

---

## DES TRESSES, DES ELEVES

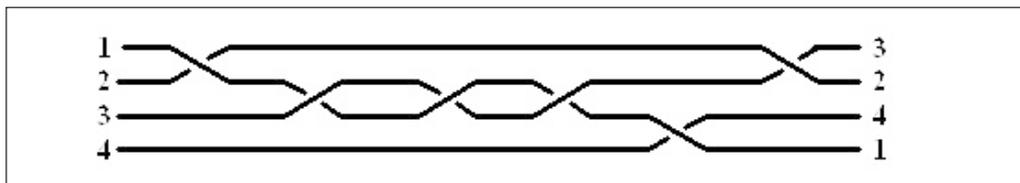
---

Francis JAMM  
Irem de Strasbourg

Le nœud gordien a pour fils les entrelacs celtiques et pour filles les tresses.

Si ces dernières comptaient conserver leurs secrets, elles doivent être bien désappointées. Car c'était sans compter avec la sagacité d'un groupe d'élèves, qui, dans le cadre d'un club scientifique en TS, a entrepris d'en percer les mystères.

Une tresse, ce sont des brins qui se croisent. Par exemple :



Sans déflorer le sujet, mais pour donner un fil d'Ariane, disons tout de suite que les tresses à  $n$  brins forment un ensemble quotient qui peut être muni d'une structure de groupe, non abélien, défini par générateurs et relations. C'est la découverte de ces notions par les élèves que relate cet article.

### LES DEBUTS

A la première séance, j'apporte des bouts de grosse laine aux couleurs vives. Les élèves

\* Cet article est paru dans l'OUVERT :  
<http://irem.u-strasbg.fr/irem/structure/frameouvline.html>

voient tout de suite que l'opération élémentaire est le croisement de deux brins adjacents, avec deux cas possibles, par au-dessus et par en dessous. Ensuite par concaténation de tels croisements on obtient une tresse.



Rapidement ils constatent que certaines tresses ne sont pas tressées du tout ! Une tresse est réellement tressée si, en tirant sur les brins, sans modifier leur ordre aux extrémités, on n'obtient pas des brins parallèles. Un exemple trivial de tresse non réellement tressée est :



D'emblée, une élève dit : « Si on appelle le premier croisement 1 et le second -1, alors c'est comme  $1 - 1 = 0$  ». Ils appellent une telle tresse une *tresse nulle*. Là, je sens que c'est bien parti pour explorer les groupes de tresses.

Dans la foulée les élèves décident que deux tresses qui diffèrent seulement par de tels croisements, donc par des tresses nulles, seront déclarées égales (ci-dessous). Il s'agit en fait de l'*isotopie* des tresses qui est une relation d'équivalence.

Pour s'en convaincre on réalise deux telles tresses, puis on tire sur les brins, sans modifier leur ordre en bout de tresse, et on constate que l'on obtient alors deux tresses identiques. Ils appellent *vraie tresse* une tresse débarrassée de ces croisements inutiles ; donc une classe d'équivalence pour l'isotopie.

Ils décident de noter  $T_{i, i+1}$  le croisement où le brin  $i$  passe au dessus du brin  $i+1$  ; et  $\bar{T}_{i, i+1}$  le croisement où le brin  $i$  passe en dessous du brin  $i+1$  :

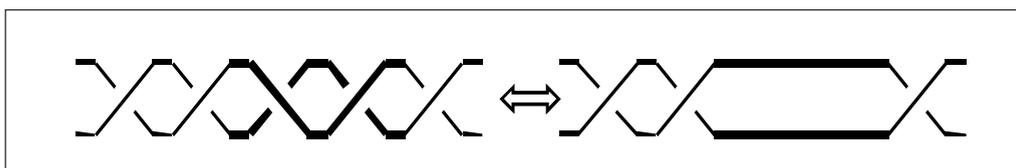
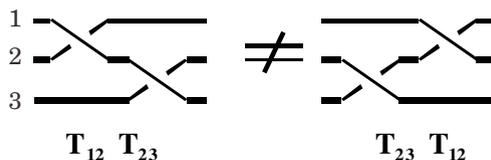


