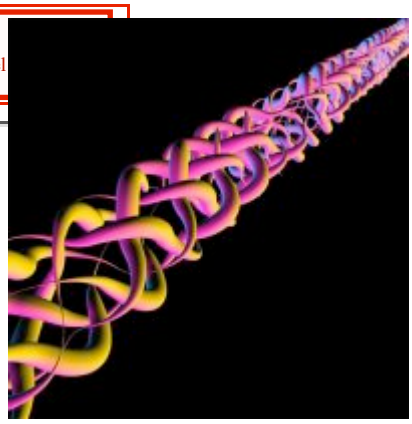
Les tresses : de la topologie à la cryptographie

Luis Paris

Les tresses : de la topologie à la cryptographie

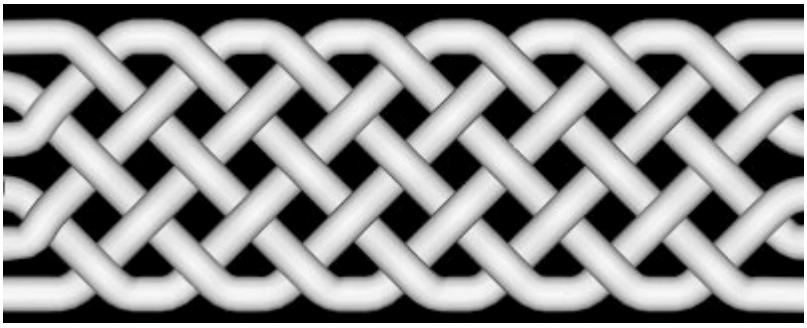


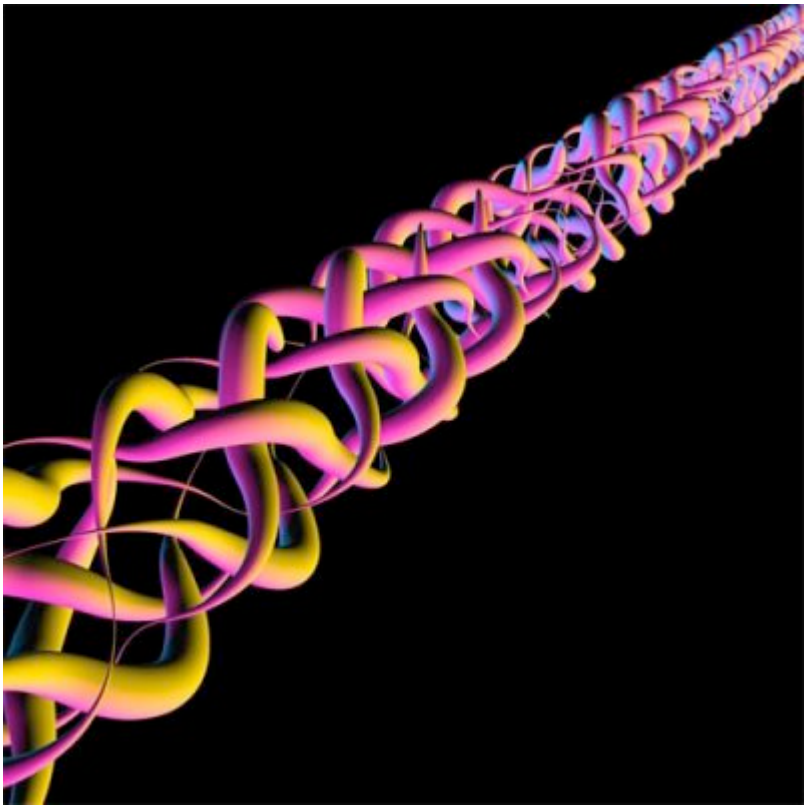
Le 11 janvier 2009, par **Luis Paris**
Professeur, Université de Bourgogne (**page web**)

Introduction

De la tresse...

LA notion de tresse, vue comme objet « tressé, natté ou entrelacé » remonte à plusieurs siècles et a été universellement utilisée à des fins décoratives ou même pratiques, par exemple dans la confection de cordes ou de câbles. Une tresse peut être un entrelacement de trois cordelettes ou brins, le brin gauche passant par dessus le brin central, puis le brin droit, puis le gauche, puis le droit, cette opération étant répétée autant de fois que nécessaire (voir la figure 1). Mais une tresse désigne aussi tout entrelacement de plusieurs cordes ou brins à condition que celles-ci suivent une direction précise. Des exemples de tresses décoratives sont donnés dans les figures 2 et 3.





... à la théorie des tresses

Les mathématiciens décrivent les tresses à l'aide de modèles abstraits qui sont au centre d'une théorie appelée « théorie des tresses ». Celle-ci joue un rôle central en mathématiques et a des ramifications dans d'autres branches des mathématiques mais aussi d'en d'autres sciences telles que la physique, la biologie, l'informatique et la cryptographie.

Le dessein de cet article est de présenter à un lecteur non mathématicien un aperçu de cette théorie. Nous allons donner une définition des tresses mathématiques, puis illustrer leur utilisation dans trois domaines : les nœuds (branche des mathématiques), l'algorithmique (branche à la croisée des mathématiques et de l'informatique) et la cryptographie (domaine des mathématiques, de l'informatique, et des sciences de la communication). Il existe de nombreuses autres applications ou interactions, surtout avec d'autres parties des mathématiques, mais aussi, par exemple, avec l'astrophysique. En effet, les lignes de champ magnétique dans l'atmosphère solaire forment des tresses et la complexité de leur « tressage » est directement liée à l'intensité du champ.

La théorie des tresses est un domaine très actif en France organisé autour d'un Groupe de Recherche (GDR 2105 du CNRS) appelé GDR TRESSES. Celui-ci a été créé en 2000 par Patrick Dehornoy (voir encadré) pour une période de 2 ans, puis a été renouvelé pour 4 ans, de 2003 à 2007, sous la direction de Christian Blanchet, Professeur à l'Université de Bretagne Sud, et est dirigé depuis janvier 2008 par Luis Paris, Professeur à l'Université de Bourgogne. Dès son début, une spécificité importante de ce groupement a été de mélanger des chercheurs de différents domaines. Il comprend 18 équipes de mathématiques et 2 d'informatique, réparties

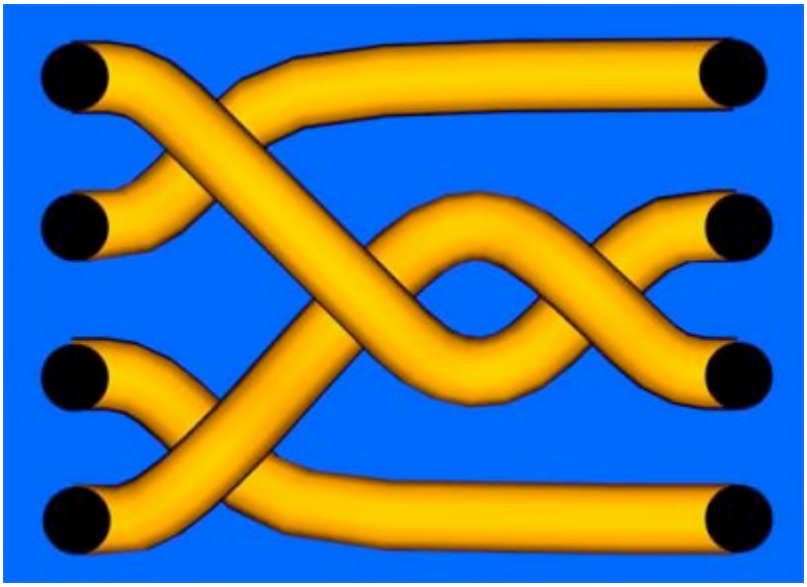
dans toute la France. Par ailleurs, un nombre important d'étrangers participe régulièrement à ses réunions. Le GDR TRESSES a acquis une renommée internationale comme en témoigne la présentation d'un colloque sur le domaine qui s'est tenu à Banff (Canada) en avril dernier (voir [1]) et qui présente le GDR TRESSES comme un modèle.

