Séminaire BOURBAKI Novembre 1999
52ème année, 1999–2000, n° 865

L'ORDRE DE DEHORNOY SUR LES TRESSES

par **Christian KASSEL**

Une des découvertes récentes les plus intéressantes et inattendues concernant le groupe des tresses B_n d'Artin est due à Dehornoy qui a démontré fin 1991 que B_n a un ordre total invariant par multiplication à gauche. Il en résulte notamment que l'anneau du groupe B_n n'a pas de diviseurs de zéro. Dehornoy déduit cet ordre de l'étude générale des systèmes autodistributifs, définis comme des ensembles munis d'une loi de composition vérifiant l'identité $x(yz) = (xy)(xz)$. Des travaux sur un axiome indémontrable de théorie des ensembles avaient mis en évidence un système autodistributif remarquable et suggéré que l'étude de tels systèmes devait donner des résultats non triviaux.

Fenn, Greene, Rolfsen, Rourke et Wiest ont donné en 1997 une construction géométrique de l'ordre de Dehornoy. Leurs techniques ont permis également de mettre des structures d'ordre sur des groupes de difféotopies de surfaces. Plus récemment, Thurston a indiqué comment construire un ordre total sur B_n en utilisant les travaux de Nielsen sur les surfaces.

Le but de cet exposé est de présenter ces travaux ainsi que le lien inattendu avec la théorie des ensembles. Au n° 1 nous énonçons le résultat principal sur l'ordre des tresses et quelques propriétés de cet ordre. Les deux numéros suivants sont consacrés à une présentation des techniques de Dehornoy et à sa démonstration du résultat principal ; le lien entre tresses et systèmes autodistributifs est exposé au n° 2 tandis qu'au n° 3 nous étudions deux systèmes autodistributifs particulièrement importants. Au n° 4 nous indiquons comment l'étude des grands cardinaux en théorie des ensembles a été à l'origine de ces travaux. La construction géométrique de Fenn *et al.* ainsi que l'approche à la Nielsen seront présentées au n° 5. Pour plus de détails, le lecteur pourra consulter les références citées, et notamment la monographie [D00] en cours d'achèvement.

Thomas Delzant m'a aidé à comprendre l'idée de Thurston et à mettre le n° 5.2 en forme. Je le remercie très chaleureusement ainsi que Patrick Dehornoy, Dale Rolfsen et Bertold Wiest qui m'ont fait profiter de leurs commentaires.

1. LES RÉSULTATS PRINCIPAUX

Dans ce numéro nous rappelons la définition des groupes de tresses et celle des groupes ordonnables avant d'énoncer le théorème principal de Dehornoy impliquant l'existence d'un ordre sur les tresses.

1.1. Le groupe des tresses d'Artin. Soit n un entier ≥ 2. Définissons B_n comme le groupe engendré par $n-1$ générateurs $\sigma_1, \ldots, \sigma_{n-1}$ soumis aux relations

$$\sigma_i \sigma_j = \sigma_j \sigma_i \tag{1.1}$$

si $|i-j| > 1$ et

$$\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \tag{1.2}$$

si $|i-j| = 1$. On utilisera souvent le mot *tresse* pour désigner un élément de B_n.

E. Artin a introduit le groupe B_n dans les années 1920 et a résolu le problème des mots[1] pour ce groupe (voir [A26], [A47]). En 1967 Garside [Ga] résout à la fois ce problème et le problème de conjugaison[1] (voir aussi [Mk]). D'autres solutions ont été proposées, fondées notamment sur une forme normale due à Adyan [Ad], et redécouverte un peu plus tard par ElRifai et Morton [EM] et par Thurston, ce dernier élaborant à cette occasion la théorie des groupes automatiques et établissant l'automaticité de B_n (les résultats de Thurston sont exposés au chapitre 9 de [E+]). Rappelons aussi que les groupes de tresses jouent un rôle important dans des branches des mathématiques aussi diverses que la théorie des nœuds, la théorie de l'homotopie, la géométrie algébrique, la théorie des groupes, celle des représentations, *etc.* (on trouvera un reflet de cette diversité dans [B+] et dans [Ca]).

Un *mot de tresse* w est un mot formé à partir des générateurs $\sigma_1, \ldots, \sigma_{n-1}$ et de leurs inverses. Il est commode de représenter w par une configuration plane formée par n intervalles, appelés les brins de w, plongés de manière lisse dans une bande verticale bornée du plan. Une telle configuration s'obtient comme suit.

[1] Résoudre le problème des mots (resp. le problème de conjugaison) dans un groupe, c'est trouver un algorithme permettant de reconnaître ou de décider si deux mots donnés représentent ou non le même élément dans le groupe (resp. la même classe de conjugaison).

(a) On représente le générateur σ_i et son inverse σ_i^{-1} par les configurations de la figure 1. Le croisement de la configuration de σ_i (resp. de σ_i^{-1}) est dit *positif* (resp. *négatif*).

(b) Si D est la configuration associée au mot w et D' celle du mot w', alors la configuration associée à ww' est obtenue en plaçant D au-dessus de D' et en joignant les extrémités inférieures des brins de D aux extrémités supérieures de D'.

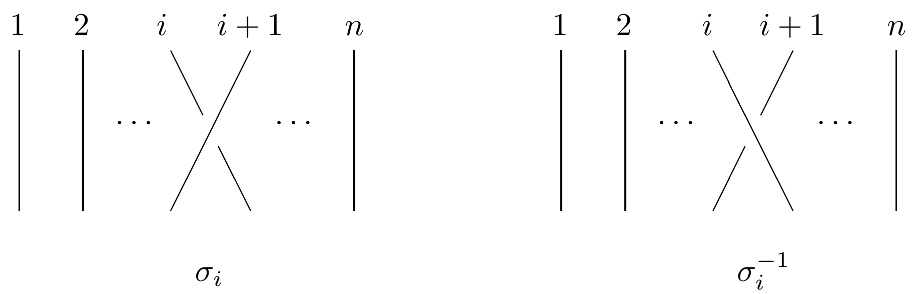


Figure 1

1.2. Groupes ordonnables. 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 (c'est-à-dire $a < b \Rightarrow ac < bc$), on dit que le groupe est *biordonnable*.

Pour tout groupe ordonnable G, notons P l'ensemble $\{x \in G \mid x > 1\}$ de ses éléments positifs. Le caractère total de l'ordre se traduit par la partition $G = P \amalg \{1\} \amalg P^{-1}$ où $P^{-1} = \{x \in G \mid x^{-1} \in P\}$. L'invariance par multiplication à gauche se traduit par $P^2 \subset P$, 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

$$G = P \amalg \{1\} \amalg P^{-1} \quad \text{et} \quad P^2 \subset P,$$

alors G est ordonnable pour l'ordre défini par $x < y$ si $x^{-1}y \in P$. L'ordre en question fait de G un groupe biordonnable si et seulement si $xPx^{-1} \subset P$ pour tout $x \in G$.

L'ordonnabilité d'un groupe a de nombreuses conséquences (voir [MR], chap. 7 ou [Pa], chap. 13). D'abord, tout groupe ordonnable G est sans torsion. Si, de plus, R est un anneau sans diviseurs de zéro, alors l'algèbre du groupe $R[G]$ n'a pas de diviseurs de zéro (elle vérifie donc une fameuse conjecture de Kaplansky). Il en résulte que les seuls idempotents de $R[G]$ sont triviaux, à savoir 0 ou 1. En outre, les seuls éléments inversibles de $R[G]$ sont triviaux, c'est-à-dire de la forme rx où r est un élément inversible de R et $x \in G$.

Les groupes libres de type fini, les groupes fondamentaux de surfaces fermées, les groupes abéliens libres de type fini sont biordonnables. Pour ce qui concerne les tresses, les groupes B_n ne sont pas biordonnables alors que les groupes de tresses pures le sont (*cf.* [KR] et [RZ]).

1.3. L'ordre de Dehornoy sur B_n. Pour $i \in \{1, \ldots, n-1\}$, on dit qu'un mot de la forme $w_0\sigma_i w_1\sigma_i \ldots \sigma_i w_r$ est σ_i-positif si les sous-mots $w_0, w_1, \ldots, w_r$ sont des mots dans les lettres $\sigma_j^{\pm 1}$ avec $j > i$. En d'autres termes, dans un mot σ_i-positif, le générateur σ_i d'indice minimal n'apparaît qu'avec des puissances positives. S'il n'apparaît qu'avec des puissances négatives, on dit que le mot est σ_i-négatif (donc un mot est σ_i-négatif si son inverse est σ_i-positif). Une tresse est dite σ_i-positive (resp. σ_i-négative) si elle peut être représentée par un mot σ_i-positif (resp. σ_i-négatif). Par exemple, le mot $\sigma_1\sigma_2\sigma_1^{-N}$ n'est pas σ_1-positif si N est un entier ≥ 1, mais la tresse qu'il représente l'est (le montrer !).