Il est clair que :

$$T_{i, i+1} \bar{T}_{i, i+1} = \bar{T}_{i, i+1} T_{i, i+1} = 0.$$

Une vraie tresse est définie par une formule du genre  $T_{12} \bar{T}_{23} \bar{T}_{23} T_{23} T_{34} T_{12}$  (voir le premier dessin)

Ils constatent vite que  $T_{12} T_{23}$  est différent de  $T_{23} T_{12}$ . Tout simplement car l'ordre des brins à l'arrivée n'est pas le même. Et voilà pour la non commutativité ; mais nous y reviendrons.



**L'INVERSE D'UNE TRESSE**

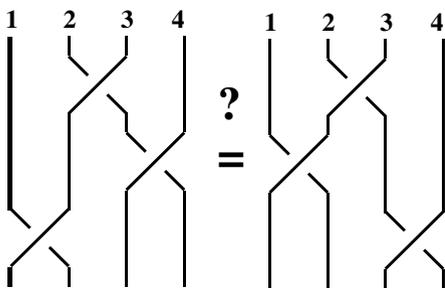
Ils construisent alors  $T_{12}T_{34}T_{23} \bar{T}_{23} \bar{T}_{34} \bar{T}_{12}$  qui est la tresse nulle, découvrant ainsi que  $(ab)^{-1} = b^{-1}a^{-1}$ .

Ils appellent  $\bar{T}_{23} \bar{T}_{34} \bar{T}_{12}$  la *tresse inverse* de  $T_{12}T_{34}T_{23}$ . Oui, je sais, ils mélangent un peu le vocabulaire des lois additives et multiplicatives. Toute tresse admet donc un inverse ; et ils ont un procédé pour le construire.

Constatant la symétrie de cette tresse nulle ainsi obtenue ; ils se posent alors la question de savoir si toute tresse nulle admet un axe de symétrie.

Ils découvrent alors que l'on a aussi  $T_{12}T_{34}T_{23} \bar{T}_{23} \bar{T}_{12} \bar{T}_{34} = 0$ . Comment font-ils ? Mais tout simplement ils réalisent la tresse, puis tirent sur les brins et obtiennent des brins parallèles, donc la tresse nulle. Doit-on en déduire que l'on a :

$$\bar{T}_{23} \bar{T}_{34} \bar{T}_{12} = \bar{T}_{23} \bar{T}_{12} \bar{T}_{34} ?$$



Visuellement la réponse est oui, car on passe de l'une à l'autre en faisant glisser les croisements sans en créer de nouveaux.

Plus rigoureusement ils décident de dire

que  $T = T'$  si et seulement si  $T \bar{T}' = 0$ . Ici on a donc :

$$\bar{T}_{23} \bar{T}_{34} \bar{T}_{12} (\bar{T}_{23} \bar{T}_{12} \bar{T}_{34})^{-1} = \bar{T}_{23} \bar{T}_{34} \bar{T}_{12} T_{34}T_{12}T_{23} .$$

Quand on réalise cette tresse, et que l'on tire sur les brins on aboutit à la tresse nulle. Donc, par glissement des brins, on peut permuter deux croisements, pourvu qu'ils portent sur des brins distincts . C'est-à-dire :

$$T_{i, i+1} T_{k, k+1} = T_{k, k+1} T_{i, i+1} \text{ ssi } | i - k | \geq 2.$$

Et voilà pour la deuxième relation.

Toute tresse admet une tresse inverse. Mais est-elle unique ? Ils chercheront un bon moment avant de se lasser. Plus tard je ferai un topo sur les groupes et leur démontrerai l'unicité de l'élément réciproque dans tout groupe. Pour le moment ils concluent, joliment, qu'il existe une tresse inverse mais « écrivable » de plusieurs façons.

**DENOMBREMENT DES TRESSSES**

*Tresses à deux croisements*

A ce stade ils se posent la question de savoir combien il existe de vraies tresses à  $n$  brins et  $p$  croisements.