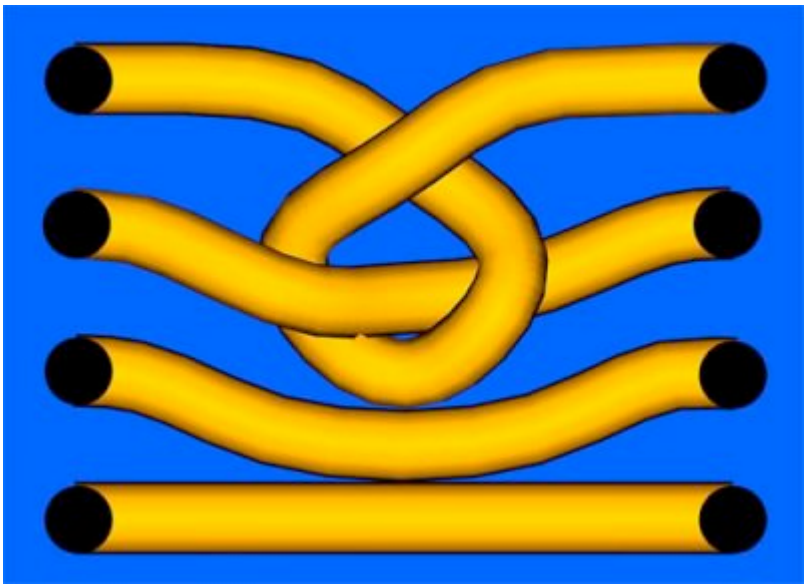
Patrick Dehornoy (né le 11 septembre 1952 à Rouen) est un mathématicien français connu pour ses travaux en théorie des ensembles et en théorie des tresses. Il est professeur à l'Université de Caen et membre senior de l'Institut Universitaire de France. C'est le fondateur du groupe de recherche « GDR TRESSES » qui regroupe la recherche française dans la théorie des tresses.

Les tresses mathématiques

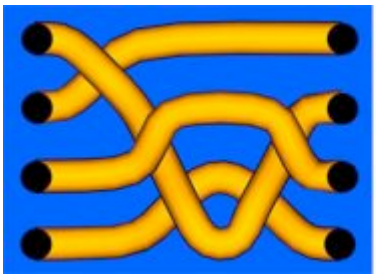
Qu'est ce qu'une tresse au sens mathématique ?

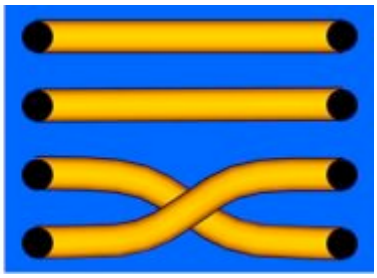
La *théorie des tresses* dégage le concept de tresse à partir des tresses telles qu'on les imagine. Tout d'abord, on se fixe un nombre entier n. Pour faciliter la tache de l'exposé nous prendrons $n = 4$ tout en sachant que les descriptions qui suivent sont valables quelque soit la valeur de n. On se donne deux ensembles de 4 objets (des clous, par exemple) que l'on dispose sur une table (ce sont les points noirs dans la figure 4). Les objets de chaque famille sont alignés verticalement de sorte que le premier ensemble de « clous » est situé en face du deuxième ensemble. En utilisant quatre cordelettes (que l'on appelle *brins*) on relie tout objet de la première famille à un objet de la seconde. Une telle connexion est appelée tresse. Les brins peuvent passer les uns sur les autres, mais jamais revenir en arrière. Ainsi, la connexion de la figure 5 n'est pas une tresse (au sens mathématique).

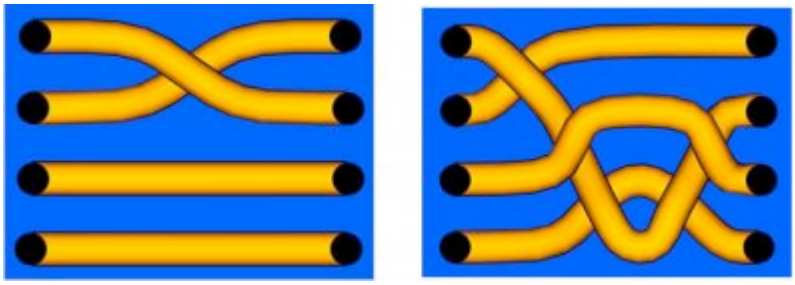




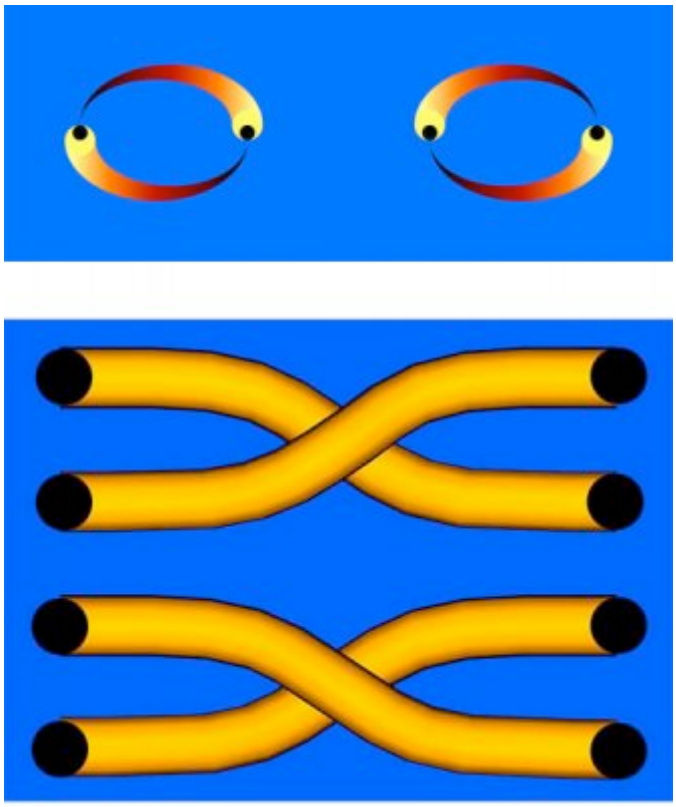
Les deux connexions de la figure 6 sont différentes. Par contre les connexions de la figure 7 sont les mêmes car on peut passer de l'une à l'autre en « bougeant les brins ».





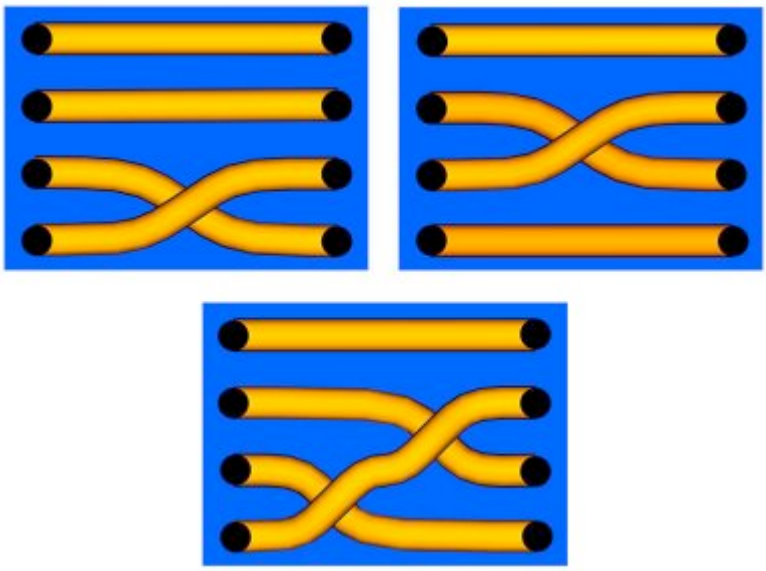


Une tresse peut aussi être considérée comme une série de chemins décrits par 4 particules qui ne se rencontrent pas (ou n'entrent pas en collision). Ici l'ensemble des points de départ doit coïncider avec l'ensemble des points d'arrivée. Par exemple, les trajectoires des 4 particules représentées dans la partie haute de la figure 8 correspondent à la tresse du bas. Plus prosaïquement, les tresses peuvent être vues comme des danses où, à la fin, chaque danseur prendrait la place d'un autre.