Nous dirons qu'une tresse est *σ-positive* (resp. *σ-négative*) s'il existe un entier i tel qu'elle est σ_i-positive (resp. σ_i-négative). On peut alors énoncer le théorème de Dehornoy.

Théorème 1.— *Toute tresse différente de* 1 *est soit σ-positive, soit σ-négative.*

La démonstration de ce théorème occupera les numéros 2 et 3. Celui-ci a pour conséquence les résultats nouveaux suivants non connus antérieurement.

Corollaire.— *(a) Pour tout n, le groupe B_n est ordonnable.*

(b) Pour tout n et tout anneau R sans diviseurs de zéro, l'algèbre $R[B_n]$ du groupe B_n n'a pas de diviseurs de zéro, ni d'unités ou d'idempotents non triviaux.

DÉMONSTRATION.— (a) Soit P l'ensemble des tresses σ-positives de B_n. Il est clair que P^2 est inclus dans P. Le théorème 1 implique $B_n = P \amalg \{1\} \amalg P^{-1}$. Il en résulte que B_n est ordonnable.

(b) C'est une conséquence de (a) et des remarques faites au n° 1.2. $\square$

1.4. Propriétés. L'ordre de Dehornoy ainsi défini est l'unique ordre total de B_n invariant par multiplication à gauche tel que $\beta\,\sigma_1\,\beta' > 1$ pour tous les éléments β, β' du sous-groupe de B_n engendré par $\sigma_2, \ldots, \sigma_{n-1}$. Dans [D97b] Dehornoy a construit un algorithme de résolution du problème des mots fondé sur l'ordre total des tresses. En pratique, cet algorithme est beaucoup plus efficace que les algorithmes antérieurs (mais le problème reste ouvert de montrer qu'il est quadratique).

Soit B_n^+ le sous-monoïde de B_n constitué des tresses représentées par des produits des générateurs $\sigma_1, \ldots, \sigma_{n-1}$, mais non de leurs inverses. Laver [L96] a montré que l'ordre de Dehornoy prolonge l'ordre partiel considéré par ElRifai et Morton dans [EM] ; il en déduit le résultat remarquable suivant, qui distingue probablement cet ordre parmi les ordres de B_n mentionnés au n° 5.2.

Théorème 2.— *L'ordre de Dehornoy restreint à B_n^+ est un bon ordre.*

Rappelons qu'un ordre total sur un ensemble E est un *bon ordre* si toute partie de E a un élément minimal. Dans un bon ordre, chaque élément a un rang ; par exemple, le générateur σ_{n-1} de B_n^+ est le plus petit élément > 1. Comme tout élément de B_n possède une écriture canonique comme fraction de deux éléments de B_n^+ (voir [E+]), le théorème de Laver permet de spécifier une tresse à l'aide d'un couple d'ordinaux. Burckel [Bu] a donné une autre preuve du théorème 2 et montré que le type de l'ordre de B_n^+ est $\omega^{\omega^{n-2}}$, où ω désigne le plus petit ordinal infini. Voir aussi l'article de Wiest [W] basé sur la définition géométrique de l'ordre de B_n présentée au n° 5.1.

2. COLORIAGE DES TRESSES ET SYSTÈMES AUTODISTRIBUTIFS

Le but du n° 2 est d'indiquer comment Dehornoy démontre le théorème 1.

2.1. Comment colorier les tresses ? L'idée n'est pas nouvelle ; elle a notamment été utilisée par Joyce [Joy], Matveev [Mt] et Brieskorn [Br] dans les années 1980. Partons d'un mot de tresse w représentant un élément de B_n. Colorions de gauche à droite les extrémités supérieures des brins de la configuration plane associée à w avec les éléments $a_1, a_2, \ldots, a_n$ d'un ensemble S. Si nous propageons ces couleurs le long des brins, nous lirons au bas de la configuration une suite de couleurs qui est une permutation de la suite $a_1, a_2, \ldots, a_n$ de départ : c'est évidemment la permutation sous-jacente à la tresse.

Les choses deviennent plus intéressantes si nous autorisons les couleurs à interagir à chaque croisement des brins. Supposons que les croisements soient exclusivement positifs, c'est-à-dire que le mot w soit un produit des générateurs σ_i et non de leurs inverses. On dira d'un tel mot qu'il est *positif*. Décidons qu'à chaque croisement la couleur a du brin inférieur reste inchangée tandis que la couleur b du brin supérieur s'amalgame avec la couleur a de l'autre brin pour former une nouvelle couleur $a*b$ qui dépend de a et de b (voir la figure 2). Ceci revient à munir S d'une loi de composition $(a,b) \mapsto a*b$. Procédant de cette manière pour tous les croisements, nous construisons ainsi une action (à droite) du monoïde des mots de tresse positifs à n brins sur la puissance n-ième S^n de l'ensemble S. Si on note ε le mot vide, alors cette action est définie par récurrence sur la longueur des mots par $(a_1, \ldots, a_n)\, \varepsilon = (a_1, \ldots, a_n)$ et

$$(a_1, \ldots, a_n)\, \sigma_i w = (a_1, \ldots, a_{i-1}, a_i * a_{i+1}, a_i, a_{i+2}, \ldots, a_n)\, w \tag{2.1}$$

où $(a_1, a_2, \ldots, a_n) \in S^n$, w est un mot de tresse et $1 \leq i < n$.

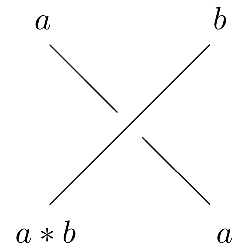


Figure 2

Au n° 1.4 nous avons défini B_n^+ comme le sous-monoïde du groupe B_n formé des tresses représentées par des mots positifs. On sait que le monoïde B_n^+ a une présentation donnée par les relations (1.1) et (1.2).

Lemme 1.— *La formule (2.1) définit une action du monoïde B_n^+ sur S^n si et seulement si, pour tout a, b, $c \in S$, on a*

$$a * (b * c) = (a * b) * (a * c). \tag{AD}$$

Démonstration.— On se ramène aux calculs suivants où a, b, c, d désignent des éléments de l'ensemble S. Le premier calcul reflète la relation (1.1) :

$$(a, b, c, d)\, \sigma_1 \sigma_3 = (a * b, a, c * d, c) = (a, b, c, d)\, \sigma_3 \sigma_1.$$

La relation non triviale (1.2) montre la nécessité de l'identité (AD) :

$$\begin{aligned} (a, b, c)\, \sigma_1 \sigma_2 \sigma_1 &= \big((a * b) * (a * c), a * b, a\big), \\ (a, b, c)\, \sigma_2 \sigma_1 \sigma_2 &= \big(a * (b * c), a * b, a\big). \end{aligned} \qquad \square$$

Définition.— *Un système autodistributif (ou encore un système AD) est un ensemble muni d'une loi de composition vérifiant la relation (AD) du lemme 1.*

Par la suite, on utilisera les notions évidentes de morphisme de systèmes AD, de sous-système AD, de partie génératrice d'un système AD.

2.2. Ensembles automorphes. Dans ce numéro, nous donnons des exemples de systèmes autodistributifs. Il s'agit ici de ce que Brieskorn Ê[Br] a appelé des *ensembles automorphes*, à savoir des systèmes autodistributifs pour lesquels les multiplications à gauche $b \mapsto a * b$ sont bijectives (ces systèmes particuliers ont également été utilisés sous d'autres noms, comme "wrack" chez Conway et Wraith, "rack" chez Fenn et

Rourke [FR], “crystal” chez Kauffman [Kau] ; on trouvera dans [FR] une introduction historique aux ensembles automorphes).

Si S est un ensemble automorphe, alors l'action de B_n^+ sur S^n, qui est à valeurs dans un ensemble de bijections, s'étend en une action du groupe B_n tout entier. On obtient ainsi une méthode systématique de construction de représentations de B_n, méthode dont les exemples (a) et (b) ci-dessous montrent l'intérêt.

(a) *(Conjugaison)* Tout groupe G est muni d'une structure de système AD dont la loi de composition $*$ est définie par $a * b = aba^{-1}$ où a, $b \in G$.

Si G est le groupe libre F_n sur n générateurs $x_1, \ldots, x_n$, posons $(y_1, \ldots, y_n) = (x_1, \ldots, x_n)\,\beta$ pour tout $\beta \in B_n$ La correspondance $(x_1, \ldots, x_n) \mapsto (y_1, \ldots, y_n)$ définit un automorphisme $\widehat{\beta}$ de F_n. L'application $\beta \mapsto \widehat{\beta}^{-1}$ est l'homomorphisme injectif de groupes $B_n \to \mathrm{Aut}(F_n)$ bien connu (voir par exemple [BZ], chap. 10).