Avec  $n$  brins et un croisement, il existe  $2(n-1)$  cas, à savoir  $T_{12}$  jusqu'à  $T_{n-1,n}$  et leurs inverses.

Pour les tresses à deux brins, et  $p$  croisements, il n'y a que deux cas  $T_{12} \dots T_{12}$  ( $p$  fois) et son inverse.

DES TRESSSES,  
DES ELEVES

Avec 3 brins et 2 croisements on a 12 cas, hormis la tresse nulle.

Dans cette activité, mon principal rôle est de tenir la craie et de coucher sur le tableau les idées des élèves. Je trouve leur notation  $T_{i, i+1}$  lourde et leur propose de noter  $T_{12}$  par  $a$ ,  $T_{23}$  par  $b$  et par  $A$  et  $B$  leurs inverses.

Les 12 cas s'écrivent alors :

aa    ab    aB    AA    Ab    AB  
ba    bA    bb    Ba    BA    BB

Par une disposition astucieuse des différents cas ; ils montrent, de proche en proche, que pour les tresses à deux croisements il y a, hormis la tresse nulle, 26 cas pour 4 brins, 44 pour 5 brins et 66 pour 6 brins.

Les élèves sont allés jusqu'aux tresses à 6 brins. La séance suivante, ils ont montré qu'il existe  $2n^2 - 6$  tresses à  $n$  brins et deux croisements, hormis la tresse nulle .

Voici comment ils ont procédé. Il faut dire à leur décharge, qu'ils ne connaissaient ni les dénombrements ni le raisonnement par récurrence ; mais ils auraient pu avoir l'idée d'un tableau.

On note  $t_i$  le croisement du  $i$ ème brin sur le suivant et  $T_i$  sont inverse. Avec  $n$  brins il existe  $2n - 2$  croisements possibles,  $i$  variant de 1 à  $n - 1$  .

Il y a  $(2n - 2)^2$  couples possibles  
(sans aucune condition)  
On ôte  $2n - 2$  cas  $t_i T_i$  ou  $T_i t_i$  qui donne la tresse nulle

Avec 3 brins

1er croisement	2ème croisement	1er croisement	2ème croisement
a	a, b, B	A	A, b, B
b	a, A, b	B	a, A, B

On retrouve les 12 cas précités.

Avec 4 brins : On note « c » le croisement du troisième brin sur le quatrième et « C » sont inverse. « a » et « c » portant sur des brins indépendants il faut éliminer les doublons : ac, aC, Ac et AC.

1er croisement	2ème croisement	1er croisement	2ème croisement
a	a, b, B + c	A	A, b, B + C
b	a, A, b, c, C + d	B	a, A, B, c, C + D
c	A, b, B, C	C	A, b, B, C

On retrouve les 26 cas.

Avec 5 brins

On note « d » le croisement du quatrième brin sur le cinquième et « D » son inverse. Il faut éviter les doublons portant sur des brins non adjacents, donc sur des lettres non consécutives.

1er croisement	2ème croisement	1er croisement	2ème croisement
a	a, b, B, c + d	A	A, b, B, C + D
b	a, A, b, c, C + d	B	a, A, B, c, C + D
c	A, b, B, C + d, D	C	A, b, B, C + d, D
d	a, B, c, C, d	D	a, b, c, C, D

On retrouve les 44 cas.

On ôte  $2n - 2$  cas  $t_i t_j$  ou  $T_i T_j$   
 Il reste  $(2n - 2)^2 - 2(2n - 2)$  cas qui correspondent à  $i$  différent de  $j$   
 On divise par 2  $2(n - 1)^2 - (n - 1)$  cas qui correspondent à  $i < j$   
 On ajoute  $2n - 2$  on remet les cas  $t_i t_j$  et  $T_i T_j$   
 Il reste  $2(n - 1)^2$  cas qui correspondent à  $i \leq j$   
 On ajoute  $4(n - 2)$  cas qui correspondent aux croisement :  $t_{i+1} t_i, t_{i+1} T_i, T_{i+1} t_i, T_{i+1} T_i$  (donc non commutatifs) avec  $i > j$   
 On obtient  $2n^2 - 6$ .