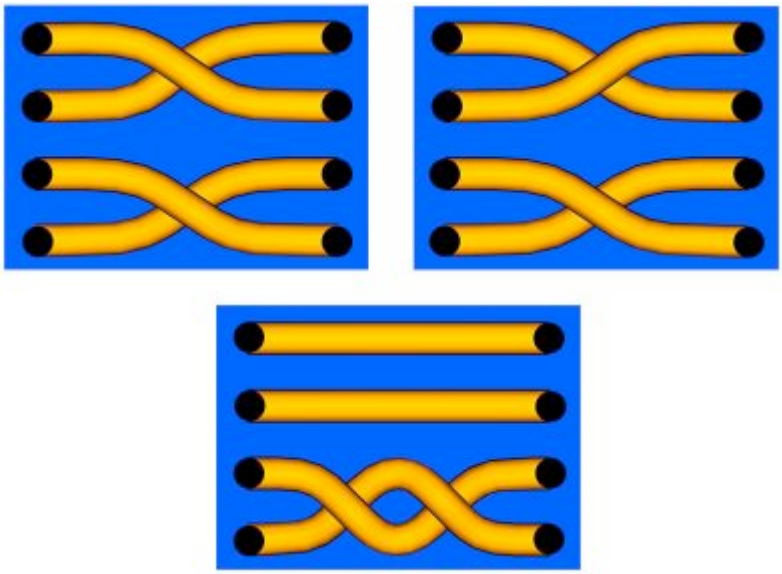


Compliquons un peu en juxtaposant les tresses

A partir de deux tresses α et β on peut construire une troisième tresse, notée $\alpha\beta$ et appelée *composée de* α *et* β simplement en juxtaposant (ou concaténant) les deux tresses. Ainsi, la composée des tresses α et β en haut de la figure 9 est la tresse $\alpha\beta$ du bas de la même figure.

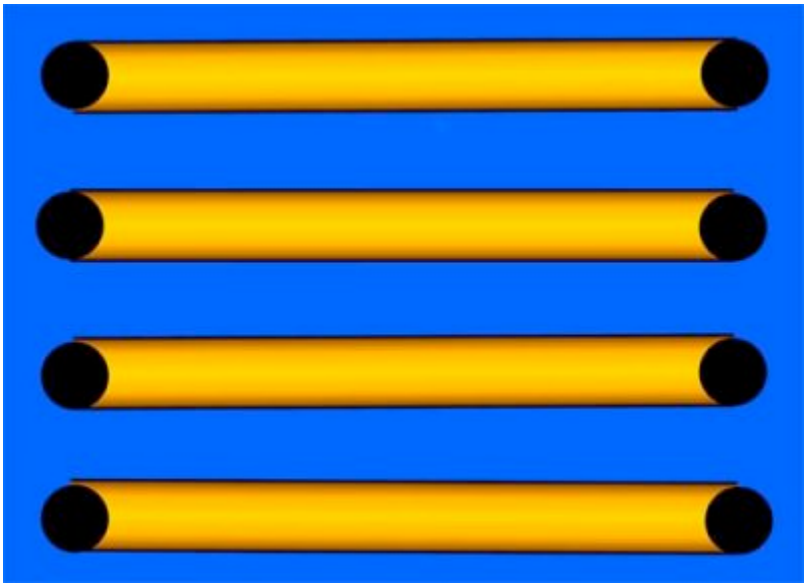


Un autre exemple est donné dans la figure 10.

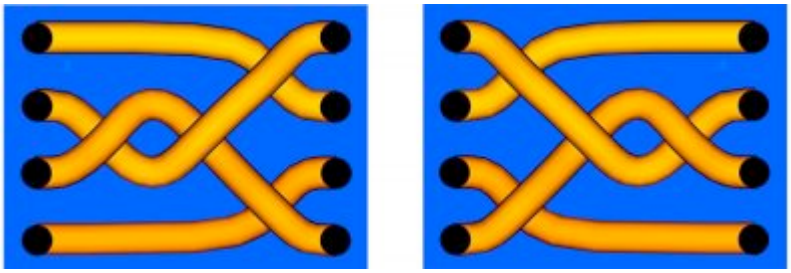


Le lecteur averti remarquera que la tresse $\alpha\beta$ peut être différente de la tresse $\beta\alpha$: c'est le cas pour l'exemple de la figure 9 mais pas pour celui de la figure 10.

La tresse de la figure 11 s'appelle la *tresse triviale*. On observe facilement que la composition d'une tresse α avec la tresse triviale, que se soit à gauche comme à droite, n'altère pas la tresse α.

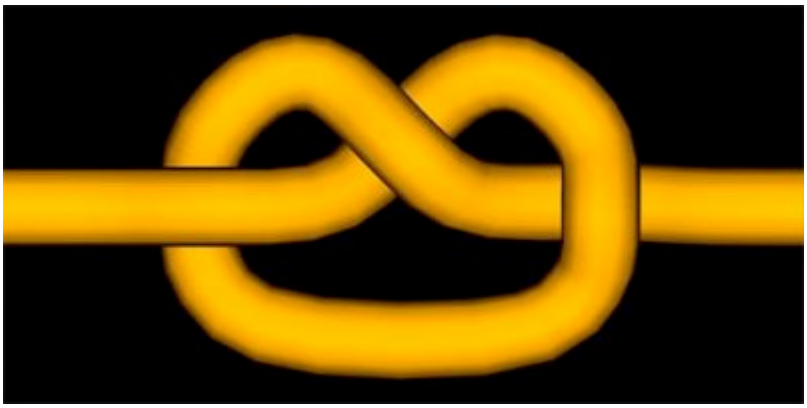


Le reflet d'une tresse α sur un *miroir* que l'on aurait posé perpendiculairement à la table à hauteur de la seconde famille de « clous » s'appelle la tresse miroir de α (voir la figure 12). La composition d'une tresse avec sa tresse miroir donne la tresse triviale. Ceci peut être aisément vérifié dans l'exemple de la figure 12.



Des tresses aux groupes de tresses

Les tresses telles que nous les avons définies ainsi que leurs compositions forment ce que les mathématiciens appellent le *groupe des tresses*. On a un groupe des tresses à deux brins, un groupe des tresses à trois brins, etc. Le groupe des tresses à un brin ne contient que la tresse triviale car un brin ne peut pas être tressé bien qu'il puisse être noué (voir la figure 13).

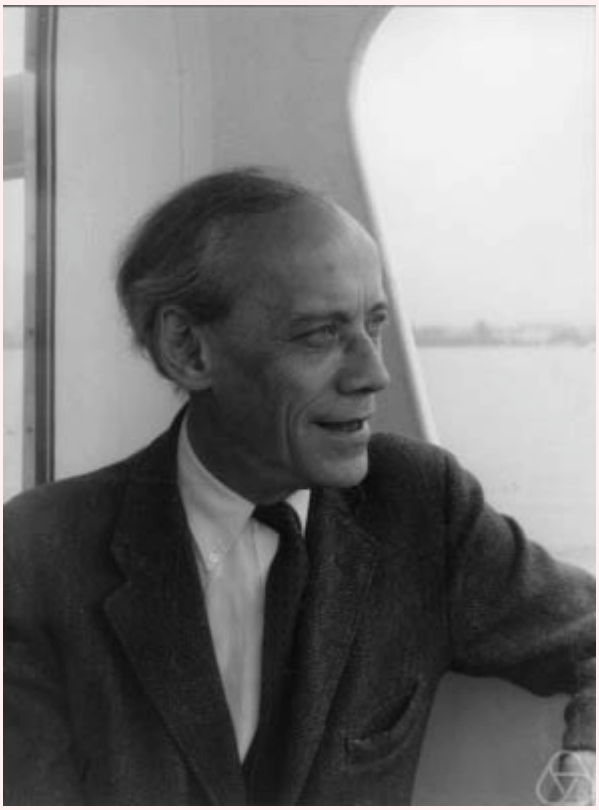


La composition des tresses respecte un certain nombre de règles qui sont toutes aussi

importantes pour un mathématicien que les tresses elles-mêmes, si ce n'est plus.

L'origine de la théorie des tresses

On fait généralement remonter l'étude mathématique des tresses à un article d'Emile Artin [**Art-25**] datant de 1925 dans lequel il décrit la notion de tresse sous différents aspects, l'un étant celui évident, comme une « série de brins tendus et entrelacés », et d'autres, d'ordre plus mathématiques mais tout aussi profonds, par exemple, comme groupe donné par « générateurs et relations », comme « groupe d'automorphismes d'un groupe libre » ou comme « groupe de difféotopies d'un disque pointé ». C'est la diversité de ces différentes approches qui fait l'intérêt des groupes des tresses.

