Algèbre/*Algebra*

Deux propriétés des groupes de tresses.

Patrick Dehornoy

Résumé – On décrit d'une part un algorithme de comparaison des mots de tresse, et, d'autre part, on établit des propriétés d'ordre sur les groupes de tresses liées à une réalisation de la structure distributive libre à un générateur.

Two properties of braid groups.

Abstract – We describe a new algorithm for comparing braid words, and establish some order properties for the braid groups which are connected with left distributive operations.

Abridged English Version. We apply to braids some tools used in the study of left distributive operations (*c.f.* [2]). The results deal with special decompositions of braid words. One describes a new quadratic algorithm for comparing braid words (*c.f.* [3]). Denote by $\mathcal{W}$ and $\mathcal{W}^+$ respectively the free monoids of braid words and of positive braid words.

Theorem 1.- *There exist two mappings* $\mathbf{D}_{LR}$ *and* $\mathbf{N}_{LR}$ *of* $\mathcal{W}$ *into* $\mathcal{W}^+$ *such that*
i) for every α *in* $\mathcal{W}$, α *and* $\mathbf{D}_{LR}(\alpha)^{-1}\mathbf{N}_{LR}(\alpha)$ *represent the same braid ;*
ii) the word α *represents the trivial braid if and only if the words* $\mathbf{D}_{LR}(\alpha)$ *and* $\mathbf{N}_{LR}(\alpha)$ *are empty ;*
iii) when only a fixed number of generators are used, the determination of $\mathbf{D}_{LR}(\alpha)$ *and* $\mathbf{N}_{LR}(\alpha)$ *for* α *with length* N *requires* $O(N^2)$ *steps.*

One also transfers to braids some ordering properties previously established for free distributive structures.

Theorem 2.- *For any* i, *a braid word with at least one occurrence of the generator* σ_i *but no occurrence of* σ_i^{-1} *cannot be trivial.*

Theorem 3.- *There exists a unique ordering on the braid group* B_∞ *which is compatible with the product on the left and is such that every generator is infinitely large with respect to the family of all* σ_k *with* $k > i$. *This ordering is linear, and there exists an effective algorithm for comparing braid words.*

The author thanks S. Burckel, G. Duchamp, Ch. Kassel and P. Vogel for their interest in the subject.

Let $\equiv$ be the congruence on $\mathcal{W}$ which presents Artin's braid group B_∞ as $\mathcal{W}/\equiv$. Define a mapping $\boldsymbol{c}_R$ by

$$\boldsymbol{c}_R(\sigma_i,\sigma_j)=\begin{cases}1 & \text{if } i=j\ ,\\ \sigma_i\sigma_j & \text{if } |i-j|=1\ ,\\ \sigma_i & \text{if } |i-j|\geq 2\ .\end{cases}$$

The pairs $\{\sigma_i\boldsymbol{c}_R(\sigma_j,\sigma_i),\sigma_j\boldsymbol{c}_R(\sigma_i,\sigma_j)\}$ generate the restriction of $\equiv$ to positive words, and

$$\sigma_i^{-1}\sigma_j\equiv\boldsymbol{c}_R(\sigma_j,\sigma_i)\boldsymbol{c}_R(\sigma_i,\sigma_j)^{-1}$$

always holds. This invites to transform any braid word α by iteratively replacing the factors $\sigma_i^{-1}\sigma_j$ by the corresponding factors $\boldsymbol{c}_R(\sigma_j,\sigma_i)\boldsymbol{c}_R(\sigma_i,\sigma_j)^{-1}$. In this way one finally obtains for α an equivalent expression as a right quotient of two positive words

$$\alpha\equiv\mathbf{N}_R(\alpha)\mathbf{D}_R(\alpha)^{-1}.$$

Similarly one constructs a left transformation leading to a symmetric decomposition

$$\alpha\equiv\mathbf{D}_L(\alpha)^{-1}\mathbf{N}_L(\alpha).$$

The congruence $\equiv$ is compatible with none of the above decompositions, but compatibility arises when both transformations are composed. Set

$$\begin{cases}\mathbf{N}_{LR}(\alpha)=\mathbf{N}_L(\mathbf{N}_R(\alpha)\mathbf{D}_R(\alpha)^{-1}),\\ \mathbf{D}_{LR}(\alpha)=\mathbf{D}_L(\mathbf{N}_R(\alpha)\mathbf{D}_R(\alpha)^{-1}).\end{cases}$$