*Tresses à trois croisements*

Pour 3 brins et 3 croisements on ajoute  $a, b, A$  ou  $B$  à droite des cas à deux croisements en évitant de former une sous-tresse nulle. On trouve :

aaa	baa	Baa	<b>aba</b>	bba	Aba
<b>aBa</b>	ABa	BBa	aab	<b>bab</b>	Bab
<b>bAb</b>	BAb	Aab	abb	bbb	Abb
bAA	BAA	AAA	abA	bbA	<b>AbA</b>
aBA	<b>ABA</b>	BBA	aaB	baB	<b>BaB</b>
bAB	<b>BAB</b>	AAb	aBB	ABB	BBB

**LA TROISIEME RELATION**

Les cas en caractères gras posent problème. Examinons-les de plus près : peut-on affirmer que  $aba = bab$  ?

Les avis sont partagés quant à l'égalité de ces deux tresses. Pour en décider construisons  $abaBAB$  (cf. figures ci-dessous) : en tirant sur les brins on obtient la tresse nulle.

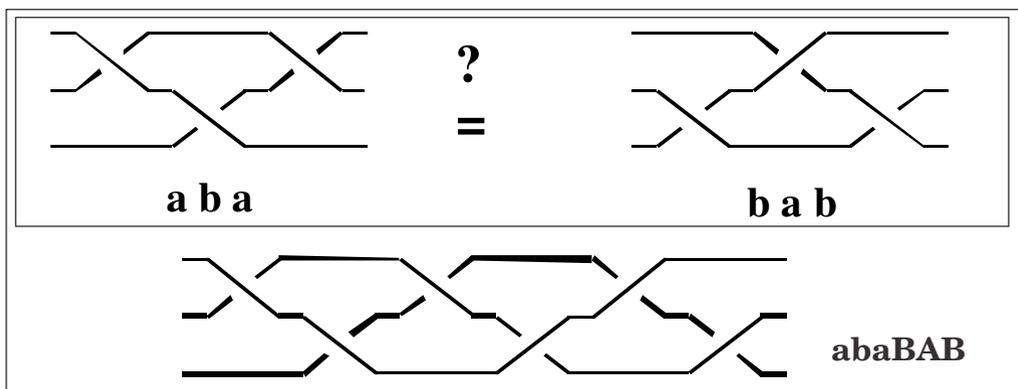
On a donc bien  $aba = bab$ .

Et voilà la troisième relation.

Arrivé à ce stade le dénombrement devient problématique à cause des cas d'égalité qu'engendre cette relation. Après six semaines de travail les élèves décident de faire une pause. Je termine en faisant un topo sur les groupes et en plaçant ce qu'ils ont trouvé dans ce cadre.

**LE GROUPE DES TRESSSES**

Les tresses, physiques, sont des objets tridimensionnels que l'on représente par des diagrammes plans. Ces diagrammes sont codés par les croisements élémentaires



$\sigma_1^{\pm 1}, \sigma_2^{\pm 1} \dots \sigma_{n-1}^{\pm 1}$ , où  $\sigma_i^1$  représente le croisement du  $i$ ème brin sur le  $i+1$ ème et  $\sigma_i^{-1}$  le même croisement dans l'autre sens.

Une tresse à  $n$  brins est représentée par la concaténation de tels croisements, on parle de mots de tresses. L'ensemble des diagrammes à  $n$  brins, muni de l'opération de concaténation, a une structure de monoïde. En effet il n'y a pas unicité de l'inverse.

L'isotopie des diagrammes est une relation d'équivalence compatible avec la concaténation et induit donc une opération sur les classes. Des mots différents peuvent coder la même tresse ; par exemple  $\sigma_1 \sigma_3$  et  $\sigma_3 \sigma_1$ .