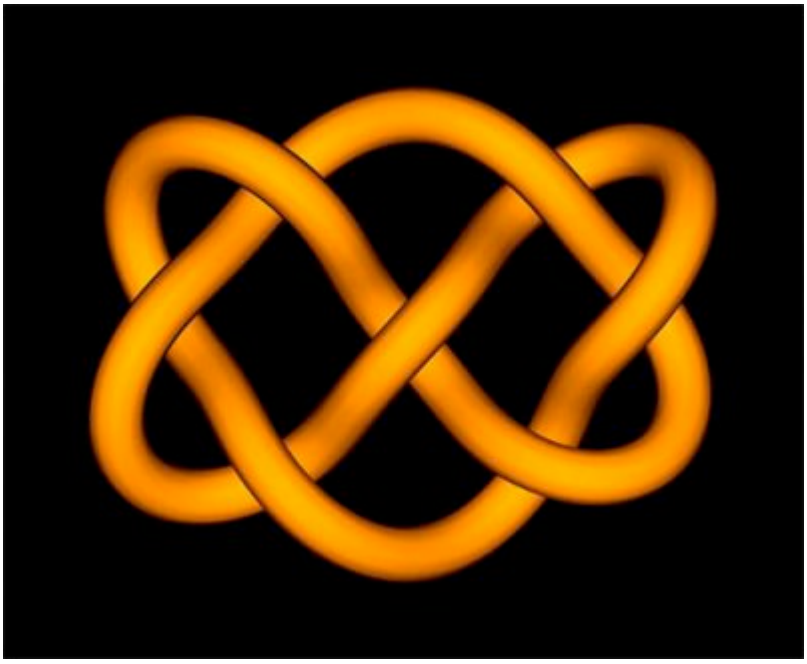


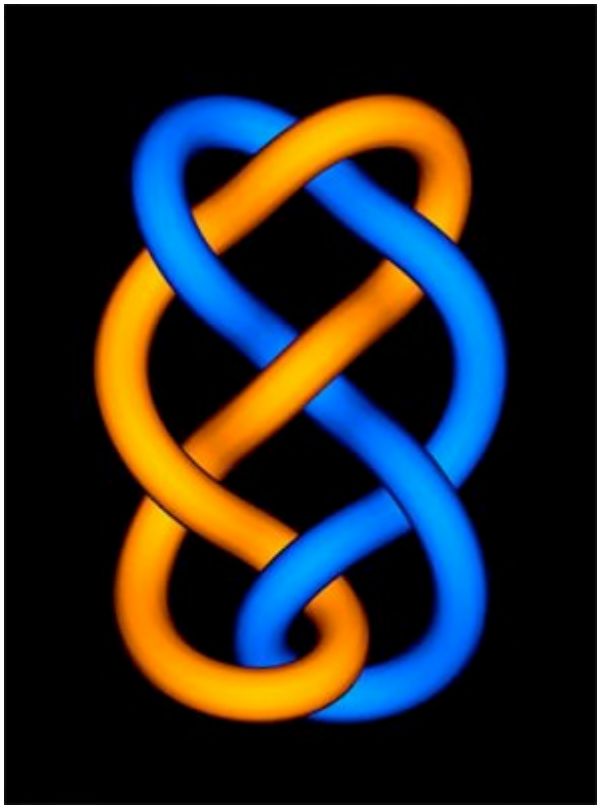
Emil Artin (1898-1962) fut un mathématicien autrichien. Il a fait sa carrière en Allemagne (principalement à Hambourg) jusqu'à l'arrivée des nazis en 1937. Il émigra alors aux Etats-Unis où il fut professeur à l'Université d'Indiana de 1938 à 1946, puis à l'Université de Princeton de 1946 à 1958. Il fut un des algébristes les plus éminents du 20ème siècle. Il est en particulier à l'origine de la théorie des tresses.

Des tresses à la théorie des nœuds

Qu'est-ce qu'un nœud en mathématiques ?

Un *nœud* en mathématiques est une corde fermée (qui n'a pas de bout) (voir la figure 14). Un *entrelacs à deux composantes* est formé de deux cordes fermées (voir la figure 15), un *entrelacs à trois composantes* est formé de trois cordes fermées, etc. La *théorie des nœuds* est la branche de la topologie qui étudie les nœuds et les entrelacs. En topologie une sphère ne se différencie pas d'un cube et un beignet est la même chose qu'une tasse. On n'y tient pas compte des propriétés rigides des objets telles que les longueurs ou les angles, le but étant de comprendre des propriétés qu'aucune torsion, étirement ou contraction ne peut changer.





En dehors des mathématiques, et plus particulièrement de la topologie, la théorie des nœuds a des applications à des problèmes de biologie et de chimie. Elle est utilisée par exemple dans l'étude de molécules *isomères* (arrangements différents de la même formule chimique) ou dans l'étude de l'action de certaines enzymes sur l'ADN.

L'origine de la théorie des nœuds

La première contribution significative à la théorie des nœuds semble être due à Sir William

Thomson (Lord Kelvin) et sa théorie des « vortex atomiques ». En 1867, après avoir observé des expériences du physicien écossais Peter Tait impliquant des anneaux de fumée, Thomson est arrivé à la conclusion que les atomes sont des nœuds de « vortex tourbillonnants dans le luminiferous æther ». Les éléments chimiques correspondraient ainsi à des nœuds ou entrelacs. Suivant cette idée, Peter Tait a commencé à classer les nœuds en croyant qu'il faisait une table des éléments.

Sir William Thomson

(1824-1907) fut un physicien, mathématicien et ingénieur écossais. Il est considéré comme un des leaders de la Physique du 19ème siècle.

Problème central de la théorie des nœuds : distinguer deux nœuds

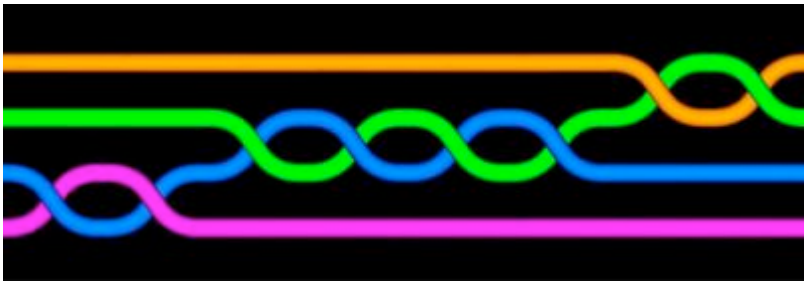
Le problème central de la théorie des nœuds est de les distinguer ou, plus encore, de les classer. Pour les distinguer il faut être capable de décider si deux dessins de nœuds (ou d'entrelacs) représentent le même nœud (ou entrelacs) ou non. Dans les années 20 Alexander et Briggs [**AlBr-26**] (mathématiciens américains) et, indépendamment, Reidemeister [**Rei-26**] (mathématicien allemand) proposent un algorithme partiel pour résoudre ce problème. Cet algorithme répond OUI si deux dessins représentent le même nœud (ou entrelacs) et ne répond pas sinon. En d'autres termes, on sait dire si deux nœuds sont les mêmes, mais on ne sait pas dire s'ils sont différents. Ceci peut paraître contradictoire au lecteur, mais c'est un paradoxe typique des mathématiques. Imaginez que vous attendez quelqu'un. Vous vous dites : « s'il vient, c'est un ami ». Conclusion : s'il n'arrive pas, vous ne saurez pas si c'est un ami.

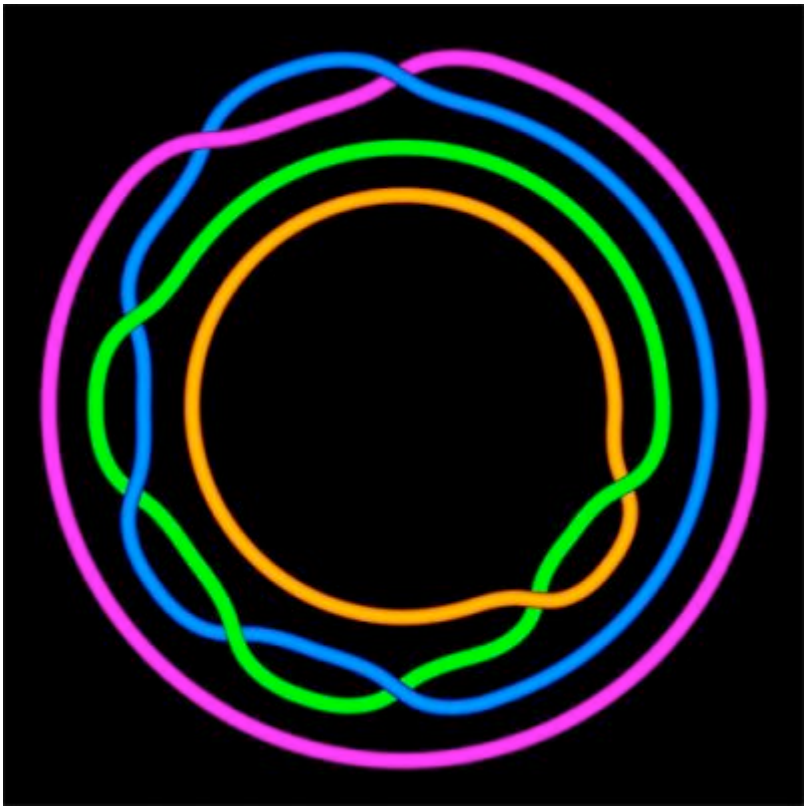
Pour distinguer deux nœuds on fait appel à ce que les mathématiciens appellent des « *invariants* ». A chaque dessin de nœud on attribue un objet (souvent un nombre ou un polynôme) que l'on sait ne dépendre que du nœud et non de sa représentation. Si les invariants de deux nœuds sont différents, les nœuds sont différents. Sinon, on ne sait pas conclure.