PROPOSITION 6.- *Every braid word α satisfies $\alpha\equiv\mathbf{D}_{LR}(\alpha)^{-1}\mathbf{N}_{LR}(\alpha)$, and $\alpha\equiv\alpha'$ holds if and only if both $\mathbf{N}_{LR}(\alpha)\equiv\mathbf{N}_{LR}(\alpha')$ and $\mathbf{D}_{LR}(\alpha)\equiv\mathbf{D}_{LR}(\alpha')$ hold.*

This turns to be an algorithm for comparing braid words, since α is equivalent to 1 if and only if its numerator and denominator are *equal* to 1. One obtains a quadratic complexity for this method by observing that it preserves the length of the words with respect to an extended family of generators (the simple braids), and that there are only a finite number of simple braids (namely $n!$) in B_n.

A set equipped with a binary bracket $(x,y)\mapsto x[y]$ satisfying $x[y[z]]=x[y][x[z]]$ is called an LD-magma. Theorem 2 is proved by attaching to the strings in a braid labels which are chosen in the free LD-magma with one generator $\mathfrak{f}$. Apply the following rules : when the generator σ_i (*resp.* σ_i^{-1}) causes a string labelled y to go over a string labelled x, then the label y becomes $x[y]$ (*resp.* becomes the unique z such that $x=y[z]$, if it exists). For any given braid word, the initial choice of the labels can be made so that the rules above are obeyed. Then if σ_1^{-1} does not occur in the braid word α, the labels of the leftmost string make a nondecreasing sequence w. r. to the linear ordering of $\mathfrak{f}$ with satisfies $x<x[y]$ ([2]), and, if σ_1 occurs at least once, the final label is strictly above the initial one, and α cannot be trivial. As a corollary we have

PROPOSITION 8.- *The bracket on $\mathcal{W}$ defined by*

$$\alpha[\beta]=\alpha s(\beta)\sigma_1 s(\alpha)^{-1}$$

where s is the shift operator which maps every σ_i to the corresponding σ_{i+1} induces a left distributive bracket on B_∞ and the closure of 1 under this bracket is a free LD-magma.

This gives a decision method for the consequences of left distributivity (with only one variable) whose complexity is exponential, and drastically lowers the previous upper bound.

Introduction. Cette Note présente deux applications aux groupes de tresses de techniques utilisées pour l'étude des opérations distributives (voir [2]), et dont la motivation remonte en dernier ressort à la théorie des ensembles. Dans les deux cas, on s'intéresse à des écritures particulières des mots de tresse sous forme de quotients de mots positifs (c'est à dire où les inverses des générateurs n'apparaissent pas). On note $\mathcal{W}^+$ et $\mathcal{W}$ respectivement les monoïdes libres engendrés par des suites $(\sigma_1, \sigma_2, \ldots)$ et $(\sigma_1, \sigma_1^{-1}, \sigma_2, \sigma_2^{-1}, \ldots)$, dont les éléments seront appelés mots de tresse positifs et mots de tresse.

THÉORÈME 1. – *Il existe deux applications* $\mathbf{D}_{LR}$ *et* $\mathbf{N}_{LR}$ *de* $\mathcal{W}$ *dans* $\mathcal{W}^+$ *telles que*
i) pour tout mot de tresse α, $\mathbf{D}_{LR}(\alpha)^{-1}\mathbf{N}_{LR}(\alpha)$ *représente la même tresse que* α *;*
ii) le mot α *représente la tresse triviale si et seulement si les mots* $\mathbf{D}_{LR}(\alpha)$ *et* $\mathbf{N}_{LR}(\alpha)$ *sont vides ;*
iii) lorsque le nombre de générateurs σ_i *est borné, la détermination de* $\mathbf{D}_{LR}(\alpha)$ *et* $\mathbf{N}_{LR}(\alpha)$ *pour un mot* α *de longueur* N *se fait en un nombre d'étapes de l'ordre de* N^2*.*

On obtient ainsi un nouvel algorithme de complexité quadratique pour comparer deux mots de tresse, qui à la différence de la méthode de Thurston dans [3], évite toute réduction à une forme normale particulière.