(b) *(Barycentre)* L'anneau $\mathbf{Z}[t, t^{-1}]$ des polynômes de Laurent à coefficients entiers a une structure de système AD avec $a * b = (1-t)a + tb$ où a, $b \in \mathbf{Z}[t, t^{-1}]$. L'action linéaire de B_n^+ sur $\mathbf{Z}[t, t^{-1}]^n$ s'étend en un homomorphisme de groupes $B_n \to \mathrm{GL}_n(\mathbf{Z}[t, t^{-1}])$: c'est la *représentation de Burau.*

Les ensembles automorphes pour lesquels $a * a = a$ pour tout a, comme dans les exemples (a) et (b), ont été appelés “quandles” par Joyce [Joy] et “distributive groupoids” par Matveev [Mt] (tous deux ont utilisé ce type de systèmes AD pour classifier les nœuds dans $\mathbf{R}^3$). Voici deux autres exemples d'ensembles automorphes.

(c) *(Systèmes de racines)* Les vecteurs non nuls d'un espace vectoriel euclidien forment un ensemble automorphe : si a et b sont non nuls, on définit $a * b$ comme l'image de b par la symétrie orthogonale par rapport à l'hyperplan orthogonal à a. En particulier, tout système de racines est un ensemble automorphe.

(d) Si l'on note F_X le groupe libre engendré par les éléments d'un ensemble X, on peut munir l'ensemble-produit $B_X = F_X \times X$ d'une loi autodistributive par

$$(w_1, x_1) * (w_2, x_2) = (w_1 x_1 w_1^{-1} w_2, x_2)$$

où $w_1, w_2 \in F_X$ et $x_1, x_2 \in X$. Le système B_X est un ensemble automorphe libre ; tout ensemble automorphe S est quotient de B_X où X est une partie génératrice de S.

2.3. Cycles et acyclicité. Si a et b sont des éléments d'un système autodistributif S, nous dirons que a divise b (à gauche) s'il existe $c \in S$ tel que $b = a * c$. Un *cycle* est une suite $(a_1, \ldots, a_k)$ d'éléments de S tels que a_i divise a_{i+1} pour tout $i < k$ et a_k divise a_1. On dit qu'un système AD est *acyclique* s'il ne possède pas de cycle. Un ensemble automorphe n'est pas acyclique puisque tout élément se divise lui-même.

L'observation suivante montre l'intérêt des systèmes acycliques. Sur un système autodistributif S on peut définir une relation binaire $\prec$ comme suit : $a \prec b$ s'il existe un entier $k \geq 1$ et des éléments $a_1, \ldots, a_k$ de S tels que $a_1 = a$, $a_k = b$ et a_i divise a_{i+1} pour tout $i < k$. La relation $\prec$ est transitive, et c'est une relation d'ordre partiel si S est acyclique. Avant les travaux de théorie des ensembles exposés au n° 4, on ne connaissait pas d'exemple de système acyclique.

Proposition 1.— *Il existe des systèmes autodistributifs acycliques.*

Démonstration.— Il suffit d'exhiber un exemple. Voici celui de Larue [La] qui utilise l'image dans les automomorphismes d'un groupe libre de l'opération sur les tresses que nous décrirons au n° 3.3. Soit F_∞ le groupe libre sur une infinité dénombrable de lettres $x_1, x_2, \ldots$ et $\mathrm{Aut}(F_\infty)$ le groupe de ses automorphismes de groupe. Nous allons munir $\mathrm{Aut}(F_\infty)$ d'une loi autodistributive $*$. Soit α l'automorphisme de F_∞ déterminé par

$$\alpha(x_i) = \begin{cases} x_1 x_2 x_1^{-1} & \text{si } i = 1, \\ x_1 & \text{si } i = 2, \\ x_i & \text{si } i > 2, \end{cases}$$

et T_0 l'endomorphisme de F_∞ donné par $T_0(x_i) = x_{i+1}$ pour tout $i \geq 0$. Ce dernier permet de définir l'endomorphisme T de $\mathrm{Aut}(F_\infty)$ par les formules $T(\varphi)(x_1) = x_1$ et $T(\varphi)(x_i) = T_0(\varphi(x_{i-1}))$ si $i > 1$ et $\varphi \in \mathrm{Aut}(F_\infty)$. Pour φ et $\psi \in \mathrm{Aut}(F_\infty)$, posons

$$\varphi * \psi = \varphi \circ T(\psi) \circ \alpha \circ T(\varphi^{-1}). \tag{2.2}$$

On vérifie par un calcul direct que la loi de composition $*$ est autodistributive.

Nous affirmons que le système $(\mathrm{Aut}(F_\infty), *)$ est acyclique. En effet, soit E l'ensemble des éléments de F_∞ dont l'expression réduite en les générateurs $x_1, x_2, \ldots$ et leurs inverses se termine par x_1^{-1}. On observe d'abord que α, ainsi que tout élément $\varphi \in \mathrm{Aut}(F_\infty)$ qui est dans l'image du décalage T, préserve le sous-ensemble E. Supposons maintenant que le système $\mathrm{Aut}(F_\infty)$ possède un cycle. Cette hypothèse se traduit par une égalité de la forme $\varphi = \varphi \circ T(\varphi_0) \circ \alpha \circ T(\varphi_1) \circ \cdots \circ T(\varphi_{k-1}) \circ \alpha \circ T(\varphi_k)$, où $k \geq 1$ et φ, $\varphi_0, \ldots, \varphi_{k-1}, \varphi_k$ sont des automorphismes de F_∞. De manière équivalente, on a

$$\mathrm{id} = T(\varphi_0) \circ \alpha \circ T(\varphi_1) \circ \cdots \circ T(\varphi_{k-1}) \circ \alpha \circ T(\varphi_k) \tag{2.3}$$

où id représente l'automorphisme identité de F_∞. Appliquons les deux membres de (2.3) à l'élément x_1 de F_∞. A gauche, on obtient x_1 qui n'appartient pas au sous-ensemble E. Par contre, comme $(\alpha \circ T(\varphi_k))(x_1) = \alpha(x_1) = x_1 x_2 x_1^{-1}$ appartient à E, il résulte de l'observation ci-dessus que l'élément de F_∞ obtenu en appliquant le membre de droite de (2.3) à x_1 appartient à E. D'où une contradiction. □

2.4. Retournement des mots. Nous avons vu au n° 2.1 comment définir une action du monoïde B_n^+ sur la puissance n-ième d'un système AD S et au n° 2.2 que cette action s'étend au groupe B_n tout entier si (et seulement si) S est un ensemble automorphe. Or, à la vue des remarques faites au n° 2.3 et des travaux dont nous parlerons au n° 4, la question se pose d'étendre l'action du monoïde B_n^+ à B_n lorsque S est acyclique. En développant une méthode spécifique, dite de retournement des mots, Dehornoy a réussi à définir une action partielle de B_n sur S^n lorsque S est un système AD *simplifiable* (à gauche), c'est-à-dire un système pour lequel les multiplications à gauche sont injectives.

On dit qu'un mot de tresse w *se transforme par retournement* (à gauche) en le mot w' si w' s'obtient en remplaçant dans w des facteurs du type $\sigma_i\sigma_j^{-1}$ par le mot vide si $i = j$, par $\sigma_j^{-1}\sigma_i$ si $|i-j| > 1$, et par $\sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i$ si $|i-j| = 1$. Par définition du retournement, w et w' représentent le même élément dans B_n.

Garside [Ga] avait démontré que toute tresse est le quotient de deux tresses représentées par des mots de tresse positifs. Dehornoy reprend les ingrédients de l'approche de Garside, mais travaille sur les mots de tresse plutôt que sur les tresses, ce qui lui permet d'établir dans [D97a] le résultat plus fin suivant.

Lemme 2.— *Tout mot de tresse se transforme par retournement en un mot de la forme $u^{-1}v$ où u et v sont des mots de tresse positifs.*

Remarquons qu'il n'est pas évident *a priori* que l'algorithme de retournement converge en un nombre fini d'étapes car la longueur des mots peut augmenter à chaque retournement ; on pourra observer ce phénomène sur le mot $\sigma_2\sigma_4\sigma_6\sigma_5^{-1}\sigma_3^{-1}\sigma_1^{-1}$. Signalons que des techniques analogues de retournement des mots permettent la construction de formes normales et de structures automatiques pour d'autres groupes dont les groupes d'Artin de groupe de Coxeter fini (voir [D98], [DP]).

Soit maintenant S un système AD simplifiable et n un entier ≥ 2. L'action à droite $(\vec{a}, w) \mapsto \vec{a}w$ du monoïde B_n^+ sur le produit S^n, donnée par la formule (2.1), se prolonge à certains éléments $(\vec{a}, w)$ de $S^n \times B_n$ de façon que les règles de coloriage restent vérifiées. C'est par exemple le cas de $(\vec{b}u, u^{-1})$ avec $b \in S^n$ et $u \in B_n^+$. Dans ce cas, on dira que l'élément $\vec{a}w$ est défini.