Des tresses aux nœuds

A partir d'une tresse on peut construire un entrelacs (ou un nœud) en reliant les bouts de la tresse entre eux comme dans la figure 16. Un tel entrelacs s'appelle une *tresse fermée*. Alexander [**Ale-23**] (encore lui) a démontré que tout entrelacs peut être obtenu de la sorte. Faites l'essai avec les exemples des figures 14 et 15. Plus tard Markov [**Mar-45**] découvrit un algorithme partiel qui, étant données deux tresses, détermine si elles ont la même fermeture

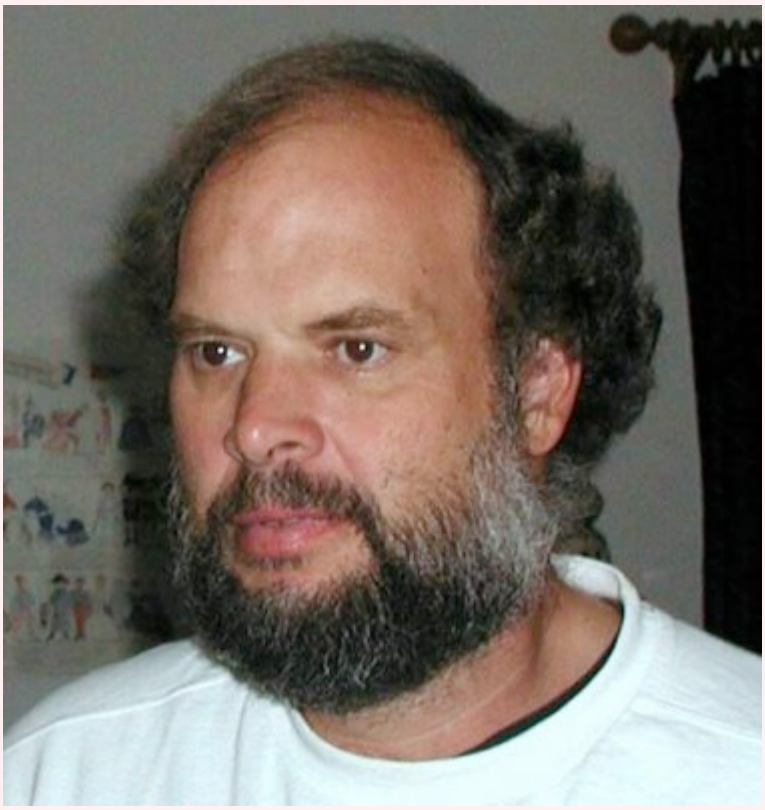
(mais ne répond pas sinon). Ces deux résultats sont cruciaux dans l'application de la théorie des tresses aux nœuds. En particulier ils sont à l'origine d'un profond renouveau dans la théorie des nœuds dans les années 80 avec les travaux de Jones [**Jon-85**] [**Jon-87**] et ses invariants définis à partir de la théorie des tresses.





James W. Alexander (1888 -1971) fut un mathématicien américain célèbre. L'un des premiers membres de l'Institut for Advanced Study (1933-1951), il fut également professeur à l'Université de Princeton (1920-1951). C'est des pionniers de la topologie algébrique et de la théorie des nœuds. C'était aussi un grand alpiniste, ayant réussi de nombreuses ascensions

importantes. Vers la fin de sa vie il est devenu solitaire et reclus. Il était connu comme socialiste actif et sa renommée attira l'attention des MacCarthistes. Il n'a pas été revu en public depuis 1954 après qu'il ait signé une lettre de soutien à Robert Oppenheimer.



Vaughan F.R. Jones (né le 31 décembre 1952) est un mathématicien néo-zélandais connu pour ses travaux sur les algèbres de von Neumann, les invariants des nœuds et la théorie conforme des champs. Il a reçu la médaille Fields en 1990 et est actuellement professeur à l'Université de Californie à Berkeley. Ses travaux sur les invariants des nœuds ont conduit à des solutions inattendues de plusieurs problèmes classiques de la théorie des nœuds et de la topologie de basse dimension.

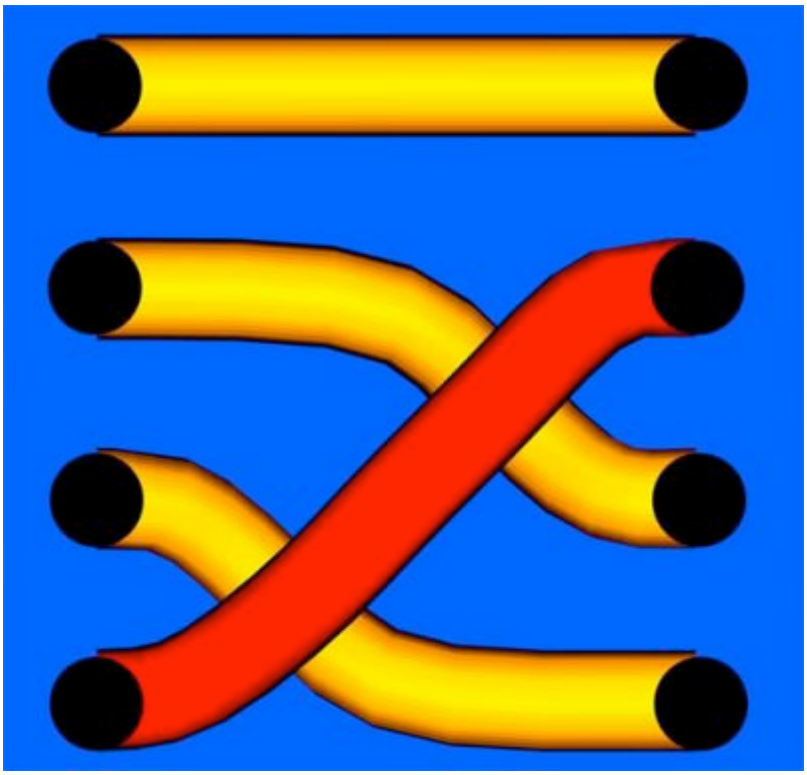
Comment distinguer deux tresses

Contrairement aux nœuds, il existe des algorithmes qui, étant donnés deux dessins de tresses, déterminent si ceux-ci représentent la même tresse ou non. Plusieurs de ces algorithmes sont très rapides et sont implémentés dans différents logiciels de calcul tels que GAP ou MAGMA. L'existence de ces algorithmes est liée au fait que les tresses sont non seulement des objets topologiques, mais aussi des *objets algébriques* puisque, comme on l'a vu, on peut leur appliquer la composition (juxtaposition). Voici une façon de décider si deux tresses sont égales. Ce procédé était probablement déjà connu d'Artin en 1925.

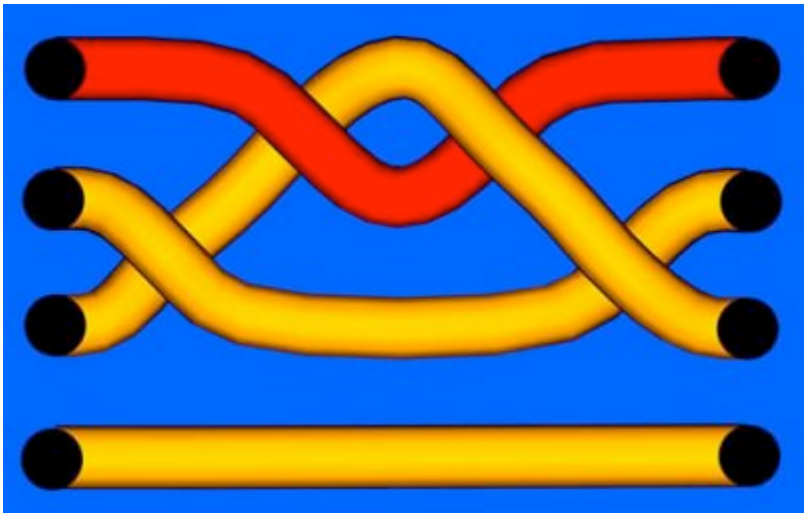
On se donne deux (dessins de) tresses α et β.

