Le calcul des tresses(*)

Patrick Dehornoy

Introduction

Qu'est-ce qu'une tresse ? Une tresse n'est pas a priori un objet mathématique, mais les tresses ont une structure mathématique. Pourquoi ce titre, le calcul des tresses ? En un sens que l'on va préciser, les tresses généralisent les entiers et, de même qu'on peut calculer avec les entiers, on peut calculer avec les tresses. De manière plus précise, il existe des algorithmes de calcul pour les tresses. Pour terminer, on décrira des applications récentes de ces algorithmes de calcul à la cryptographie.

Le groupe des tresses

Une tresse c'est une suite de croisements (Fig. 1).

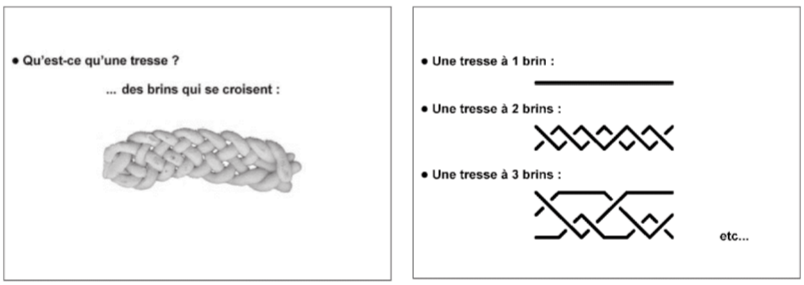
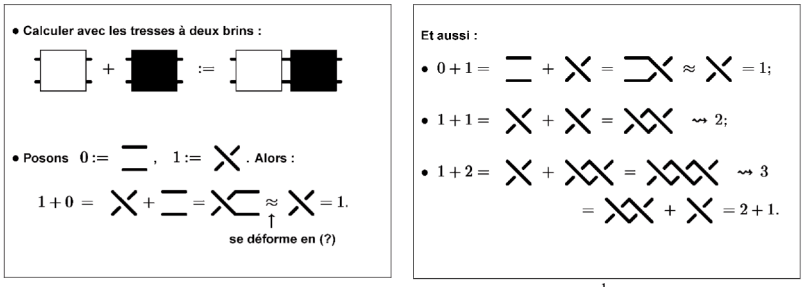


Figure 1

Comment calculer avec les tresses à deux brins ? Pour définir la somme de deux tresses, il suffit de considérer chacune d'entre elles comme une boîte avec deux brins en entrée et deux brins en sortie. Les ajouter est simplement défini comme les mettre bout à bout. Notons **0** la tresse triviale (sans croisement) et **1** la tresse où le brin du bas passe **sous** celui du haut. En ajoutant ces deux tresses, on retrouve la tresse **1** après déformation des brins – cette déformation, l'isotopie, notée $\approx$, sera précisée plus tard. Donc l'addition vérifie $1 + 0 = 1$ (Fig. 2 a).
On peut ainsi, par induction, obtenir des tresses correspondant à chaque entier naturel (Fig. 2 b).

Pour définir une soustraction, on note **−1** la tresse où le brin du bas passe **sur** celui du haut (c'est la tresse qui est l'image de la tresse **1** par une symétrie d'axe vertical). On obtient, en faisant comme précédemment, l'égalité $1 + (-1) = 0$ (Fig. 3 a).

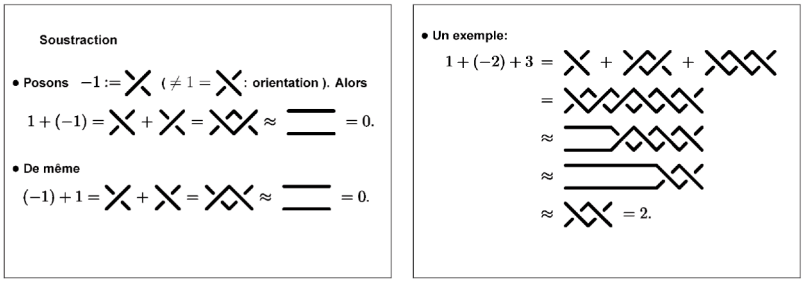
(*) Notes rédigées par Didier Trotoux d'après l'exposé de Patrick Dehornoy.