Lemme 3.— *Soit S un système AD simplifiable et $\vec{a} \in S^n$. Si le mot de tresse w se transforme par retournement en w' et si $\vec{a}w'$ est défini, alors $\vec{a}w$ est défini.*

Les lemmes 2 et 3 impliquent la proposition suivante selon laquelle on peut toujours trouver un ensemble de couleurs dans un système AD simplifiable pour colorier une tresse donnée en suivant la règle énoncée au n° 2.1.

Proposition 2.— *Soit S un système AD simplifiable. Pour tout mot de tresse w, il existe $\vec{a} \in S^n$ tel que $\vec{a}w$ soit défini. Si w et w' représentent la même tresse et que $\vec{a}w$ et $\vec{a}w'$ soient définis, alors $\vec{a}w = \vec{a}w'$.*

Démonstration.— Contentons-nous d'établir la première assertion. D'après le lemme 2, w se transforme par retournement en $w' = u^{-1}v$ où u et v sont des mots positifs. Posons $\vec{a} = \vec{b}u$ où $\vec{b}$ est n'importe quel élément de S^n. Alors $\vec{a}w' = \vec{b}v$ est défini. On termine en appliquant le lemme 3.

Pour établir la seconde assertion, on utilise une version à droite du retournement des mots de tresse et l'hypothèse que le système est simplifiable. □

2.5. Démonstration du théorème 1. Supposons que nous disposions d'un système autodistributif S acyclique et monogène (c'est-à-dire engendré par un seul élément) tel que l'ordre $\prec$ associé (défini au n° 2.3) soit total. On vérifie que $a \prec b$ implique $c * a \prec c * b$, d'où l'on déduit que S est simplifiable.

Puisque S possède un ordre total, on peut munir chaque puissance S^n de S de l'ordre total lexicographique $\prec_\ell$ défini par $(a_1, \ldots, a_n) \prec_\ell (b_1, \ldots, b_n)$ s'il existe $i \geq 1$ tel que $a_j = b_j$ pour tout $j < i$ et $a_i \prec b_i$. Nous utilisons l'ordre total $\prec_\ell$ sur S^n pour définir une partie "positive" P de B_n comme suit. Si w est un mot de tresse, alors, d'après la proposition 2, il existe $\vec{a} \in S^n$ tel que $\vec{a}w$ soit défini. Nous dirons que la tresse représentée par w est dans P si $\vec{a} \prec_\ell \vec{a}w$.

Proposition 3.— *Une tresse est dans P si et seulement si elle est σ-positive. La relation $\beta < \beta'$ définie sur B_n par $\beta^{-1}\beta' \in P$ est une relation d'ordre total invariant par multiplication à gauche, qui coïncide avec l'ordre de Dehornoy du n° 1.3.*

Démonstration.— Montrons que, si un mot de tresse est σ-positif, alors il représente une tresse du sous-ensemble P défini ci-dessus. Un mot σ_i-positif w est de la forme $w = w_0\sigma_i w_1 \sigma_i \ldots \sigma_i w_k$ où $w_0, w_1, \ldots, w_k$ sont des mots dans les lettres σ_j et σ_j^{-1} avec $j > i$. Soit $\vec{a} = (a_1, \ldots, a_n) \in S^n$ tel que $\vec{a}w = (b_1, \ldots, b_n) \in S^n$ soit défini. La formule (2.1) implique que $b_j = a_j$ pour tout $j < i$ et que b_i est de la forme $b_i = (\cdots((a_1 * c_1) * c_2) * \cdots) * c_k$ où $c_1, c_2, \ldots, c_k \in S$ et k est le nombre d'occurrences de σ_i dans w. Par définition de l'ordre $\prec$ de S, il en résulte que $a_i \prec b_i$. Par conséquent, $\vec{a} \prec_\ell \vec{a}w$ et $w \in P$.

La réciproque, à savoir qu'une tresse dans P est σ-positive, utilise la notion de tresse spéciale que nous introduirons au n° 3.3, et sera démontrée au n° 3.4.

Une fois l'équivalence précédente établie, il est clair que la relation $<$ est bien définie et que c'est l'ordre total du n° 1.3, dont l'existence est ainsi démontrée. □

3. SYSTÈME AUTODISTRIBUTIF LIBRE ET TRESSES SPÉCIALES

Nous étudions maintenant deux systèmes autodistributifs particuliers. Le premier est libre et fournit le type de systèmes nécessaires à la démonstration du théorème 1, telle qu'elle est donnée au n° 2.5. Le second est constitué de tresses.

3.1. Le système autodistributif libre sur un générateur. Il est caractérisé par la propriété universelle suivante.

Proposition 4.— *Il existe un système autodistributif D_1 engendré par un singleton $\{x\}$ tel que, pour tout système autodistributif S et tout élément s de S, il existe un unique morphisme $f : D_1 \to S$ de systèmes AD vérifiant $f(x) = s$. Le système D_1 est unique à isomorphisme près.*

Démonstration.— L'unicité est claire. Pour l'existence, on considère le magma libre M sur un générateur x (voir [Bo], I, § 7, n° 1). Les éléments de M sont des parenthésages complets de puissances strictement positives de la lettre x. Notons $*$ la loi de composition du magma. Sur M on considère la relation d'équivalence $\equiv_{\mathrm{AD}}$ invariante par composition et engendrée par les paires $(t_1*(t_2*t_3), (t_1*t_2)*(t_1*t_3))$. On définit D_1 comme l'ensemble des classes d'équivalence $M/\equiv_{\mathrm{AD}}$. On vérifie aisément que D_1 est un système AD satisfaisant à la propriété universelle ci-dessus. □

Rappelons la relation binaire $\prec$ introduite au n° 2.3. Le théorème suivant, établi par Dehornoy dans [D94], fournit l'exemple qui nous manquait au n° 2.5 pour construire un ordre total sur les groupes de tresses.

Théorème 3.— *Le système autodistributif D_1 est acyclique et la relation $\prec$ le munit d'un ordre total.*

Le système libre D_1 est un ensemble de classes d'équivalence de parenthésages pour la relation $\equiv_{\mathrm{AD}}$ définie dans la preuve de la proposition 4. Avant de démontrer le théorème 3, établissons quelques propriétés de ces parenthésages.

Pour tout entier $n \geq 1$ définissons les puissances droites $x^{[k]}$ de x par $x^{[1]} = x$ et $x^{[k]} = x * x^{[k-1]}$ si $k > 1$. La relation d'équivalence $\equiv_{\mathrm{AD}}$ vérifie la propriété fondamentale d'absorption suivante.

Lemme 4.— *Pour tout parenthésage t, on a $x^{[k+1]} \equiv_{\mathrm{AD}} t * x^{[k]}$ pour tout k suffisamment grand.*

Démonstration.— On procède par récurrence sur la longueur de t. Si $t = x$, alors $x^{[k+1]} = t * x^{[k]}$ par définition des puissances droites. Si $t = t_1 * t_2$, et si

$x^{[k+1]} \equiv_{\mathrm{AD}} t_1 * x^{[k]}$ et $x^{[k+1]} \equiv_{\mathrm{AD}} t_2 * x^{[k]}$ pour tout k suffisamment grand, alors

$$\begin{aligned} x^{[k+2]} &\equiv_{\mathrm{AD}} t_1 * x^{[k+1]} \equiv_{\mathrm{AD}} t_1 * (t_2 * x^{[k]}) \\ &\equiv_{\mathrm{AD}} (t_1 * t_2) * (t_1 * x^{[k]}) \equiv_{\mathrm{AD}} t * x^{[k+1]}. \end{aligned}$$

La troisième équivalence est une conséquence de la définition de $\equiv_{\mathrm{AD}}$. □

Nous dirons qu'un parenthésage t' est une *expansion* d'un parenthésage t si on l'obtient en remplaçant à partir de t des sous-expressions de la forme $t_1 * (t_2 * t_3)$ par $(t_1 * t_2) * (t_1 * t_3)$, c'est-à-dire en appliquant l'identité (AD), exclusivement de la gauche vers la droite. Il est clair que $t' \equiv_{\mathrm{AD}} t$ si t' est une expansion de t. On a la réciproque suivante.

Lemme 5.— *Si t_1 et t_2 sont des parenthésages tels que $t_1 \equiv_{\mathrm{AD}} t_2$, alors ils ont une expansion commune.*

Définissons maintenant les sous-termes gauches $G_k(t)$ d'un parenthésage t. Si $t = x$, seul $G_0(t) = t$ est défini. En général, posons $G_0(t) = t$ et, si $t = t_1 * t_2$ et $k \geq 1$, posons $G_k(t) = G_{k-1}(t_1)$ si ce dernier est défini. On a $G_\ell(G_k(t)) = G_{k+\ell}(t)$ lorsque ces expressions sont définies. Notons que l'élément de D_1 représenté par un sous-terme gauche $G_k(t)$, où $k \geq 1$, est plus petit pour l'ordre $\prec$ que l'élément représenté par t.