THÉORÈME 2. – *Un mot de tresse où un générateur* σ_i *apparaît, mais pas son inverse, ne peut pas être trivial.*

Dans un groupe G, muni d'un ordre (strict) $\prec$, on dira que l'élément a est infiniment grand par rapport à la partie X si $x \prec yay^{-1}$ est vrai pour tous x, y dans le sous-groupe engendré par X.

THÉORÈME3. – *Il existe un unique ordre sur le groupe* B_∞ *qui soit compatible avec les translations à gauche, et tel que, pour tout entier* i*, le générateur* σ_i *est infiniment grand par rapport à la famille des* σ_k *pour* $k > i$*. Cet ordre est un ordre total, et il existe un algorithme effectif pour comparer les mots de tresse.*

Je remercie Gérard Duchamp, Christian Kassel et Pierre Vogel qui ont bien voulu examiner la propriété du théorème 2 lorsqu'elle était une conjecture. Par ailleurs, la formulation en termes de complexité des propritétés de retournement énoncées dans le théorème 1 a été suggérée par Serge Burckel.

Retournements de mots de tresse. La congruence sur $\mathcal{W}^+$ engendrée par les paires $\{\sigma_i\sigma_j, \sigma_j\sigma_i\}$ avec $|i-j| \geq 2$ et $\{\sigma_i\sigma_j\sigma_i, \sigma_j\sigma_i\sigma_i\}$ avec $|i-j| = 1$ est notée $\equiv^+$. Si $\equiv$ désigne la congruence sur $\mathcal{W}$ engendrée par $\equiv^+$ et les paires $\{\sigma_i\sigma_i^{-1}, 1\}$ et $\{\sigma_i^{-1}\sigma_i, 1\}$, le groupe B_∞ est le quotient $\mathcal{W}/\equiv$ ([1]). Par [4], on sait que $\equiv^+$ est la restriction de $\equiv$ à $\mathcal{W}^+$. Considérons alors la « fonction de complément » $\boldsymbol{c}_R$ définie par

$$\boldsymbol{c}_R(\sigma_i, \sigma_j) = \begin{cases} 1 & \text{si } i = j \ , \\ \sigma_i\sigma_j & \text{si } |i-j| = 1 \ , \\ \sigma_i & \text{si } |i-j| \geq 2 \ . \end{cases}$$

Les paires $\{\sigma_i\boldsymbol{c}_R(\sigma_j, \sigma_i), \sigma_j\boldsymbol{c}_R(\sigma_i, \sigma_j)\}$ engendrent la congruence $\equiv^+$. Pour tous i, j, on a

$$\sigma_i^{-1}\sigma_j \equiv \boldsymbol{c}_R(\sigma_j, \sigma_i)\boldsymbol{c}_R(\sigma_i, \sigma_j)^{-1},$$

ce qui invite, partant d'un mot α quelconque dans $\mathcal{W}$, à « retourner à droite » les facteurs $\sigma_i^{-1}\sigma_j$ qui y figurent en l'expression $\boldsymbol{c}_R(\sigma_j, \sigma_i)\boldsymbol{c}_R(\sigma_i, \sigma_j)^{-1}$ correspondante, et à itérer le processus. Partant d'un mot quelconque α, l'ordre des retournements n'importe pas, de sorte que l'itération, si elle se termine, aboutit à une forme unique bien définie de type AB^{-1} où A et B sont des mots positifs, qu'on notera respectivement $\mathbf{N}_R(\alpha)$ et $\mathbf{D}_R(\alpha)$. Pour la terminaison de l'itération, le problème est l'augmentation de la longueur des mots. Pour le résoudre, on détermine une clôture de l'ensemble des générateurs pour l'opération $\boldsymbol{c}_R$. Ceci revient à introduire de nouveaux générateurs par rapport auxquels la longueur n'augmente pas. La définition suivante est suggérée par l'algèbre distributive