a b

Figure 2

On peut construire alors des tresses représentant chaque entier relatif et effectuer des opérations sur les tresses dont le résultat correspond aux égalités vérifiées par les entiers relatifs (Fig. 3 b).



a b

Figure 3

En conclusion, les tresses à deux brins forment un groupe isomorphe à l'ensemble **Z** des entiers relatifs, ce qui se conçoit bien car une tresse à deux brins est complètement caractérisée par le nombre de demi-tours effectués (avec un signe qui indique l'orientation des croisements). Notons que ce ne sont pas exactement les tresses qui constituent un groupe au sens de l'algèbre, mais les tresses à isotopie près, c'est-à-dire les objets qu'on obtient quand on identifie deux à deux les tresses isotopes.

Pour n ≥ 3, on définit l'addition comme précédemment et on définit l'opposé d'une tresse en prenant son image miroir par rapport à un axe vertical (Fig. 4). Pour chaque entier *n*, on construit, à partir des tresses à *n* brins, un groupe qu'on note B_n (B pour *braid*, qui signifie *tresse* en anglais). Ce groupe a été considéré implicitement par C. F. Gauss et A. Hurwitz et étudié explicitement par E. Artin en 1925.

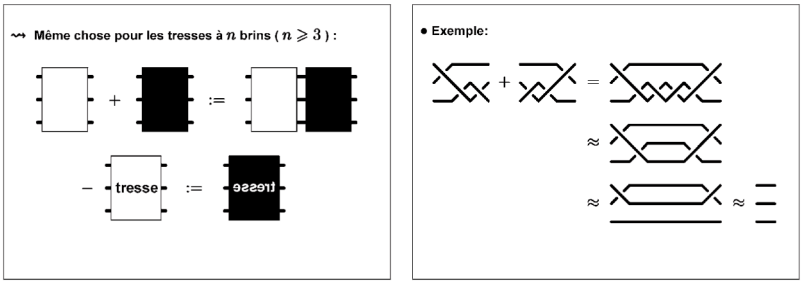


Figure 4

Ce groupe n'est pas commutatif comme le montre l'exemple suivant ($n = 3$) :

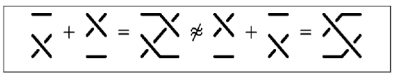


Figure 5

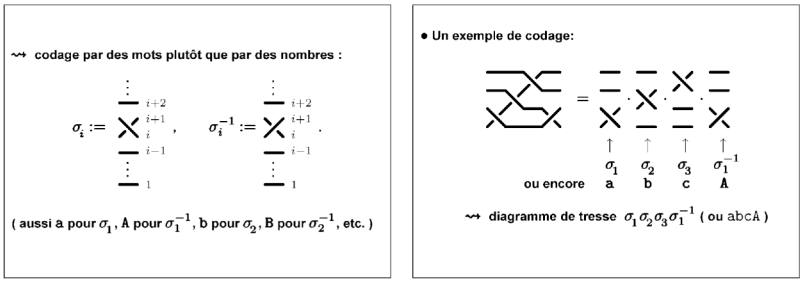
Comme l'addition n'est pas commutative dans B_n pour $n \geq 3$, on remplacera dans la suite de cet exposé l'addition par la multiplication, on notera 1 la tresse triviale et on remplacera opposé par inverse.

Le codage des tresses

L'existence du produit des tresses permet de passer du langage des dessins à celui des mots. En effet, une conséquence de la définition de la multiplication de tresses est qu'une tresse quelconque est décomposable en un produit de tresses élémentaires à un seul croisement : une telle décomposition consiste à découper la tresse en tranches verticales qui ne contiennent qu'un seul croisement. Or il est facile de coder les tresses à un seul croisement : comme les deux brins qui se croisent sont voisins (sinon il faudrait aussi croiser les brins intermédiaires, et il y aurait plus d'un croisement), il suffit, pour spécifier un croisement élémentaire, d'indiquer la position des deux brins concernés. On numérote les brins de la tresse de bas en haut de 1 à n.