Lemme 6.— *Si t' est une expansion de t, alors, pour tout k tel que $G_k(t)$ soit défini, il existe un entier $k' \geq k$ tel que $G_{k'}(t')$ soit une expansion de $G_k(t)$.*

3.2. Démonstration du théorème 3. Si le système libre D_1 n'était pas acyclique, il en serait de même de tout système AD, ce qui contredirait la proposition 1.

Montrons maintenant que deux éléments quelconques de D_1 sont comparables pour l'ordre $\prec$. Plus précisément, soit y et z deux éléments de D_1 que nous représentons respectivement par des parenthésages t_1 et t_2. Il s'agit d'établir que soit $y = z$, soit $y \prec z$, soit $z \prec y$. D'après le lemme 4, il existe un entier $k \geq 1$ tel que $t_1 * x^{[k]} \equiv_{\mathrm{AD}} t_2 * x^{[k]}$. Le lemme 5 nous permet d'affirmer que les parenthésages $t_1 * x^{[k]}$ et $t_2 * x^{[k]}$ ont une expansion commune t'. Le lemme 6 implique l'existence d'entiers naturels p et q tels que $G_p(t')$ soit une expansion de $G_1(t_1 * x^{[k]}) = t_1$ et que $G_q(t')$ soit une expansion de $G_1(t_2 * x^{[k]}) = t_2$. Les parenthésages $G_p(t')$ et $G_q(t')$ représentent respectivement les éléments y et z de D_1. Trois cas se présentent à nous :

(i) si $p = q$, alors $G_p(t') = G_q(t')$, et donc $y = z$;

(ii) si $p > q$, alors $G_p(t') = G_{p-q}(G_q(t'))$, et donc $y \prec z$.

(iii) si $p < q$, alors $G_q(t') = G_{q-p}(G_p(t'))$, et donc $z \prec y$. □

3.3. Une loi autodistributive sur les tresses. Pour achever la démonstration de la proposition 3 du n$^{\text{o}}$ 2.5, nous allons introduire ce que Dehornoy appelle des tresses spéciales. Dans ce but, considérons la limite inductive B_∞ des groupes de tresses B_n pour les inclusions évidentes ; une présentation du groupe B_∞ est obtenue en prenant une famille infinie de générateurs σ_i indexée par les entiers ≥ 1 et les relations (1.1) et (1.2). Soit T l'endomorphisme injectif de B_∞ défini par $T(\sigma_i) = \sigma_{i+1}$ pour tout $i \geq 1$. Posons

$$\alpha * \beta = \alpha\, T(\beta)\, \sigma_1\, T(\alpha^{-1}). \tag{3.1}$$

Proposition 5.— *La formule (3.1) munit B_∞ d'une structure de système AD simplifiable et acyclique.*

Démonstration.— Nous laissons au lecteur le soin de vérifier que B_∞ est un système AD simplifiable. Pour établir son acyclicité, on observe que l'homomorphisme de groupes $B_\infty \to \mathrm{Aut}(F_\infty)$ qui est la limite inductive des homomorphismes $B_n \to \mathrm{Aut}(F_n)$ mentionnés au n$^{\text{o}}$ 2.2 (a) transporte la loi (3.1) sur la loi (2.2). Comme le système $(\mathrm{Aut}(F_\infty), *)$ est acyclique, il en est de même de $(B_\infty, *)$. $\square$

Dans le système autodistributif B_∞, considérons le sous-système B_{sp} engendré par la tresse unité 1. Les éléments de B_{sp} sont appelés *tresses spéciales*. Exemples de tresses spéciales : $1*1 = \sigma_1$, $1*(1*1) = \sigma_2\sigma_1$, $(1*1)*1 = \sigma_1^2\sigma_2^{-1}$, $1*(1*(1*1)) = \sigma_3\sigma_2\sigma_1$.

Proposition 6.— *Le système autodistributif B_{sp} est acyclique et la relation $\prec$ le munit d'un ordre total.*

Démonstration.— Le système B_{sp} hérite l'acyclicité de B_∞. La relation $\prec$ est donc une relation d'ordre sur B_{sp}. Il reste à montrer que deux éléments quelconques de B_{sp} sont comparables pour $\prec$. Comme B_{sp} est engendré par le singleton $\{1\}$, c'est un quotient du système libre D_1. Par le théorème 3, deux éléments quelconques de D_1 sont comparables pour $\prec$, donc, par projection, il en est de même dans B_{sp}. $\square$

L'argument pécédent montre que, dans tout système AD acyclique et monogène, la relation $\prec$ est une relation d'ordre total. En fait, comme l'a montré Laver [L92], tout système AD acyclique monogène est isomorphe à D_1. En particulier, $B_{\mathrm{sp}} \cong D_1$.

L'intérêt des tresses spéciales vient de la possibilité d'exprimer toute tresse en termes de produit de tresses spéciales.

Lemme 7.— *Pour tout $\beta \in B_n$, il existe $2n$ tresses spéciales $\alpha_1, \ldots, \alpha_n$, $\gamma_1, \ldots, \gamma_n$ telles que*

$$\beta = T^{n-1}(\alpha_n)^{-1} \ldots T(\alpha_2)^{-1}\, \alpha_1^{-1}\, \gamma_1\, T(\gamma_2) \ldots T^{n-1}(\gamma_n). \tag{3.2}$$

Démonstration.— Comme B_{sp} est un système AD simplifiable, nous pouvons appliquer la proposition 2, qui fournit une action partielle de B_n sur B_{sp}^n. En particulier, pour toute tresse $\beta \in B_n$, il existe des n-uples $(\alpha_1, \ldots, \alpha_n)$ et $(\gamma_1, \ldots, \gamma_n) \in B_{\mathrm{sp}}^n$ tels que $(\alpha_1, \ldots, \alpha_n)\, \beta = (\gamma_1, \ldots, \gamma_n)$. On vérifie alors facilement l'égalité des produits

$$\alpha_1\, T(\alpha_2) \ldots T^{n-1}(\alpha_n)\, \beta = \gamma_1\, T(\gamma_2) \ldots T^{n-1}(\gamma_n)$$

dans le groupe B_∞, d'où la formule (3.2). □

3.4. Fin de la preuve de la proposition 3. Supposons que α et γ soient deux tresses spéciales. On a ou bien $\alpha \prec \gamma$, ou bien $\alpha = \gamma$, ou bien $\gamma \prec \alpha$. Revenant à la définition de la relation $\prec$ et de la loi (3.1), on voit que les trois relations précédentes entraînent respectivement que la tresse $\alpha^{-1}\gamma$ est σ_1-positive, égale à 1, ou σ_1-négative. Si maintenant β est une tresse quelconque, on considère une décomposition de type (3.2) de β : si i est le plus petit indice tel que $\alpha_i \neq \gamma_i$, alors β est σ_i-positive ou σ_i-négative suivant que $\alpha_i \prec \gamma_i$ ou $\gamma_i \prec \alpha_i$, ce qui achève la preuve de la proposition 3. □

4. RAPPORT AVEC LA THÉORIE DES ENSEMBLES

Dans ce numéro nous expliquons comment des développements en théorie des ensembles ont mené à la construction d'un ordre total sur les tresses.

4.1. Grands cardinaux et extensions de ZF. On sait depuis le théorème d'incomplétude de Gödel que le système ZF d'axiomes de Zermelo-Fraenkel est incomplet, c'est-à-dire qu'il existe des énoncés qui sont indécidables dans ZF. C'est le cas de l'axiome du choix et de l'hypothèse du continu. Dès lors, le but principal de la théorie des ensembles consiste à étudier, voire classifier, les extensions du système ZF dans lesquels les énoncés ouverts deviennent décidables. Gödel a émis l'idée que ces extensions pourraient être classifiées à l'aide d'axiomes de grands cardinaux comme celui qui postule l'existence de $\aleph_1$. L'un des premiers axiomes considérés a été celui qui affirme l'existence d'un cardinal inaccessible.[2] Non seulement cet axiome est indémontrable dans ZF, mais encore — à la différence de l'axiome du choix ou de l'hypothèse du continu — sa cohérence, c'est-à-dire le fait qu'il ne soit pas contradictoire, ne peut y être établie.

[2] α est inaccessible si tout ensemble de parties d'un ensemble de cardinalité $<\alpha$ et toute union d'ensembles de cardinalité $<\alpha$ sont de cardinalité $<\alpha$.

Dans les années 1960 une hiérarchie totalement ordonnée d'axiomes de grands cardinaux est apparue en théorie des ensembles, s'imposant comme les bonnes extensions de ZF (voir la monographie [Kan]). Nous allons nous intéresser au n° 4.2 à un axiome particulier de cette hiérarchie.