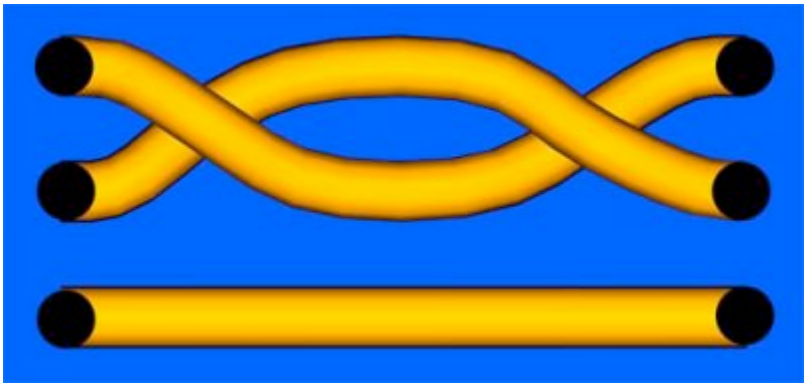
Etape 1 : On note $\tilde{\beta}$ la tresse miroir de β. On peut observer que α et β représentent la même tresse si et seulement si la composée $\alpha\tilde{\beta}$ représente la tresse triviale. On pose $\gamma = \alpha\tilde{\beta}$. Notre problème se ramène maintenant à déterminer si γ est la tresse triviale ou non.

Etape 2 : Pour que γ soit la tresse triviale, il faut que le brin issu du premier clou à gauche aille au premier clou à droite, le brin issu du second clou à gauche aille au second clou à droite, etc. On vérifie que c'est le cas pour γ. Si ce n'est pas le cas, γ n'est pas triviale. Par exemple, la tresse γ de la figure 17 n'est pas triviale car le brin issu du premier clou à gauche arrive sur le troisième clou à droite. Sinon, on passe à l'étape 3.

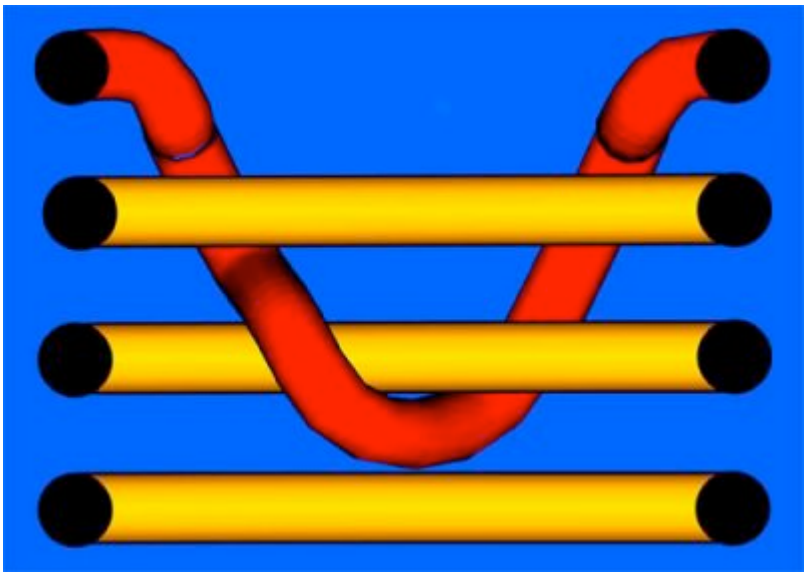


Etape 3 : si l'on enlève le quatrième brin à γ on obtient une tresse à trois brins que l'on note γ'. Ceci a un sens car ce brin relie le quatrième clou de gauche au quatrième clou de droite. On suppose que l'on sait déjà distinguer deux tresses à trois brins. Une condition nécessaire pour que γ soit triviale est que γ' soit aussi triviale. Par exemple, la tresse γ de la figure 18 n'est pas triviale car γ' ne l'est pas. Si γ' est triviale, on passe à l'étape 4.





Etape 4 : A cette étape les trois premiers brins de notre tresse sont des segments droits alors que le quatrième brin s'enlace autour des trois autres, comme dans la figure 19. Là il faut utiliser des outils mathématiques plus sophistiqués, mais le lecteur retiendra que l'on sait traiter ce cas sans trop de difficultés mais avec des outils un peu longs à expliquer.



Des tresses à l'algorithmique

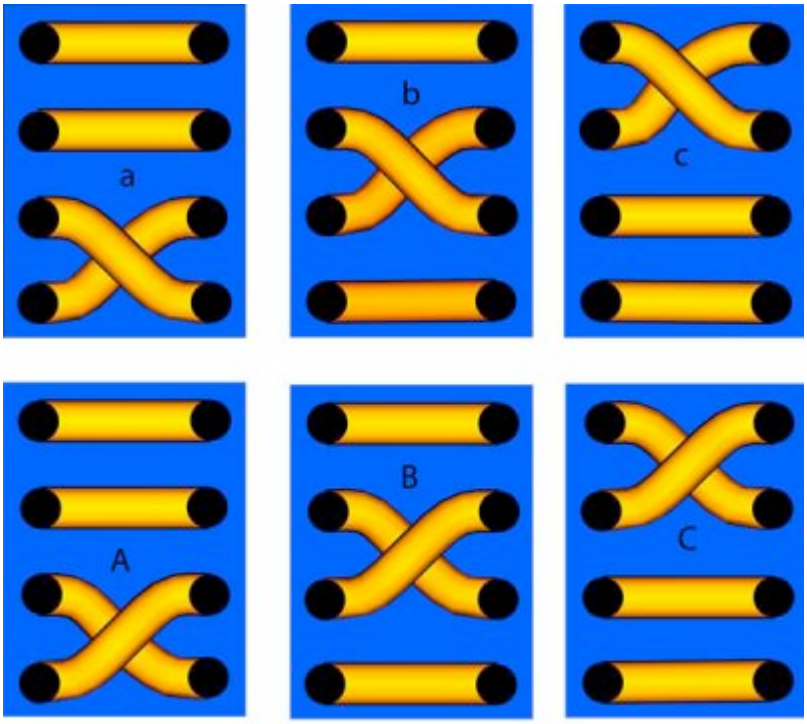
Algorithmes et langages

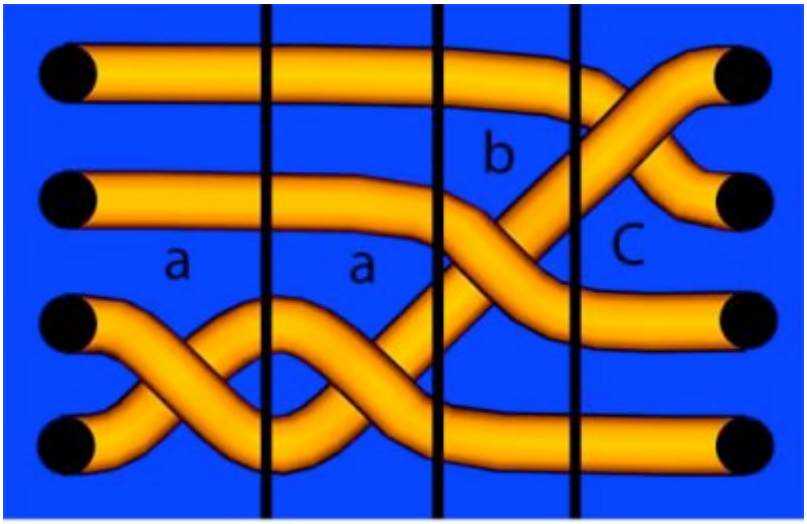
Si vous expliquez à votre ami Jacques un chemin pour qu'il se rende chez vous, vous fabriquez (et faites exécuter) un algorithme. Un *algorithme* est une suite d'instructions (mathématiques ou autres) bien définies pour remplir une tâche. Si l'algorithme est juste, le résultat sera le résultat voulu et Jacques trouvera son chemin. Si l'algorithme est faux, le résultat est imprévisible. En informatique, l'algorithme donne la méthode et la programmation la met sous forme d'instructions pour la machine.