On note σ_1 (resp. σ_1^{-1}) ou a (resp A) la tresse élémentaire où les brins 1 et 2 se croisent, le brin 1 passant sous (resp. sur) le brin 2, σ_2 (resp. σ_2^{-1}) ou b (resp. B) celle où les brins 2 et 3 se croisent, le brin 2 passant sous (resp. sur) le brin 3, et plus généralement, on note σ_i celle ou les brins i et $i + 1$ se croisent, le brin i passant sous (resp. sur) le brin $i + 1$ (Fig 6 a).

Le produit de tresses élémentaires se code alors sous la forme d'une succession de lettres – un mot – qui caractérise la tresse qui en résulte (Fig 6 b). Un tel codage facilite les calculs, un ordinateur traitant plus facilement des mots que des dessins.



a b

Figure 6

L'isotopie des tresses

Un diagramme de tresse est un objet plan. C'est la projection sur le plan d'une figure de l'espace $\mathbf{R}^3$. On déclare que deux diagrammes sont équivalents lorsqu'on obtient l'un à partir de l'autre en déplaçant des brins, sans les autoriser à se traverser ni décrocher leurs extrémités. On dit aussi que ces diagrammes sont isotopes (Fig. 7).

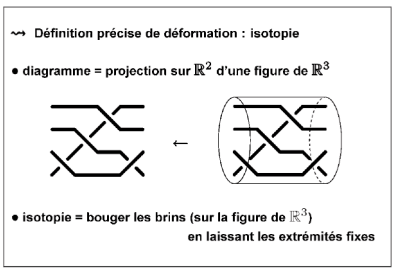
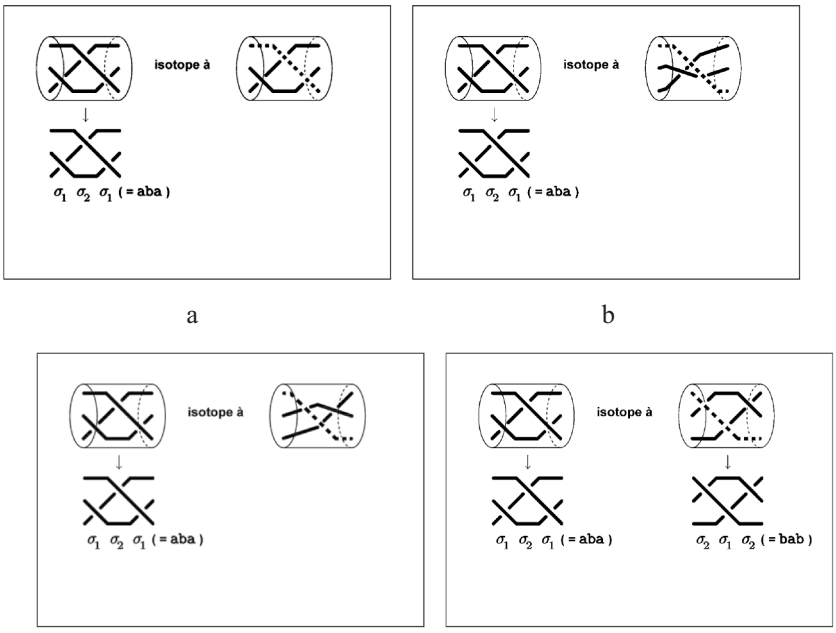


Figure 7

Considérons, par exemple, le diagramme $\sigma_1\sigma_2\sigma_1$ (ou *aba*). En déplaçant les brins, on peut transformer ce diagramme en un diagramme isotope mais distinct codé $\sigma_2\sigma_1\sigma_2$ (ou *bab*) (Fig. 8).

On a donc deux diagrammes ou deux mots distincts pour la même tresse.