On a les relations suivantes, avec  $\cong$  pour l'isotopie et  $\varepsilon$  pour le mot vide.

$$\left\{ \begin{array}{l} \forall (i, j) \in [1, n-1] \left\{ \begin{array}{l} |i-j|=1 \Rightarrow \sigma_i \sigma_j \sigma_i \cong \sigma_j \sigma_i \sigma_j \\ |i-j|>1 \Rightarrow \sigma_i \sigma_j \cong \sigma_j \sigma_i \end{array} \right. \\ \forall (i, j) \in [1, n-1] \sigma_i \sigma_i^{-1} \cong \sigma_i^{-1} \sigma_i \cong \varepsilon \end{array} \right.$$

En passant au quotient on obtient le groupe des tresses à  $n$  brins, qui est noté  $B_n$ .

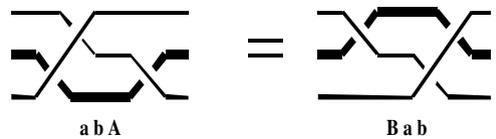
Que deux tresses sont isotopes ssi on peut passer de l'une à l'autre à l'aide des relations ci-dessus a été démontré par Artin. Les tresses à deux brins ont une structure isomorphe à  $(\mathbb{Z}, +)$ .

De tout ce jargon, un peu impressionnant pour eux, ils voient des liens avec des choses connues, comme la relation de congruence. Ils passent une séance à jouer les Monsieur Jourdain en découvrant qu'ils connaissaient, sans le savoir, plein de groupes et d'ensembles quotients. J'en profite pour leur montrer des

groupes finis isomorphes ou non. Je fus impressionné quand une élève me déclara : « Oui, c'est comme avec le log entre  $(\mathbb{R}_+, \times)$  et  $(\mathbb{R}, +)$  ».

### LA REDUCTION DES TRESSES

Les élèves constatent que  $abA$  est isotope à  $Bab$  ; en effet il suffit de tirer sur le brin en gras sans créer de nouveau croisement. Dans le jargon des tresses on parle de poignée :



Ils pensent avoir trouvé une nouvelle relation. Je leur explique que toute nouvelle « formule » doit découler des relations qui définissent le groupe des tresses. Et c'est la découverte de ce que peut être le calcul algébrique :

$$abA = BbabA = BabaA = Bab$$

De la même manière on a :

$$aBA = BAb, Aba = baB \text{ et } Aba = bAB$$

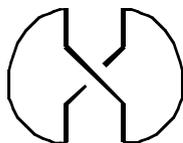
Par exemple la tresse  $ABAbab$  est clairement isotope à la tresse nulle si on fait le dessin. On le retrouve avec :

$$ABAbab = AaBAab = Bb = 0$$

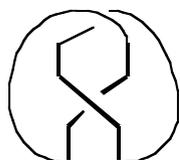
### ET LES NŒUDS ?

Dans un deuxième temps les élèves se sont essayés aux noeuds. En effet quand on noue les brins d'une tresse on obtient un noeud. La première difficulté est de savoir comment

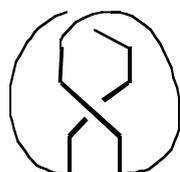
noyer une tresse. Avec la tresse la plus simple il y a déjà trois possibilités :



Qui donne un cercle.



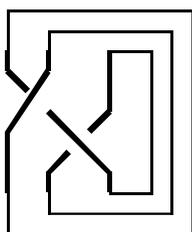
Qui donne deux cercles enlacés



Qui donne deux cercles disjoints

C'est la première méthode qui semble devoir être retenue puisqu'elle n'introduit pas de croisement supplémentaire.

La question est de savoir si deux tresses non isotopes donnent toujours des noeuds différents. La réponse est non. L'exemple suivant donne aussi un noeud réduit à un cercle :



Nous ne sommes pas allé plus loin ; entre autres, car il était difficile et long de réaliser des noeuds à partir de tresses

## CRYPTOGRAPHIE

A la fin de cette étude, que les élèves ont menée pour elle-même, ils se sont posé la question des applications possibles. Comme ils avaient vu le système RSA en arithmétique je leur ai montré que les tresses pouvaient servir en cryptographie.

Soit  $p$  une clé publique dans le groupe des tresses à  $2n$  brins que Alice et Bob décident d'utiliser.