Une notion importante en algorithmique (étude des algorithmes) est la notion de mot et de langage. Pour un algorithmicien, un *alphabet* est un ensemble fini dont les éléments s'appellent lettres, un *mot* est une suite finie de lettres et un langage un ensemble de mots. Par exemple, l'ensemble $\mathcal{A} = \{a, b\}$ est un alphabet, les suites $b, ab, aab, aaab$ sont des mots et l'ensemble $\{b, ab, aab, aaab, aaaab, ...\}$ est un langage. Autre exemple : L'ADN. C'est l'algorithme à la base de la construction d'un être vivant. C'est une chaîne construite à partir de quatre éléments : l'adénine (notée A), la thymine (notée T), la cytosine (notée C) et la guanine (notée G). C'est le nombre de ces éléments ainsi que l'ordre dans lequel ils sont arrangés qui vont déterminer si on obtient un moustique ou un lion. Bref : un mot en l'alphabet $\{A, T, C, G\}$ représente un algorithme qui produit un être vivant et l'ensemble des êtres vivants peut être vu comme un langage en l'alphabet $\{A, T, C, G\}$. C'est le début de la modélisation en génétique.

Des tresses aux mots

On peut représenter les tresses à l'aide de mots sans utiliser de support graphique. L'alphabet que nous considérons est $\mathcal{A} = \{a, b, c, A, B, C\}$. Chaque lettre de notre alphabet correspond à une tresse « élémentaire » comme dans la figure 20. Etant donnée une tresse α, il est facile de voir, en découpant α en petites tranches verticales, que α est la composée de tresses élémentaires. En d'autres termes, α s'écrit comme un mot en l'alphabet $\mathcal{A}$. Par exemple, la tresse de la figure 21 est égale à $aabC$.





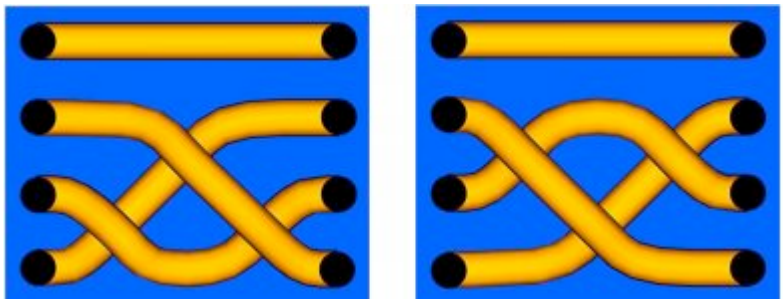
En fait, le groupe des tresses est caractérisé par les deux propriétés suivantes :

1. toute tresse s'écrit comme un mot en l'alphabet $\mathcal{A} = \{a, b, c, A, B, C\}$;

2. on a les égalités

$$aA = Aa = \epsilon, \quad bB = Bb = \epsilon, \quad cC = Cc = \epsilon, \quad aba = bab, \quad ac = ca, \quad bcb = cbc$$

où ϵ désigne le *mot vide*, c'est-à-dire un mot de longueur 0 qui n'a pas de lettre. L'égalité $aba = baba$ est illustrée dans la figure 22.



Problème des mots et problème des conjugueurs

Il existe un algorithme qui, étant donnés deux mots en l'alphabet $\mathcal{A} = \{a, b, c, A, B, C\}$, décident si ceux-ci représentent la même tresse ou non. Un tel algorithme est appelé *solution au problème des mots*. Le lecteur remarquera que ce problème est sensiblement le même que celui évoqué antérieurement à savoir : quand est-ce que deux dessins de tresses représentent la même tresse.

Voici un autre problème d'algorithmique que l'on sait résoudre sur les tresses. Si l'on se donne deux tresses α et β, on sait dire s'il existe une tresse γ telle que $\alpha\gamma = \gamma\beta$, et, en cas de réponse affirmative, on sait trouver tous les γ. Le lecteur attentif se sera rendu compte que ceci revient à résoudre l'équation $\alpha X = X\beta$. Je rappelle que, par résoudre l'équation $\alpha X = X\beta$, on entend trouver l'ensemble des X qui vérifient cette égalité. S'il n'y en a pas, cet ensemble est vide. Un algorithme qui, étant donné α et β, résout l'équation $\alpha X = X\beta$, s'appelle une solution au problème des conjugueurs.

Problèmes de décidabilité

Le problème des mots et le problème des conjugueurs font partie d'une famille de problèmes mathématiques, très proches de l'algorithmique et de l'informatique, connus sous le nom de « problèmes de décidabilité ». Ceux-ci connaissent un regain d'intérêt non seulement à travers leurs applications dans d'autres domaines, mais encore car la notion même de démonstration mathématique est en train de changer. En effet, on distingue maintenant la notion de démonstration de la notion de démonstration effective, celle qui construit la solution. Une telle construction se fait avec un algorithme et sa complexité (temps de calcul) est une donnée qui doit être calculée, eu égard à l'informaticien qui souhaiterait utiliser un tel outil.

Résultat mathématique dont la construction ne se fait pas avec un algorithme

Un exemple de résultat dont la démonstration n'est pas effective est le théorème suivant connu sous le nom du *théorème du sandwich* (voir la figure 23).

Théorème : *Etant donné un sandwich formé de pain, de jambon et de fromage, il existe une coupe équitable de ce sandwich avec la même quantité de pain, de jambon et de fromage de chaque côté.*

On sait qu'une telle coupe existe mais on ne sait pas la trouver. Contrairement aux apparences, la théorie qui conduit à ce théorème est loin d'être inutile (le théorème du sandwich est juste une illustration). Par exemple, c'est avec ces mêmes techniques que les mathématiciens ont établi l'existence d'enzymes appelées topo-isomérases qui effectuent des manipulations topologiques sur l'ADN.

Problèmes de décidabilité dans les tresses

L'algorithmique dans les groupes de tresses est spécialement active. Des problèmes de décidabilité, tels que le problème des mots ou le problème des conjugueurs, ont été résolus par Garside [**Gar-69**] en 1969. Très peu de progrès ont été faits jusqu'à la parution du livre [**Eps-92**] où sont décrits des algorithmes provenant de la théorie des automates pour résoudre des problèmes de décidabilité dans les groupes de tresses.

Frank A. Garside était directeur d'une école de garçons lorsqu'il a commencé sa thèse de doctorat à Oxford en 1968. Ayant un emploi à temps plein, il savait qu'il allait travailler lentement et choisit un sujet loin des courants dominants de l'époque : il entreprit de résoudre le problème de conjugaison dans les groupes des tresses. Il découvrit une structure alors inconnue qui a depuis eu de nombreuses applications et des généralisations qui vont au-delà de son sujet de thèse. Bien que la contribution de Garside soit la source d'un domaine de recherche encore très actif de nos jours, il n'a publié qu'un seul article dans sa vie.

Dans [**DehPar-99**] est introduit un cadre plus formel et plus général pour étudier des problèmes de décidabilité dans les groupes de tresses : les groupes de Garside. L'idée de départ est d'isoler certaines propriétés combinatoires des groupes de tresses : disons créer un modèle moins contraignant n'utilisant que des outils issus de la théorie du langage (monoïdes, réécritures) et de la combinatoire (ensembles ordonnés), domaines spécialement adaptés pour traiter des

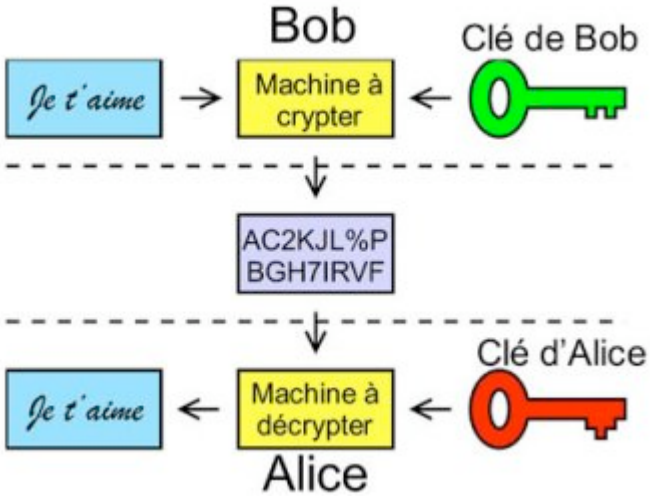
problèmes d'algorithmique. Sous l'impulsion des écoles française, américaine, coréenne et israélienne, de grands progrès ont été faits pour comprendre ces structures et des applications ont vu le jour, en particulier en cryptographie.