On en déduit que, dans le groupe B_n, on a la relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ ou $aba = bab$, appelée « relation de tresse ». Il y a donc des relations spécifiques entre certains éléments de B_n, ce que l'on exprime en disant que le groupe B_n n'est pas libre pour $n \geq 3$.



a b c d

Figure 8

Le premier théorème qui a été démontré par Artin vers 1925 est le suivant :

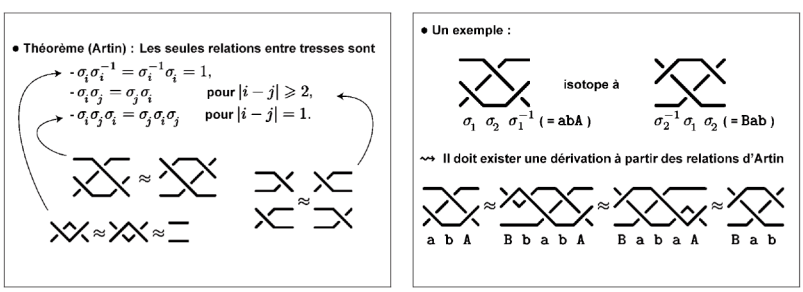
Les seules relations entre tresses sont les conséquences des relations :

$$\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1,$$

$$\sigma_i\sigma_j = \sigma_i\sigma_j \quad \text{pour } |i-j| \geq 2,$$

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \quad \text{pour } |i-j| = 1.$$

On peut voir (Fig. 9 a) les diagrammes de tresse correspondants.



a b

Figure 9

Il est relativement facile de vérifier ces relations, mais le résultat d'Artin indique que ce sont les seules relations existant entre les tresses élémentaires : si deux mots de tresse représentent la même tresse, alors nécessairement on peut passer de l'une à l'autre par les seules relations de tresse. Notons que ceci ne résout pas le problème d'isotopie, tant qu'on n'a pas d'algorithme pour reconnaître si deux mots se déduisent l'un de l'autre par les relations de tresses.

Sur l'exemple précédent (Fig. 9 b), on a eu la chance de rendre compte de l'isotopie en mettant en évidence la dérivation $ab\mathrm{A} \approx \mathrm{B}bab\mathrm{A} \approx \mathrm{B}aba\mathrm{A} \approx \mathrm{B}ab$ mais on n'a pas de méthode c'est-à-dire d'algorithme permettant de trouver systématiquement une dérivation entre deux diagrammes de tresses appartenant à une même classe d'isotopie.

Classification des tresses

Classer les tresses consiste à donner une recette pour reconnaître si deux diagramme de tresse donnés quelconques sont ou non isotopes, c'est-à-dire si l'on peut passer de l'un à l'autre en déplaçant leurs brins – ou ce qui est équivalent de reconnaître si deux mots codent la même tresse.

Dans le cas d'une tresse à deux brins, il suffit de compter les demi-tours, mais dans le cas de trois brins et plus, ce problème, appelé problème de mot de B_n, est nettement plus difficile. On sait le résoudre depuis les travaux d'Artin (1925). Pour autant, le sujet n'est pas clos, car la solution d'Artin, quoique irréprochable en théorie, est très peu efficace en pratique. Lorsque deux tresses sont un peu compliquées, même un ordinateur puissant ne peut reconnaître, par la méthode d'Artin, si elles sont isotopes. Depuis plusieurs décennies, la question de la classification des tresses a suscité de nombreux travaux, et plusieurs méthodes ont été proposées, de plus en plus efficaces. Citons notamment les solutions de F.A. Garside (1967), à Oxford, de Pierre Deligne (1972), médaille Fields en 1970, de William Thurston (1988), également médaille Fields, et celles plus récentes d'Ivan Dynnikov (1999) et la réduction des poignées de l'auteur (1997) dont on donne une idée ci-dessous.