4.2. Plongements élémentaires. Un ensemble infini se caractérise par l'existence d'une injection non bijective. Une telle injection ne préserve pas nécessairement toutes les structures de l'ensemble considéré : ainsi l'application $n \mapsto n+1$ de l'ensemble des entiers naturels dans lui-même préserve l'ordre naturel, mais non l'addition. Pour définir des notions d'infini plus fortes, il est naturel de postuler l'existence d'une injection non bijective d'un ensemble dans lui-même, préservant *toutes* les propriétés définissables par les opérations ensemblistes de base. Appelons *plongement élémentaire* une telle injection et *autosimilaire* un ensemble pour lequel il existe un plongement élémentaire. On démontre assez facilement qu'un ensemble autosimilaire est forcément très grand : son cardinal doit être inaccessible, ce qui entraîne que l'existence d'un tel ensemble ne peut être démontrée dans ZF.

Il est usuel en théorie des ensembles de considérer des ensembles particuliers appelés rangs, qui ont la propriété technique que toute fonction d'un rang R dans lui-même est (essentiellement) un élément de R. Les axiomes affirmant l'existence de plongements élémentaires d'un rang dans un autre ou d'un rang dans lui-même ont été au cœur de la théorie des ensembles dans les années 1980. Un des résultats majeurs obtenus à l'aide de tels axiomes a été la démonstration en 1984 par Martin et Steel de la propriété de détermination pour les ensembles projectifs de réels, un énoncé technique qui, d'une certaine façon, décrit complètement la structure fine de la droite réelle (voir [D89]). L'axiome qui nous intéresse est le suivant.

Axiome A.— *Il existe un rang autosimilaire.*

4.3. Le système autodistributif d'un rang autosimilaire. Notons E_R l'ensemble des plongements élémentaires du rang autosimilaire R dont nous venons de postuler l'existence. L'ensemble E_R est trivialement muni d'une structure de monoïde pour la composition des plongements. Mais, en vertu de l'axiome A et des propriétés spécifiques des rangs, il est aussi muni d'une autre opération binaire qu'on peut appeler *l'application*. En effet, nous avons dit qu'une fonction définie sur un rang R peut être vue comme un élément de R. Si donc i et j sont des plongements élémentaires de R, i s'appliquant par hypothèse aux éléments de R et j pouvant être vu comme un tel élément, nous pouvons appliquer i à j. On montre que le nouvel objet $i(j)$ ainsi obtenu, héritant de toutes les propriétés définissables de j, est aussi un plongement élémentaire de R. La loi de composition $(i,j) \mapsto i(j)$ ainsi définie sur E_R est autodistributive. L'argument est le suivant : si y est l'image de x par l'application f, alors $i(y)$ est l'image de $i(x)$ par $i(f)$ chaque fois que i est un plongement élémentaire ; en d'autres termes, on a $i(f(x)) = i(f)(i(x))$, identité valide, en particulier, lorsque f et x sont des plongements élémentaires.

Laver [L92] a établi en 1989 le résultat suivant.

Proposition 7.— *Si j est un plongement élémentaire du rang R, alors le sous-système autodistributif de E_R engendré par j est acyclique.*

Avec ce résultat, Laver a construit le premier exemple d'un système AD acyclique, mais un exemple dont l'existence dépend d'un axiome indémontrable de théorie des ensembles. La situation ainsi créée était étrange : dans des travaux indépendants, Dehornoy et Laver avaient, à cette époque, partiellement résolu le problème des mots de l'identité (AD), en construisant, sous l'hypothèse de l'existence d'un système AD acyclique, un algorithme permettant de reconnaître si deux parenthésages donnés sont ou non équivalents modulo $\equiv_{\mathrm{AD}}$. La proposition 7 prouvait donc la décidabilité du problème des mots en question à partir de l'axiome indémontrable A, établissant un lien paradoxal entre le problème des mots de (AD), qui ne met en jeu que des manipulations de mots finis, et un rang autosimilaire, qui est un objet gigantesque.

Une solution a été proposée vers la fin 1991 par Dehornoy qui, à partir d'une étude fine de l'autodistributivité dont nous donnerons une idée au numéro suivant, a montré par une démonstration directe qu'un système AD libre est acyclique, et a déduit de son analyse les liens avec les tresses (voir [D92a], [D92b], [D94]).

4.4. Le groupe de l'autodistributivité. L'étude algébrique des systèmes AD libres, en particulier celle du système D_1 à un générateur, ont fait l'objet de nombreux travaux de Laver et Dehornoy. Nous ne donnerons ici qu'un aperçu de l'approche de Dehornoy et de la façon dont elle mène aux tresses.

Pour étudier D_1, il est commode de représenter les parenthésages par des arbres binaires avec racine. On représente la variable x par l'arbre réduit à sa racine ; si t_1 et t_2 sont des parenthésages, on représente le parenthésage $t_1 * t_2$ 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 a une *adresse* qui est une suite finie de 0 et de 1 : l'adresse de la racine est la suite vide $\emptyset$, et, en s'éloignant de la racine, on passe de l'adresse d'un sommet à celui de son "successeur" gauche en ajoutant 0, et à celle de son "successeur" droit en ajoutant 1.

Au n° 3.1 nous avons défini la notion d'expansion d'un parenthésage. Cette définition se transpose facilement aux arbres binaires. Nous pouvons décrire plus finement la situation en considérant le cas où l'identité (AD) est appliquée une seule fois, toujours de la gauche vers la droite, et en prenant en compte l'adresse où elle l'est dans l'arbre correspondant. Nous noterons ∇_α l'opération consistant à appliquer (AD) à l'adresse α (l'opération ∇_α n'est pas partout définie sur M). Il est facile de vérifier les relations suivantes :

$$\nabla_{\alpha 0\beta}\,\nabla_{\alpha 1\gamma} = \nabla_{\alpha 1\gamma}\,\nabla_{\alpha 0\beta}, \tag{4.1}$$

$$\nabla_{\alpha 0\beta}\,\nabla_{\alpha} = \nabla_{\alpha}\,\nabla_{\alpha 10\beta}\,\nabla_{\alpha 00\beta}, \tag{4.2}$$

$$\nabla_{\alpha 10\beta}\,\nabla_{\alpha} = \nabla_{\alpha}\,\nabla_{\alpha 01\beta}, \tag{4.3}$$

$$\nabla_{\alpha 11\beta}\,\nabla_{\alpha} = \nabla_{\alpha}\,\nabla_{\alpha 11\beta}, \tag{4.4}$$

$$\nabla_{\alpha 1}\,\nabla_{\alpha}\,\nabla_{\alpha 1}\,\nabla_{\alpha 0} = \nabla_{\alpha}\,\nabla_{\alpha 1}\,\nabla_{\alpha}, \tag{4.5}$$

où α, β et γ sont des adresses quelconques.

Dans [D94] Dehornoy introduit alors le groupe G_{AD} engendré par les générateurs ∇_α (indexés par les adresses α) et les relations (4.1)–(4.5), et montre que ce groupe opère sur le magma libre M de telle sorte que les orbites de l'action sont exactement les classes d'équivalence d'éléments de M pour la relation $\equiv_{\mathrm{AD}}$. Il établit que le système D_1 est acyclique en étudiant le groupe G_{AD} à l'aide d'une méthode de retournement des mots semblable à celle décrite au n$^{\text{o}}$ 2.4 pour les tresses, et en construisant un préordre sur G_{AD}. Une étape essentielle consiste à reprendre la démonstration du lemme d'absorption 4, qui se lit, dans le groupe G_{AD}, comme l'existence d'une loi binaire $*$ donnée par la formule

$$a * b = a\,T(b)\,\nabla_{\emptyset}\,T(a)^{-1}, \tag{4.6}$$

où T est cette fois-ci l'endomorphisme qui envoie ∇_α sur $\nabla_{1\alpha}$ pour tout α.

Le lien avec les tresses résulte de l'observation suivante : l'application π définie par $\pi(\nabla_\alpha) = 1$ si l'adresse α contient au moins un 0, et $\pi(\nabla_\alpha) = \sigma_{i+1}$ si α est une suite constituée de i fois le chiffre 1, induit un homomorphisme surjectif de groupes de G_{AD} sur le groupe de tresses B_∞. En outre, π transporte la loi (4.6) de G_{AD} sur la loi autodistributive (3.1) de B_∞.

Signalons ici la parenté du groupe G_{AD} avec le groupe F de Thompson, qui en est l'exacte contrepartie lorsqu'on remplace l'identité AD par l'associativité. Dans cette correspondance, la relation (4.5) est l'analogue de la relation du pentagone de Mac Lane–Stasheff. On trouvera un exposé de synthèse sur le groupe F dans [CPF].

