. Posons $\hat{s} := \tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) \tilde{s}_0$, de sorte que $b = b_{m+1} \hat{s}$. On a alors nécessairement $|b| > |\hat{s}|$.

D'autre part, un calcul direct montre que $\tau^{m+1}(\hat{s} a \tau^u(\hat{s}^{-1})) = s_{m+1} a_{m+1}$.

Comme $\inf(\text{cycl}^{m+1}(g)) = \inf(g) + 1$ et que $\inf(b) = 0$ (lemme 9), on a $\inf(s_{m+1} a_{m+1}) = 1$, et donc $\inf(\hat{s} a \tau^u(\hat{s}^{-1})) = \inf(\tau^{m+1}(s_{m+1} a_{m+1})) = 1$. La tresse $\hat{s}$ vérifie donc les conditions du lemme 6, et par conséquent par minimalité de $|b|$ on doit avoir $b_{m+1} = \epsilon$, et donc $b = \hat{s}$, ce qui est bien le résultat attendu. $\square$

L'expression que l'on vient d'établir pour b n'est en général pas sous forme normale, on va donc s'intéresser aux têtes des termes successifs composant l'écriture $\tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) \tilde{s}_0$.

Posons donc, pour tout k dans $\{0, \dots, m\}$, $h_k := T(\tau^m(\tilde{s}_m) \dots \tau^k(\tilde{s}_k))$.

Dans l'énoncé suivant, on écrira " $g_1 \prec g_2$ " pour signifier " $g_1 \preccurlyeq g_2$ et $g_1 \neq g_2$ ".

Proposition 3.4.2. Les tresses h_k sont positives et vérifient

$$h_m \prec h_{m-1} \prec \dots \prec h_0 \prec \Delta.$$

Démonstration. Tout d'abord, les tresses h_k sont positives en tant que tresses simples. Ensuite, d'après le lemme 9, $\inf(b) = 0$, donc h_0 , qui n'est autre que la tête de b , ne peut être égale à Δ , i.e. $h_0 \prec \Delta$.

Par définition des h_k , on a déjà $h_m \preccurlyeq h_{m-1} \preccurlyeq \dots \preccurlyeq h_0$. Il nous reste à montrer que pour tout k dans $\{0, \dots, m-1\}$, $h_k \neq h_{k+1}$. On détaille la preuve pour $k = 0$, les autres cas étant essentiellement les mêmes.

Raisonnons par l'absurde et supposons $h_1 = h_0$. On va montrer que cela entraîne une contradiction avec le choix de la tresse b .

On sait par la proposition 3.4.1 que $b = \tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) \tilde{s}_0$, et considérons de plus la forme normale de b que l'on va écrire $(t_l, \dots, t_1)$. On a donc :

$$\tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) \tilde{s}_0 = t_l \dots t_1.$$

De plus, d'après le lemme 8, la forme normale de $b^{-1} \Delta$ est $b^{-1} \Delta = \tau(\tilde{t}_1) \tau^2(\tilde{t}_2) \dots \tau^l(\tilde{t}_l)$. Par définition de h_1 comme tête de $\tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1)$, il existe une tresse positive r_1 telle que $\tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) = h_1 r_1$. Par hypothèse, $h_1 = h_0 = t_l$, donc

$$\tau^m(\tilde{s}_m) \dots \tau(\tilde{s}_1) = h_0 r_1 = t_l r_1.$$

D'autre part, comme $t_l b_1 \tilde{s}_0 = b = t_l \dots t_1$ avec b_1 défini comme dans la preuve de la proposition 3.4.1, il vient $t_{l-1} \dots t_1 = b_1 \tilde{s}_0$. Ainsi, en nous rappelant du fait que $a = s_0 a_0$, on a $t_{l-1} \dots t_1 a = b_1 \tilde{s}_0 s_0 a_0 = b_1 \Delta a_0$, d'où on déduit $\Delta \preccurlyeq t_{l-1} \dots t_1 a$.