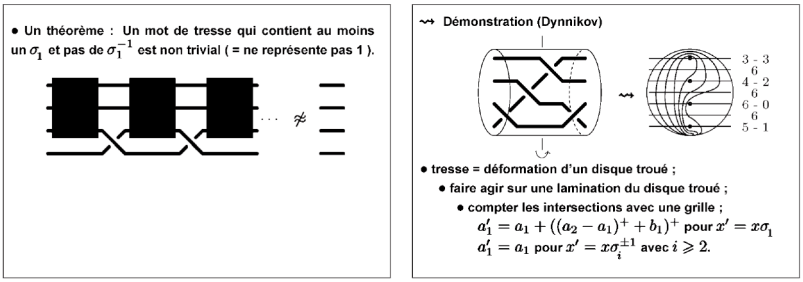
Une première remarque est la suivante. Comme toute tresse a un inverse, notre problème se ramène à reconnaître si une tresse donnée est isotope à la tresse triviale. En effet, pour que la tresse t' soit isotope à la tresse t ($t' \approx t$) il faut et il suffit que la tresse $t^{-1}t'$ soit isotope à la tresse $t^{-1}t$, donc à la tresse triviale ($t^{-1}t' \approx 1$). Le problème de mot revient donc à savoir si une tresse est triviale c'est-à-dire si une tresse peut être détressée ou non.

Signalons tout de suite que la méthode physique, qui consisterait à réaliser un modèle physique de la tresse avec des ficelles et à tirer sur ces ficelles pour effectuer le démêlage ne marche pas ! Il y a des cas où les algorithmes de relaxation ne fonctionnent pas et où il faut commencer par emmêler la tresse pour pouvoir la démêler ensuite.

L'idée théorique qui permet de construire l'algorithme de démêlage qu'on va décrire est le théorème suivant :

Théorème : Un mot de tresse qui contient au moins un σ_1 et pas de σ_1^{-1} est non trivial.

Ce résultat peut être illustré par le schéma suivant (Fig. 10 a) où tous les croisements du bas sont dans le même sens. Dans cette situation, on ne peut pas déformer cette tresse en une tresse triviale ce qui peut sembler une banalité mais n'est pas facile à prouver.



a b

Figure 10

On regarde la tresse en dimension 3 et on regarde le cylindre vu du bout : on a un disque avec n trous correspondant aux n brins qui se déforment et on peut voir une tresse comme la déformation d'un disque troué. L'idée de Dynnikov est de mettre dans ce disque une lamination (une famille de courbes fermées qui entourent le premier trou, les deux premiers trous, etc.) puis de compter les intersections de la transformée de la lamination avec une grille et de prendre ces nombres (en fait les différences entre le nombre de points d'intersection à gauche et celui à droite, soit $a_1 = 5 - 1 = 4$, $a_2 = 6 - 0$, $a_3 = 4 - 2 = 2$, $a_1 = 3 - 3 = 0$, dans l'exemple de la Fig. 10 b) comme coordonnées de la tresse.

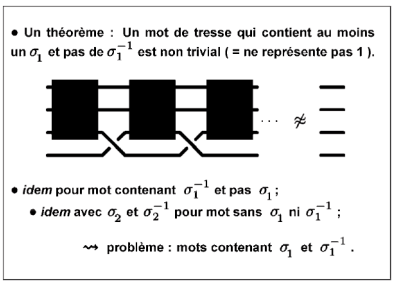


Figure 11

Quand on multiplie une tresse par un σ_1, les a_1' de la tresse x' sont liés aux a_1 de x par les formules :

$$a_1' = a_1 + \left((a_2 - a_1)^+ + b_1\right)^+ \text{ pour } x' = x\sigma_1,$$

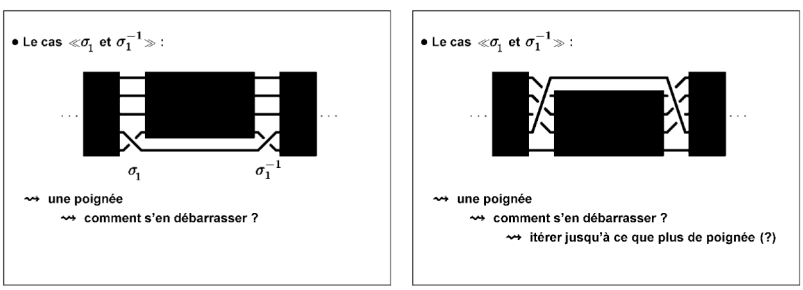
$$a_1' = a_1 \text{ pour } x' = x\sigma_i^{\pm 1} \text{ avec } i \geq 2,$$

où $x^+ = \sup(x, 0)$. On voit que a_1 ne peut qu'augmenter quand on multiplie par des σ_1 (à cause de la fonction x^+) et que si l'on ne multiplie pas par des σ_1^{-1}, on ne peut pas obtenir $a_1 = 0$, ce qui est nécessaire si on veut avoir une tresse triviale.