4.5. Systèmes autodistributifs finis. En étudiant les quotients finis du système AD associé à un plongement élémentaire, Laver [L95] a montré que, pour tout entier $n \geq 1$, il existe une unique structure autodistributive A_n sur l'ensemble fini $\{1, 2, \ldots, 2^n\}$ tel que $k * 1 \equiv k + 1$ modulo 2^n (on trouvera plus bas les tables de multiplication de A_1, A_2 et A_3). Les ensembles A_n forment un système projectif de systèmes AD et jouent un rôle-clé parmi les systèmes autodistributifs. En particulier, Drápal [Dr] a montré que tout système AD monogène fini se construit simplement à partir de systèmes A_n. Chaque ligne de la table de multiplication de A_n est la répétition périodique d'un suite croissante de nombres allant jusqu'à 2^n. De par l'existence du système projectif mentionné ci-dessus, la période p_n de la première ligne de la table de A_n est une suite croissante au sens large. En traduisant une propriété non triviale des ordinaux et des plongements élémentaires, Laver [L95] a démontré la proposition suivante, qui implique notamment que le sous-système AD engendré par 1 dans la limite projective des A_n est libre.

Proposition 8.— *S'il existe un rang autosimilaire, alors la suite $(p_n)_n$ tend vers l'infini.*

Pour l'instant aucune tentative pour démontrer ce résultat finitiste sans faire appel à la théorie des ensembles n'a abouti. On sait seulement que la première valeur de n pour laquelle p_n dépasse 32 est gigantesque [Do], [DJ]. Les systèmes A_n sont des objets d'une très grande complexité combinatoire, et restent encore très mal connus. Une question évidente, mais complètement ouverte, est de se demander s'ils sont susceptibles d'applications topologiques.

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

Tables de multiplication de A_1, A_2 et A_3

5. APPROCHES GÉOMÉTRIQUES

Récemment, deux constructions géométriques de l'ordre de Dehornoy ont été proposées par des topologues.

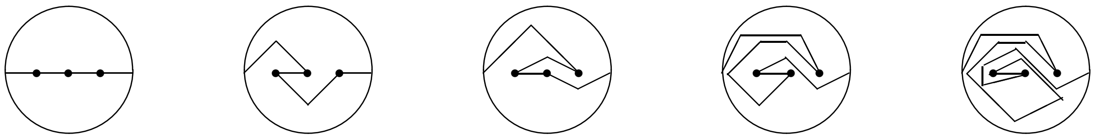
5.1. La définition de Fenn, Greene, Rolfsen, Rourke et Wiest. Notons D_n le disque unité fermé du corps $\mathbf{C}$ des nombres complexes, muni de n points marqués $P_1, \ldots, P_n$ intérieurs au disque et situés sur le diamètre réel $\Gamma = [-1, 1]$. Ordonnons les points marqués de sorte que le diamètre Γ soit la juxtaposition des $n+1$ segments $[P_0, P_1]$, $[P_1, P_2]$, $\ldots$, $[P_{n-1}, P_n]$, $[P_n, P_{n+1}]$ que nous numéroterons de 1 à $n+1$ (pour simplifier, on a posé $P_0 = -1$ et $P_{n+1} = 1$).

On sait (voir [BZ], chap. 10) que le groupe de tresses B_n est isomorphe au groupe des classes d'isotopie des homéomorphismes de D_n qui fixent le bord du disque point par point et permutent les points marqués. Considérons l'image de Γ par un tel homéomorphisme φ : la courbe simple $\varphi(\Gamma)$ sépare D_n en deux composantes connexes et est l'union de $n+1$ "petites courbes" $\varphi([P_i, P_{i+1}])$ dont les extrémités sont les points $P_0, P_1, \ldots, P_{n+1}$. On appelle $\varphi(\Gamma)$ le *diagramme de courbes* de φ. Suivant un procédé bien connu et utilisé par exemple dans [Mo], on rectifie $\varphi(\Gamma)$ en raccourcissant les petites courbes de manière à faire coïncider le maximum d'entre elles avec des segments $[P_i, P_{i+1}]$ et à éliminer les intersections inutiles avec Γ. Il est montré dans [F+] que deux tels homéomorphismes de D_n représentent la même tresse dans B_n si et seulement leurs diagrammes de courbes rectifiés sont isotopes *via* une isotopie qui fixe les petites courbes coïncidant avec des segments $[P_i, P_{i+1}]$. Pour $i = 1, \ldots, n-1$, on peut donc considérer l'ensemble Π_i des éléments de B_n correspondant aux diagrammes de courbes rectifiés pour lesquels $\varphi([P_{j-1}, P_j]) = [P_{j-1}, P_j]$ pour tout $j < i$ et $\varphi([P_{i-1}, P_i])$ monte vers le demi-plan supérieur de $\mathbf{C}$. On pose $\Pi = \bigcup_{i=1}^{n-1} \Pi_i$.

Fenn *et al.* [F+] ont établi en 1997 que la relation $\beta <_\Pi \beta'$ définie par $\beta^{-1}\beta' \in \Pi$ est une relation d'ordre total invariant par multiplication à gauche sur le groupe B_n. Ils ont aussi montré qu'une tresse est dans Π_i si et seulement si elle est σ_i-positive, ce qui entraîne que l'ordre $<_\Pi$ coïncide avec celui défini au n° 1.3. On obtient ainsi une définition géométrique de l'ordre de Dehornoy.

Utilisant les mêmes techniques, Rourke et Wiest [RW] (voir aussi [SW]) ont montré que le groupe des difféotopies ("mapping class group" en anglais) d'une surface compacte (non nécessairement orientable) à bord non vide est un groupe ordonnable. Ils ont aussi construit un algorithme qui décide en temps quadratique si un élément différent de l'identité est positif ou négatif pour l'ordre construit.

La figure 3 montre les diagrammes de courbes de cinq tresses. On voit, par exemple, sur ces diagrammes que $\sigma_1\sigma_2\sigma_1^{-1}$ et $\sigma_1\sigma_2\sigma_1^{-2}$ sont σ_1-positifs.



1 $\qquad \sigma_1 \qquad \sigma_1\sigma_2 \qquad \sigma_1\sigma_2\sigma_1^{-1} \qquad \sigma_1\sigma_2\sigma_1^{-2}$

Figure 3

5.2. L'approche à la Nielsen. En septembre 1998, W. P. Thurston [Th] a expliqué comment les travaux classiques de Nielsen sur les surfaces permettaient de construire un ordre invariant sur B_n à partir de la proposition suivante.

Proposition 9.— *Le groupe B_n opère sur la droite réelle par des homéomorphismes croissants de sorte que l'action soit libre en au moins un point réel.*

Avant d'établir la proposition 9, montrons comment on en déduit un ordre total sur B_n. Soit $x \in \mathbf{R}$ un point pour lequel l'action de la proposition 9 est libre (c'est-à-dire un point dont le stabilisateur est trivial). Pour β, $\beta' \in B_n$, posons $\beta <_x \beta'$ si $\beta(x) < \beta'(x)$ pour l'ordre naturel de $\mathbf{R}$. La liberté de l'action en x implique que la relation $<_x$ est un ordre, et c'est alors clairement un ordre total. Comme B_n opère par des homéomorphismes croissants, l'ordre $<_x$ est invariant par multiplication à gauche.

Short et Wiest [SW] ont classifié les ordres $<_x$ à conjugaison près (il y en a une infinité non dénombrable) et montré que l'on retrouve ainsi l'ordre de Dehornoy.

5.3. Démonstration de la proposition 9. Soit S une surface orientée fermée de genre un marquée en n points $P_1, \ldots, P_n$ et C une courbe simple séparant S en une surface A de genre un et une surface de genre zéro contenant les points marqués. Le groupe de tresses B_n s'identifie aussi au groupe des classes d'isotopie de difféomorphismes de S préservant l'orientation, induisant l'identité sur A et permutant les points marqués.

Munissons $S - \{P_1, \ldots, P_n\}$ d'une métrique hyperbolique complète pour laquelle C est une géodésique et les points marqués sont des “cusps.” Fixons un point-base x_0 sur C et le revêtement universel $(D, 0)$ de $(S - \{P_1, \ldots, P_n\}, x_0)$. La métrique hyperbolique identifie $(D, 0)$ avec le disque unité de $\mathbf{C}$. Tout difféomorphisme φ de S qui fixe x_0 et permute les points marqués se relève en un difféomorphisme $\widetilde{\varphi}$ de D fixant 0.

Dans [Ni], § 10, Nielsen a montré que $\widetilde{\varphi}$ se prolonge en un homéomorphisme $\partial\widetilde{\varphi}$ du bord ∂D de D, c'est-à-dire du cercle unité, que $\partial\widetilde{\varphi}$ conserve l'orientation si φ la conserve, et que $\partial\widetilde{\varphi}$ ne dépend que de la classe d'isotopie de φ. On obtient ainsi une action de B_n sur le cercle, préservant l'orientation. Pour obtenir une action sur $\mathbf{R}$, il suffit de remarquer que l'action précédente fixe un point, par exemple l'une des extrémités d'un relèvement de C passant par 0.