Définition. – Un mot de tresse positif A est *simple* s'il est équivalent à un produit (fini) $\prod_{i=0}^{\infty} \sigma_i^{(k_i)}$, où $\sigma_i^{(k)}$ est $\sigma_{i+k-1}\sigma_{i+k-2}\ldots\sigma_{i+1}\sigma_i$ pour $k \geq 1$ et 1 pour $k = 0$.

Les tresses simples sont aussi les facteurs des « demi-tours » Δ_n de [4].

Lemme 4. – *Si A, B sont des mots de tresse simples, les mots $\mathbf{N}_R(A^{-1}B)$, $\mathbf{D}_R(A^{-1}B)$ existent et sont simples.*

Le retournement d'un mot α de longueur ℓ ne fera apparaître que des mots écrits comme produits de ℓ mots simples, et pourra se déterminer par au plus $\ell^2/4$ retournements de mots du type $A^{-1}B$ avec A et B simples. Donc, pour chaque mot α, les mots $\mathbf{N}_L(\alpha)$ et $\mathbf{D}_L(\alpha)$ existent toujours. Pour les mots du type $A^{-1}B$ avec A et B simples, les valeurs de $\mathbf{N}_R$ et $\mathbf{D}_R$ peuvent être déterminées géométriquement en utilisant une correspondance bijective entre tresses simples et permutations des entiers qui coïncident finalement avec l'identité. Si on se restreint au cas du groupe B_n, c'est à dire au cas de $n-1$ générateurs, il y a exactement $n!$ tresses simples. Ayant déterminé une fois pour toutes une table de retournement pour ces mots, on obtient un algorithme qui, pour tout mot α, détermine $\mathbf{N}_R(\alpha)$ et $\mathbf{D}_R(\alpha)$ en un nombre d'étapes proportionnel au carré de la longueur de α.

Comme chaque étape de retournement transforme un mot en un mot équivalent, l'équivalence

$$\alpha \equiv \mathbf{N}_R(\alpha)\mathbf{D}_R(\alpha)^{-1}$$

est vérifiée pour tout mot α. Grâce aux propriétés particulières de la fonction $\boldsymbol{c}_R$, on peut caractériser la dépendance des fonctions $\mathbf{N}_R$ et $\mathbf{D}_R$ par rapport à la congruence $\equiv$.

LEMME 5. – *Soient A, B, A', B' des mots de tresse positifs.*
i) Supposons $A \equiv^+ A'$ et $B \equiv^+ B'$; alors on a

$$\mathbf{N}_R(A^{-1}B) \equiv^+ \mathbf{N}_R(A'^{-1}B') \text{ et } \mathbf{D}_R(A^{-1}B) \equiv^+ \mathbf{D}_R(A'^{-1}B').$$

ii) Supposons $AB^{-1} \equiv A'B'^{-1}$; alors il existe des mots positifs C, C' satisfaisant

$$\mathbf{N}_R(A^{-1}B)C \equiv^+ \mathbf{N}_R(A'^{-1}B')C' \text{ et } \mathbf{D}_R(A^{-1}B)C \equiv^+ \mathbf{D}_R(A'^{-1}B')C'.$$

Le point (ii) est insuffisant pour obtenir par projection sur B_∞ une notion bien définie de numérateur et de dénominateur. Mais on peut exploiter le caractère palindromique des relations de tresse. Si $\boldsymbol{c}_L$ est défini par

$$\boldsymbol{c}_L(\sigma_i, \sigma_j) = \begin{cases} 1 & \text{si } i = j \ , \\ \sigma_j\sigma_i & \text{si } |i-j| = 1 \ , \\ \sigma_i & \text{si } |i-j| \geq 2, \end{cases}$$