La méthode de démêlage décrite plus loin sous le nom de réduction des poignées est fondée sur ce résultat.

Le théorème donne un quart de la réponse (cas où il y a du σ_1 et pas de σ_1^{-1}). Il donne aussi une réponse analogue dans le cas où il y a du σ_1^{-1} et pas de σ_1, car la tresse inverse a du σ_1 et pas de σ_1^{-1} et, par conséquent, n'est pas triviale. Et s'il n'y a ni σ_1, ni de σ_1^{-1}, on va recommencer avec σ_2 et de σ_2^{-1}. On peut imaginer alors une preuve par récurrence.

Le problème arrive quand il y a à la fois du σ_1 et du σ_1^{-1}, car alors le théorème ne permet pas de conclure. On peut alors représenter la tresse comme sur la figure 12 a. Le brin qui sort en position 2 de la boîte de gauche, passe sous la boîte du centre puis entre en position 2 dans la boîte de droite sera appelé une poignée. Il faut donc se débarrasser des poignées. Une façon de faire est de faire passer cette poignée vers le haut en utilisant un algorithme de saut à la corde comme sur la figure 12 b. L'idée serait alors de recommencer cette procédure jusqu'à ce qu'il n'y ait plus de poignées.



a b

Figure 12

Réduction des poignées

Considérons l'exemple de la figure 13. On fait disparaître la première poignée en la faisant passer vers le haut mais ce faisant on crée une nouvelle poignée. Supprimons cette nouvelle poignée en la faisant passer vers le haut : on obtient alors une tresse qui contient deux σ_1 et pas de σ_1^{-1}. D'après le théorème, cette tresse est donc non triviale.

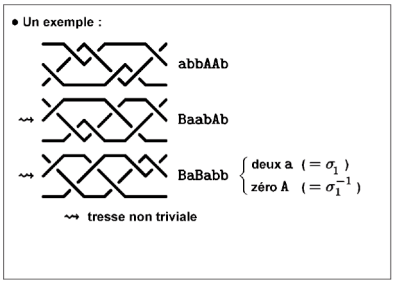
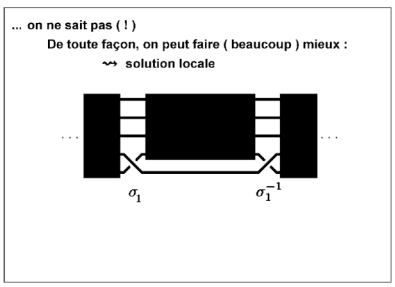
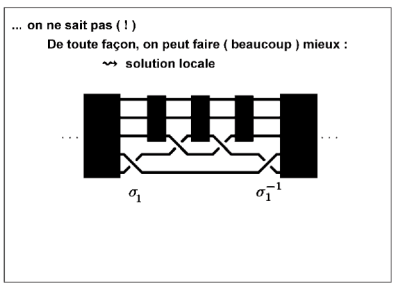


Figure 13

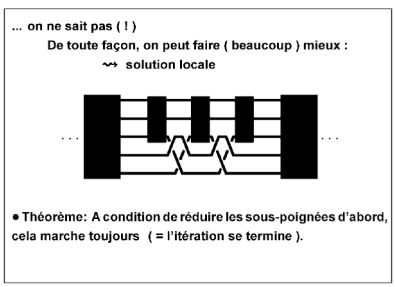
L'exemple précédent est-il juste un exemple bien choisi ou bien cette méthode marche-t-elle toujours ? On ne sait pas. On attend encore une démonstration mais ce n'est pas très grave car on sait faire mieux. Reprenons l'exemple précédent et regardons plus précisément ce qui se trouve dans la boîte du centre. Dans cette boîte, il peut y avoir des σ_2 des σ_2^{-1}, des σ_3 des σ_3^{-1}… Au lieu de faire le grand tour comme précédemment pour se débarrasser de la poignée, on ne va faire que le tour des σ_2. C'est une solution locale qui paraît beaucoup plus économique (Fig. 14 a, b et c).