L'existence d'un point de $\mathbf{R}$ pour lequel l'action est libre se déduit également d'un résultat de Nielsen qui dit que, si φ n'est pas isotope à l'identité, alors l'ensemble des points fixes de $\partial\widetilde{\varphi}$ est un fermé d'intérieur vide (voir [Ni], § 14). Comme une union dénombrable de fermés d'intérieur vide est d'intérieur vide (théorème de Baire), il résulte que l'action de B_n sur $\mathbf{R}$ est libre sur une partie G_δ-dense, donc en au moins un point. □

Remarque. La lecture de [Ni] montre que Nielsen avait déjà établi l'existence d'une action de B_n sur le cercle, préservant l'ordre cyclique, fixant un point et ayant une orbite libre.

BIBLIOGRAPHIE

[Ad] S. I. ADYAN - *Fragments of the word Δ in a braid group*, Mat. Zametki **36** (1984), 25–34 (= Math. Notes **36** (1984), 505–510).

[A26] E. ARTIN - *Theorie der Zöpfe*, Abh. Math. Sem. Univ. Hamburg **4** (1926), 47–72.

[A47] E. ARTIN - *Theory of braids*, Ann. of Math. **48** (1947), 101–126.

[Bo] N. BOURBAKI - *Algèbre*, chapitres 1 à 3, Hermann, Paris, 1970.

[B+] *Braids*, Actes Conf. Santa Cruz (1986) publiés par Joan S. Birman et Anatoly Libgober, Contemp. Math., **78**, Amer. Math. Soc., Providence, RI, 1988.

[Br] E. BRIESKORN - *Automorphic sets and braids and singularities*, publié dans [B+], pages 45–115.

[Bu] S. BURCKEL - *The wellordering on positive braids*, J. Pure Appl. Algebra **120** (1997), 1–17.

[BZ] G. BURDE, H. ZIESCHANG - *Knots*, Studies in Math. **5**, Walter de Gruyter, Berlin-New York, 1985.

[CFP] J. W. CANNON, W. J. FLOYD, W. R. PARRY - *Introductory notes on Richard Thompson's groups*, Enseign. Math. (2) **42** (1996), 215–256.

[Ca] P. CARTIER - *Développements récents sur les groupes de tresses ; applications à la topologie et l'algèbre*, Séminaire Bourbaki, exposé **716** (novembre 1989), Astérisque, vol. 189–190, Soc. Math. France, Paris (1991), 17–67.

[D89] P. DEHORNOY - *La détermination projective (d'après Martin, Steel et Woodin)*, Séminaire Bourbaki, exposé **710** (juin 1989), Astérisque, vol. 177–178, Soc. Math. France, Paris (1989), 261–276.

[D92a] P. DEHORNOY - *Preuve de la conjecture d'irréflexivité pour les structures distributives libres*, C. R. Acad. Sci. Paris Sér. I Math. **314** (1992), 333–336.

[D92b] P. DEHORNOY - *Deux propriétés des groupes de tresses*, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), 633–638.

[D94] P. DEHORNOY - *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345** (1994), 115–150.

[D95] P. DEHORNOY - *From large cardinals to braids via distributive algebra*, J. Knot Theory Ramifications **4** (1995), 33–79.

[D96] P. DEHORNOY - *Une autre application de la théorie des ensembles*, Gaz. Math. **69** (1996), 3–20.

[D97a] P. DEHORNOY - *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997), 115–137.

[D97b] P. DEHORNOY - *A fast method for comparing braids*, Adv. Math. **125** (1997), 200–235.

[D98] P. DEHORNOY - *Gaussian groups are torsion free*, J. of Algebra **210** (1998), 291–297.

[D00] P. DEHORNOY - *Braids and self-distributivity*, disponible sur la Toile à l'URL http://www.math.unicaen.fr/~dehornoy/book.html, à paraître dans Progress in Math., Birkhäuser, Basel, Boston.

[DP] P. DEHORNOY, L. P. PARIS - *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. 79 (1999), 569–604.

[Do] R. DOUGHERTY - *Critical points in an algebra of elementary embeddings*, Ann. Pure Appl. Logic **65** (1993), 211–241.

[DJ] R. DOUGHERTY, T. JECH - *Finite left-distributive algebras and embedding algebras*, Adv. Math. **130** (1997), 201–241.

[Dr] A. DRÁPAL - *Finite left distributive algebras with one generator*, J. Pure Appl. Algebra **121** (1997), 233–251.

[EM] E. A. ELRIFAI, H. R. MORTON - *Algorithms for positive braids*, Quart. J. Math. Oxford Ser. (2) **45** (1994), 479–497.

[E+] D. B. A. EPSTEIN, J. W. CANNON, D. F. HOLT, S. V. F. LEVY, M. S. PATERSON, W. P. THURSTON - *Word processing in groups*, Jones and Bartlett Publ., Boston, Mass., 1992.

[F+] R. FENN, M. T. GREENE, D. ROLFSEN, C. ROURKE, B. WIEST - *Ordering the braid groups*, Pacific J. Math. 191 (1999), 49–74.

[FR] R. FENN, C. ROURKE - *Racks and links in codimension two*, J. Knot Theory Ramifications **1** (1992), 343–406.

[Ga] F. A. GARSIDE - *The braid group and other groups*, Quart. J. Math. Oxford **20** (1969), 235–254.

[Joy] D. JOYCE - *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65.

[Kan] A. KANAMORI - *The higher infinite. Large cardinals in set theory from their beginnings.* Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1994.

[Kau] L. H. KAUFFMAN - *Knots and physics*, Series on Knots and Everything, vol. 1, World Scientific Publishing Co., Inc., River Edge, NJ, 1991.

[KR] D. M. KIM, D. ROLFSEN - *Ordering groups of pure braids and hyperplane arrangements*, prépublication Univ. British Columbia, 1998.

[La] D. M. LARUE - *On braid words and irreflexivity,* Algebra Universalis **31** (1994), 104–112.

[L92] R. LAVER - *The left distributive law and the freeness of an algebra of elementary embeddings*, Adv. Math. **91** (1992), 209–231.

[L95] R. LAVER - *On the algebra of elementary embeddings of a rank into itself*, Adv. Math. **110** (1995), 334–346.

[L96] R. LAVER - *Braid group actions on left distributive structures, and well orderings in the braid groups*, J. Pure Appl. Algebra **108** (1996), 81–98.

[Mk] G. S. MAKANIN - *The conjugacy problem in the braid group*, Dokl. Akad. Nauk SSSR **182** (1968), 495–496 (= Soviet Math. Dokl. **9** (1968), 1156–1157).

[Mt] S. V. MATVEEV - *Distributive groupoids in knot theory*, Mat. Sb. (N.S.) **119 (161)** (1982), 78–88 (= Math. USSR Sbornik **47** (1984), 73–83).

[Mo] L. MOSHER - *Mapping class groups are automatic*, Ann. of Math. (2) **142** (1995), 303–384.

[MR] R. BOTTO MURA, A. H. RHEMTULLA - *Orderable groups*, Lecture Notes in Pure and Applied Mathematics, vol. **27**, Marcel Dekker, Inc., New York, Basel, 1977.

[Ni] J. NIELSEN, *Untersuchungen zur Topologie der geschlossenen zweiseitigen Flächen*, Acta Math. **50** (1927), 189–358 ; traduit en anglais par John Stillwell dans Jakob Nielsen, *Collected mathematical papers*, Birkhäuser, Boston, Basel, Stuttgart, 1986.

[Pa] D. S. PASSMAN - *The algebraic structure of group rings*, Pure and Applied

Mathematics, Wiley-Interscience, New York, London, Sydney, 1977.

[RZ] D. ROLFSEN, J. ZHU - *Braids, orderings and zero divisors*, J. Knot Theory Ramifications **7** (1998), 837–841.

[RW] C. ROURKE, B. WIEST - *Order automatic mapping class groups*, prépublication University of Warwick 1998, à paraître dans Pacific J. Math.

[SW] H. SHORT, B. WIEST - *Orderings of mapping class groups after Thurston*, prépublication CMI, Université de Provence 1999, math.GT/9907104.

[Th] W. P. THURSTON - courrier électronique à Bertold Wiest, 4 septembre 1998.

[W] B. WIEST - *Dehornoy's ordering of the braid groups extends the subword ordering*, Pacific J. Math. 191 (1999), 183–188.

Christian Kassel
Institut de Recherche Mathématique Avancée
Université Louis Pasteur - C.N.R.S.
7 rue René Descartes
67084 Strasbourg Cedex, France
E-mail : `kassel@math.u-strasbg.fr`
Fax : +33 (0)3 88 61 90 69
http://www-irma.u-strasbg.fr/~kassel/

(3 février 2000)