les paires $\{\boldsymbol{c}_L(\sigma_j, \sigma_i)\sigma_i, \boldsymbol{c}_L(\sigma_i, \sigma_j)\sigma_j\}$ engendrent elles aussi la congruence $\equiv^+$. Par des retournements à gauche consistant à remplacer un facteur $\sigma_i\sigma_j^{-1}$ par le facteur $\boldsymbol{c}_L(\sigma_j, \sigma_i)^{-1}\boldsymbol{c}_L(\sigma_i, \sigma_j)$ correspondant, on obtient pour tout mot α une écriture

$$\alpha \equiv \mathbf{D}_L(\alpha)^{-1}\mathbf{N}_L(\alpha).$$

Posons, pour tout mot de tresse α,

$$\begin{cases} \mathbf{N}_{LR}(\alpha) = \mathbf{N}_L(\mathbf{N}_R(\alpha)\mathbf{D}_R(\alpha)^{-1}), \\ \mathbf{D}_{LR}(\alpha) = \mathbf{D}_L(\mathbf{N}_R(\alpha)\mathbf{D}_R(\alpha)^{-1}). \end{cases}$$

Alors par le critère du lemme 5.ii (et sa contrepartie pour les retournements à gauche) on a

PROPOSITION 6. – *Pour tout mot de tresse α, on a $\alpha \equiv \mathbf{D}_{LR}(\alpha)^{-1}\mathbf{N}_{LR}(\alpha)$, et la relation $\alpha \equiv \alpha'$ est équivalente à la conjonction de $\mathbf{N}_{LR}(\alpha) \equiv^+ \mathbf{N}_{LR}(\alpha')$ et $\mathbf{D}_{LR}(\alpha) \equiv^+ \mathbf{D}_{LR}(\alpha')$.*

On a ainsi une notion intrinsèque de numérateur et de dénominateur pour les tresses. Ceci constitue un algorithme de comparaison, puisqu'un mot est équivalent à 1 si et seulement si son numérateur et son dénominateur sont équivalents à 1, donc *égaux* à 1 (puisqu'il s'agit de mots positifs).

Etiquetage des brins d'une tresse. Le théorème 2 provient de l'algèbre distributive. Une structure formée d'un ensemble muni d'un crochet distributif à gauche, c'est à dire d'une opération $(x, y) \mapsto x[y]$ satisfaisant $x[y[z] = x[y][x[z]]$, étant appelée un LD-magma, notons $\mathfrak{f}$ le LD-magma libre engendré par un unique élément a. Suivant l'idée de [6], on utilise les éléments de $\mathfrak{f}$ pour étiqueter les brins des tresses. Soit d'abord A un mot de tresse positif. Partant d'un étiquetage des brins par des éléments de $\mathfrak{f}$, on propage les étiquettes en posant que, lorsque σ_i prescrit de faire passer un brin étiqueté y par dessus un brin étiqueté x, l'étiquette y devient $x[y]$. Il est facile de voir que cet étiquetage est compatible avec les relations de tresses. Pour l'étendre à des mots non nécessairement positifs, le problème est que, si σ_i^{-1} prescrit de faire passer x sur y, alors le brin x doit être renommé par un z vérifiant $y[z] = x$. La théorie de $\mathfrak{f}$ indique que la solution est unique quand elle existe. On dira que le mot de tresse α est $\mathfrak{f}$-étiquetable s'il existe un étiquetage initial des brins qui puisse s'étendre à tout le mot de proche en proche.

LEMME 7. – *Tout mot de tresse est* $\mathfrak{f}$*-étiquetable.*

On montre d'abord que tout mot de la forme $A^{-1}B$ est $\mathfrak{f}$-étiquetable en inscrivant l'étiquetage $(a, a, \ldots)$ « au milieu » puis en le propageant vers le haut par A et vers le bas par B. Pour le cas général on utilise le retournement à gauche : un mot quelconque se retourne en un mot de type $A^{-1}B$, et on peut montrer qu'un mot qui se retourne en un mot $\mathfrak{f}$-étiquetable est lui-même $\mathfrak{f}$-étiquetable.