a



b



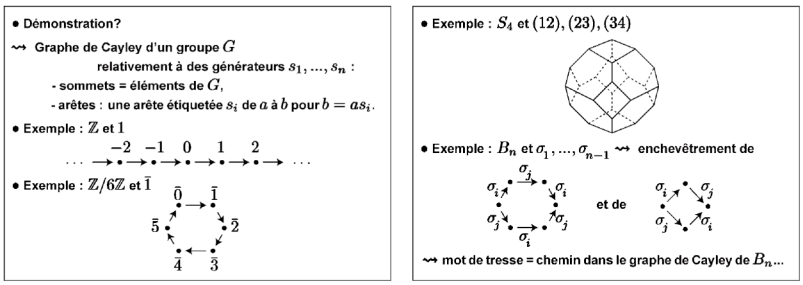
c

Figure 14

Et en faisant comme cela, on arrive toujours à supprimer les poignées grâce au résultat suivant :

Théorème : À condition de savoir réduire les sous-poignées en premier, l'itération se termine toujours en un nombre fini d'étapes – et on a donc une solution au problème d'isotopie des tresses.

La démonstration de ce théorème est difficile et fait intervenir la notion de graphe de Cayley d'un groupe G relatif à des générateurs s_1, s_2, …, s_n. Les sommets de ce graphe sont les éléments du groupe G et les arêtes du graphe sont étiquetées par les générateurs s_i : il y a une arête étiquetée de a à b si $b = as_i$. Ce graphe permet de visualiser le groupe. Par exemple, le graphe de Cayley du groupe symétrique S_4 est un graphe fini constitué d'hexagones et de carrés.
Le graphe de Cayley du groupe des tresses est nettement plus compliqué. Mais il est constitué d'un enchevêtrement d'hexagones et de carrés correspondant aux relations de tresse (Fig. 15 b), comme celui de S_4, ce qui n'est pas un hasard car chaque tresse induit une permutation sur les brins.
La preuve de la démonstration du théorème ci-dessus utilise le fait qu'un mot de tresse est une suite de générateurs et constitue un chemin dans le graphe de Cayley de B_n.



a b

Figure 15

Implémentation de l'algorithme de réduction des mots

Cet algorithme est facile à traduire dans un langage informatique si l'on remarque qu'une poignée est un sous mot du type a…A ou A…a sans a ni A au milieu et que vérifier qu'il n'y a pas de sous-poignée c'est contrôler qu'il n'y a pas à la fois de b et de B au milieu de la poignée.

Réduire revient donc à :
1 : supprimer a et A ;
2 : remplacer b par Bab et B par BAb dans le cas a…A,
remplacer b par baB et B par bAA dans le cas A…a.

Cet algorithme est très efficace : un mot de tresse de 10 000 lettres sur 100 brins est traité en une seconde sur un ordinateur de bureau. C'est la méthode la plus efficace

connue aujourd'hui mais il n'y a pas de preuve élémentaire de convergence et la complexité algorithmique est inconnue : on ne sait pas en combien d'étapes cet algorithme réduit un mot, mais seulement en donner un majorant très grand.

Pourquoi étudier les tresses ? Applications.

1. Dans le domaine des mathématiques

À chaque tresse est associée une permutation. On a n brins à gauche et à l'arrivée, à droite, on retrouve les n brins dans un ordre différent. Les positions ont subi une permutation. Mais la tresse est plus que cette permutation car à partir de celle-ci, on ne peut reconstituer la tresse. La tresse contient en elle l'ordre dans lequel les croisements (transpositions) ont été effectués. C'est pour cela que l'on peut dire qu'une tresse est une permutation plus l'histoire de cette permutation.
Le groupe des tresses est donc une extension du groupe symétrique et a donné lieu à une vaste théorie qui se rattache à de la combinatoire algébrique et à la théorie de Coxeter (F. Garside, P. Deligne, E. Brieskorn, …)