On pose maintenant pour tout i dans $\{0, \dots, l\}$, $\alpha_i := \inf(t_{l-1} \dots t_1 a \tau^u(\tau(\tilde{t}_1) \tau^2(\tilde{t}_2) \dots \tau^i(\tilde{t}_i)))$. On a alors :

- $\alpha_0 \geq 1$ puisque $\Delta \preccurlyeq t_{l-1} \dots t_1 a$,
- pour tout i , $\alpha_i \leq \alpha_{i+1} \alpha_i + 1$ d'après le lemme 7, et
- si, pour un certain i , $\alpha_i = \alpha_{i+1}$, alors $\alpha_i = \alpha_{i+1} = \dots = \alpha_l$, car toutes les suites $(\tau^i(\tilde{t}_i), \tau^{i+1}(\tilde{t}_{i+1}))$ sont normales¹.

Si α_{l-1} était inférieur ou égal à l , alors on aurait (en appliquant le lemme 8) $\Delta \preccurlyeq t_{l-1} \dots t_1 a \tau^u(t_{l-1} \dots t_1)^{-1}$, ce qui contredirait une fois de plus l'hypothèse de minimalité de $|b|$. Ainsi $\alpha_{l-1} \leq l-1$, et il existe donc $i \leq l-2$ tel que $\alpha_i = \alpha_{i+1}$ et donc $\alpha_i = \alpha_{i+1} = \dots = \alpha_l \leq l-1$, ce qui implique $\inf(b a \tau^u(b^{-1})) \leq 0$. Cette dernière inégalité est absurde puisque par hypothèse $\Delta \preccurlyeq b a \tau^u(b^{-1})$. En remontant la preuve on conclut que, nécessairement, $h_1 \prec h_0$.

Pour démontrer les cas $k > 0$, on refait exactement la même chose en faisant jouer à $g_k := \text{cycl}^k(g) =: \Delta^u s_k a_k$ le rôle de g . $\square$

1. Intuitivement, la forme normale gloutonne consiste à écrire la plus grande tresse simple possible à chaque étape. Ainsi, si à un moment il n'y a "plus de place" pour insérer des itérations de la tresse fondamentale, alors il est impossible que cela puisse se faire plus tard. La forme normale gloutonne force les apparitions éventuelles de Δ à se produire "le plus tôt possible".

Concluons la preuve du théorème. On a par la proposition 3.4.2 :

$$0 < |h_m| < \dots < |h_0| < |\Delta|.$$

Ainsi la longueur de cette chaîne $(m+1)$ doit être inférieure à $|\Delta|$, ce qui entraîne bien $m \leq |\Delta| - 1$. $\square$

Références

- [Deh19] Patrick DEHORNOY. “Le calcul des tresses”. In : *Calvage & Mounet, Paris* (2019).
- [GAR69] F. A. GARSIDE. “THE BRAID GROUP AND OTHER GROUPS”. In : *The Quarterly Journal of Mathematics* 20.1 (jan. 1969), p. 235-254. ISSN : 0033-5606. DOI : 10.1093/qmath/20.1.235. eprint : <https://academic.oup.com/qjmath/article-pdf/20/1/235/4400004/20-1-235.pdf>. URL : <https://doi.org/10.1093/qmath/20.1.235>.
- [Ale23] James W ALEXANDER. “A lemma on systems of knotted curves”. In : *Proceedings of the National Academy of Sciences* 9.3 (1923), p. 93-95.
- [EM94] Elsayed A ELRIFAI et Hugh R MORTON. “Algorithms for positive braids”. In : *Quarterly Journal of Mathematics* 45.180 (1994), p. 479-497.
- [BKL01] Joan S BIRMAN, Ki Hyoung KO et Sang Jin LEE. “The infimum, supremum, and geodesic length of a braid conjugacy class”. In : *Advances in Mathematics* 164.1 (2001), p. 41-56.