Le théorème 2 est une conséquence pour les tresses de l'existence d'un ordre sur $\mathfrak{f}$ qui satisfasse $x <_{\mathfrak{f}} x[y]$ pour tous x, y ([2]). Dans le cas particulier du générateur σ_1, on peut le démontrer comme suit. Soit α un mot de tresse où σ_1^{-1} n'apparaît pas. Il existe un $\mathfrak{f}$-étiquetage de α. Soit x_0, x_1,... la suite des étiquettes des brins gauches de la tresse. Par construction, on a ou bien $x_{k+1} = x_k$ (si le k-ième facteur de α est σ_i ou σ_i^{-1} avec $i \geq 2$), ou bien $x_{k+1} = x_k[z]$ pour un certain z (si ce k-ième facteur est σ_1). Alors la suite $(x_0, x_1, \ldots)$ est croissante (au sens large) pour l'ordre $<_{\mathfrak{f}}$, et la valeur x_0 ne peut réapparaître dès que le facteur σ_1 a été rencontré au moins une fois. Ceci implique que le mot α n'est pas trivial, car l'étiquetage de sortie d'une tresse triviale coïncide nécessairement avec son étiquetage d'entrée.

Le théorème 2 est en fait équivalent à l'existence de l'ordre $<_{\mathfrak{f}}$ sur $\mathfrak{f}$. Notant s l'endomorphisme de $\mathcal{W}$ qui, pour tout i, envoie σ_i sur σ_{i+1}, on a

PROPOSITION 8. – *Le crochet défini sur* $\mathcal{W}$ *par*

$$\alpha[\beta] = \alpha s(\beta)\sigma_1 s(\alpha)^{-1}$$

induit un crochet distributif à gauche sur B_∞*, et la clôture de 1 pour ce crochet est un LD-magma libre.*

Le premier point se vérifie directement. Pour le second, on sait (voir [7]) qu'un LD-magma $\mathfrak{g}$ à un générateur est libre si (et seulement si) aucune égalité de type $x = x[y_1]\ldots[y_k]$ n'est possible dans $\mathfrak{g}$. Or une égalité de ce type dans B_∞ s'expliciterait en une égalité de type

$$x = xs(z_0)\sigma_1 s(z_2)\sigma_1 \ldots \sigma_1 s(z_k),$$

qui contredirait le théorème 2.

On déduit que, pour déterminer si une identité $P = Q$ (écrite avec le crochet et une variable) est ou non conséquence de l'identité de distributivité à gauche, il suffit de calculer les images de P et Q dans B_∞ et de comparer les mots de tresse ainsi obtenus. La complexité algorithmique est simplement exponentielle en la taille de P et Q, ce qui améliore grandement la borne de [2]. Le théorème 3 est un autre corollaire de la proposition 8. L'unique ordre (total) sur B_∞ dont l'existence est affirmée est construit à partir d'une extension lexicographique de l'ordre total $<_{\mathfrak{f}}$ sur $\mathfrak{f}$.

RÉFÉRENCES BIBLIOGRAPHIQUES.

[1] J. BIRMAN, *Braids, links, and mapping class groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

[2] P. DEHORNOY, *Preuve de la conjecture d'irréflexivité pour les structures distributives libres*, Comptes-rendus de l'Acad. des Sciences de Paris, **314-I** (1992) p. 333–336.

[3] D. EPSTEIN & *al.*, Word Processing in Groups, Jones & Barlett Publ. (1992).

[4] F. A. Garside, *The Braid Group and other Groups*, Quart. J. Math. Oxford **20** No 78 (1969) p. 235–254.

[5] A. Jacquemard, *About the effective classification of conjugacy classes of braids*, Journal of Pure and Applied Algebra, **63** (1990) 161–169.

[6] D. Joyce, *A classifying invariant of knots : the knot quandle*, Journal of Pure and Applied Algebra, **23** (1982) p. 37–65.

[7] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Mathematics, *à paraître*.

Département de Mathématiques, Université de Caen, 14032 *Caen cedex.*
adresse électronique : dehornoy@geocub.greco–prog.fr