Des tresses à la cryptographie

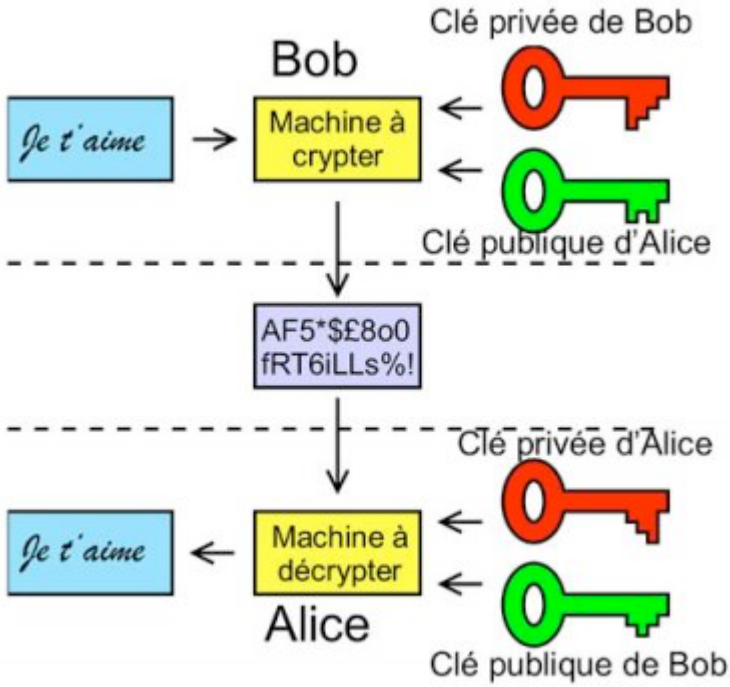
La cryptographie

La *cryptographie* est l'étude et l'utilisation de moyens pour envoyer des informations ou messages confidentiels à travers des canaux de communications publics. Elle est considérée comme une branche des mathématiques, de l'informatique et des sciences de la communication, et a de très nombreuses applications, par exemple dans la sécurisation des cartes bancaires, dans le commerce électronique ou bien dans l'authentification des téléphones portables.

Un *système de cryptage*, ou crypto-système, consiste en la donnée de deux algorithmes. Le premier algorithme est utilisé par l'envoyeur (toujours appelé Bob en cryptographie) pour crypter le message qu'il veut envoyer. Le second algorithme est utilisé par le receveur (en fait c'est une fille et elle s'appelle Alice) pour décrypter le message. Bob doit introduire dans sa machine (c'est la même pour tous) le message et une clé (la clé est en général un mot que seuls Bob et Alice connaissent) (voir la figure 24). Le baragouin inintelligible qui en sortira dépendra de ces deux paramètres. De même Alice doit introduire dans sa machine le message reçu et une autre clé (que, là encore, seuls Alice et Bob connaissent) pour lire le message. La sécurité du système dépend de la capacité qu'ont Alice et Bob de garder leurs clés secrètes.



Dans certains systèmes de cryptage récents, tels que RSA, connus sous le nom de crypto-systèmes à clé publique ou crypto-systèmes asymétriques, l'utilisateur possède deux clés : une clé publique et une clé privée. La clé privée est gardée secrète, alors que la clé publique peut être largement diffusée. Les clés sont liées entre elles, mais il ne faut pas que l'on puisse déduire la clé privée à partir de la clé publique. Dans un tel système, la machine de Bob utilisera la clé privée de Bob et la clé publique d'Alice pour crypter le message, et la machine d'Alice utilisera la clé privée d'Alice et la clé publique de Bob pour le décrypter (voir la figure 25).



Crypto-systèmes basés sur les tresses

C'est dans le cadre des groupes de tresses et des groupes de Garside que les premiers systèmes de cryptage basés sur des structures non commutatives ont vu le jour (voir [**AAG-99**] et [**KoAl-00**]). L'existence d'algorithmes rapides pour le problème des mots, la complexité importante des algorithmes pour le problème des conjugueurs, et la bonne compréhension de ces groupes en font des bons candidats. Par contre, l'utilisation de tels algorithmes demanderait des efforts technologiques et de formation trop importants pour qu'ils soient à courte échéance utilisés par l'industrie ou l'armée.

Dans le système de cryptage proposé dans [**KoAl-00**] la clé privée d'Alice est la donnée de deux tresses, γ_1 et γ_2, et sa clé publique est une troisième tresse α accompagnée de la composition $\gamma_1\alpha\gamma_2$. Pour que ce système soit fiable, il faut qu'il n'y ait pas d'algorithme rapide pour résoudre l'équation $X\alpha Y = \beta$, où α et β sont des tresses données, et X et Y sont des variables. Des études récentes [**BGGa-08**], [**BGGb-08**], [**BGGc-08**] sur les groupes de tresses montrent que l'on peut résoudre rapidement de telles équations pour « presque tous » les α et β, ce qui rend le crypto-système peu fiable. Néanmoins, des variantes avec d'autres groupes (de Garside) sont maintenant à l'étude et rien n'est encore vraiment démontré. C'est un thème de recherche très actif en ce moment.

Références

J.W. Alexander. *Deformations of an n-cell*. Proc. Nat. Acad. Sci. USA 9 (1923), 406-407.

J. W. Alexander, G. B. Briggs. *On types of knotted curves*. Ann. of Math. (2) 28 (1926/27), no. 1-4, 562-586.

I. Anshel, M. Anshel, D. Goldfeld. *An algebraic method for public-key cryptography*. Math. Res. Lett. 6 (1999), no. 3-4, 287-291.

E. Artin. *Theorie de Zöpfe*. Abhandlungen Hamburg 4 (1925), 47-72.

J.S. Birman, V. Gebhardt, J. González-Meneses. *Conjugacy in Garside groups I : cyclings, powers, and rigidity*. Groups Geom. Dyn. 1 (2007), no. 3, 221-279.

J.S. Birman, V. Gebhardt, J. González-Meneses. *Conjugacy in Garside groups II : Structure of the ultra summit set*. Groups Geom. Dyn. 2 (2008), no. 1, 13-61.

J.S. Birman, V. Gebhardt, J. González-Meneses. *Conjugacy in Garside groups III : Periodic braids*. J. Algebra 316 (2007), no. 2, 746-776. [Deh-04] P. Dehornoy. Braid-based cryptography. Group theory, statistics, and cryptography, 5-33, Contemp. Math., 360, Amer. Math. Soc., Providence, RI, 2004.

P. Dehornoy, L. Paris. *Gaussian groups and Garside groups, two generalisations of Artin groups*. Proc. London Math. Soc. (3) 79 (1999), no. 3, 569-604.

D.B.A. Epstein, J.W. Cannon, D.F. Holt, S.V.T. Levy, M.S. Paterson, W.P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992.

F.A. Garside. *The braid group and other groups*. Quart. J. Math. Oxford Ser. (2) 20 (1969), 235-254.

V.F.R. Jones. *A polynomial invariant for knots via von Neumann algebras*. Bull. Amer. Math. Soc. (N.S.) 12 (1985), no. 1, 103-111.

V.F.R. Jones. *Hecke algebra representations of braid groups and link polynomials*. Ann. of Math. (2) 126 (1987), no. 2, 335-388.

K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.-S. Kang, C. Park. *New public-key cryptosystem using braid groups*. Advances in cryptology-CRYPTO 2000 (Santa Barbara, CA), 166-183, Lecture Notes in Comput. Sci., 1880, Springer, Berlin, 2000.

A. Markoff. *Fundations of the algebraic theory of tresses*. Trav. Inst. Math. Stekloff 16 (1945).

K. Reidemeister. *Elementare Begründang der Knotentheorie*. Abh. Math. Sem. Univ. Hamburg 5 (1926), 24-32.

Notes

[▲1] http://www.birs.ca/birspages.php?task=displayevent&event_id=07w5104

Crédits images

Pour citer cet article : **Luis Paris**, **Les tresses : de la topologie à la cryptographie**. *Images des Mathématiques*, CNRS, 2009. En ligne, URL : **http://images.math.cnrs.fr/Les-tresses-de-la-topologie-a-la.html**