2. Dans le domaine de la physique

Le groupe des tresses peut être associé aux symétries de l'équation de Yang-Baxter. Si V est un espace vectoriel et R un opérateur linéaire sur $V \otimes V$, alors, en notant $R_{i,i+1}$ pour $id_{i-1} \otimes R \otimes id_{n-i-1}$, il existe une représentation de B_n dans $V^{\otimes n}$ envoyant σ_2 sur $R_{i,i+1}$ si et seulement si R satisfait l'équation de Yang–Baxter

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}.$$

On reconnaît dans cette dernière relation une analogie avec la relation de tresse $aba = bab$. Quand on étudie une équation, on étudie les symétries associées (cf. la théorie de Galois).
Ceci se rattache à la représentation matricielle des groupes de tresses et à la théorie de la cohomologie (V. Arnold, D. Krammer, V. Bigelow, …).

3. Dans le domaine de la chimie, de la biologie

Une autre approche des tresses est son lien avec la théorie des nœuds. Une tresse est un nœud ouvert. L'étude des tresses permet d'aider à la classification des nœuds. C'est un problème nettement plus difficile que la classification des tresses car on ne peut pas multiplier les nœuds. (V. Jones, V. Turaev, L. Kauffman, …)

4. Application en cryptographie

C'est une application récente et relativement élémentaire.
Pour faire de la cryptographie avec un groupe, il faut un groupe à la fois simple (c'est-à-dire dans lequel il est facile de calculer) et compliqué (c'est-à-dire dans lequel il y a des problèmes difficiles) : c'est le cas du groupe des tresses pour $n \geq 3$ car il n'est pas commutatif et on peut utiliser des tresses x et y qui ne commutent pas et pour lesquelles y est différent de xyx^{-1} (tresse conjuguée).
Il serait un peu naïf de coder y par xyx^{-1}. Ce qu'on utilise c'est la difficulté à trouver y à partir de xyx^{-1}. Au cours des années récentes, plusieurs systèmes cryptographiques basés sur les groupes de tresses ont été proposés (M. Anshell & al.,

K.-H. Ko & al.).

Échange de clé : le problème pour Alice et Bob est de se mettre d'accord à distance sur une clé commune s, de sorte qu'un intrus observant les échanges ne puisse trouver s. Le protocole est le suivant. On note $B_{n,2n}$ l'ensemble des tresses formées sur les générateurs $\sigma_{n+1}, ..., \sigma_{2n-1}$.

- On choisit p publique dans B_{2n} ;
- Alice choisit a dans B_n et envoie $p_A = apa^{-1}$ à Bob ;
- Bob choisit b dans $B_{n,2n}$ et envoie $p_B = bpb^{-1}$ à Alice ;
- La clé s est obtenue par Alice en calculant ap_Ba^{-1} et par Bob en calculant bp_Ab^{-1}.

Les tresses a et b commutent car elles font intervenir respectivement les brins 1 à n et les brins $n + 1$ à $2n$. On a donc $ab = ba$ et

$$ap_Ba^{-1} = abpb^{-1}a^{-1} = bapa^{-1}b^{-1} = bp_Ab^{-1},$$

c'est-à-dire qu'à la fin Alice et Bob ont bien la même tresse. La sécurité de cette méthode réside dans la difficulté à déterminer a à partir du couple (p, p_A) et b à partir de (p, p_B).

Pour le moment, on sait mal construire des tresses pour lesquelles il soit certain que le problème de conjugaison considéré est difficile, ce qui pose problème pour le choix des clés et rend le futur de ces approches encore incertain.

Bibliographie

P. Dehornoy, L'art de tresser, Dossier hors série Pour La Science nº 15, avril 1997, p. 68-75.

P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, Why are braids orderable ?, Panoramas et synthèses Vol. 22, Société Mathématique de France.

Le diaporama de cette conférence est téléchargeable sur les pages personnelles de P. Dehornoy http://www.math.unicaen.fr/~dehornoy

Laboratoire de Mathématiques Nicolas Oresme de l'Université de Caen – Basse Normandie http://www.math.unicaen.fr/lmno