Alice choisit la tresse  $a$  qui porte sur les brins de 1 à  $n$  et envoie à Bob  $p_A = ap_A$ . Bob choisit la tresse  $b$  qui porte sur les brins  $n+1$  à  $2n$  et envoie à Alice  $p_B = bp_B$ .

Alors on a  $ab = ba$  car ils portent sur deux groupes de brins disjoints. Maintenant Alice et Bob calculent leur clé commune, et secrète,  $s$ . Alice calcule  $a p_B A$  et Bob calcule  $b p_A B$ . Le noeud de l'affaire est que :

$$a p_B A = abp_BA = bap_AB = bp_AB$$

Ils ont maintenant un clé commune

$$s = a p_B A = b p_A B.$$

Tirer  $a$  ou  $b$  de  $(p, ap_A)$  ou de  $(p, bp_B)$  est très difficile.

Soit  $M$  le message à envoyer . On envoie  $sMs^{-1}$  qu'il suffit de décoder avec  $s^{-1}sM s^{-1}s = M$ .

## PERSPECTIVES ET CONCLUSION

Partis comme l'étaient les élèves pour explorer les groupes, ils auraient pu, avec un peu de directivité de ma part, s'attaquer, par exemple, aux deux résultats suivants.

A chaque tresse on peut associer la permutation qu'elle réalise entre la position

des brins au départ et à l'arrivée. En fait les tresses ce sont les permutations plus la mémoire de la façon dont cette permutation a été réalisée.

Les tresses dont la permutation associée est l'identité forment un sous groupe distingué du groupe  $B_n$ .

$B_n$  est engendré par  $\sigma_1$  et  $t = \sigma_{n-1} \dots \sigma_1$ .

En effet pour tout  $i$  dans  $[1, \dots, n-1]$  on a :

$$\begin{aligned} t \sigma_{i+1} &= \sigma_{n-1} \dots \sigma_{i+2} \sigma_{i+1} \sigma_i \sigma_{i-1} \dots \sigma_1 \sigma_{i+1} \\ &= \sigma_{n-1} \dots \sigma_{i+2} \sigma_{i+1} \sigma_i \sigma_{i+1} \sigma_{i-1} \dots \sigma_1 \\ &\quad [\text{car } \sigma_{i+1} \text{ permute avec } \sigma_{i-1} \dots \sigma_1] \\ &= \sigma_{n-1} \dots \sigma_{i+2} \sigma_i \sigma_{i+1} \sigma_i \sigma_{i-1} \dots \sigma_1 \\ &\quad [\text{car } aba = bab] \end{aligned}$$

$$\begin{aligned} &= \sigma_i \sigma_{n-1} \dots \sigma_{i+2} \sigma_{i+1} \sigma_i \sigma_{i-1} \dots \sigma_1 \\ &\quad [\text{car } \sigma_i \text{ permute avec } \sigma_{n-1} \dots \sigma_{i+2}] \\ &= \sigma_i t \end{aligned}$$

Donc  $\sigma_{i+1} = t^{-1} \sigma_i t$ . Et par itération on obtient tous les générateurs de  $B_n$ .

Je dois à la remarquable conférence faite lors des journées de l'APMEP, en 2005 à Caen, par Monsieur Patrick Dehornoy, de m'être lancé dans ce travail. Le sujet est tout de même assez ardu pour des lycéens et j'ai vu fondre les effectifs ; à la fin il restait une grosse demi-douzaine d'élèves. Dont une fille, acharnée par le sujet, et qui s'était même très joliment tressé les cheveux durant l'année ! Les garçons participaient bien, mais certains en renâclant. Pour une fois que j'avais des filles en club scientifique j'ai passé outre, et maintenu ce sujet. Un des grands moments a été quand elles nous ont montré comment faire des nattes à quatre brins.

**Références :**

[1] P. Dehornoy (1997) L'art de tresser, Dossier HS Pour la Science avril 1997 La science des nœuds, p 68-74  
 [2] P. Dehornoy (2006) Le calcul des tresses Bulletin Vert de l'APMEP N° 465, p 465-476  
 [3] T. Aubriot & E. Wagner (2006) Des tresses et des nœuds mathématiques L'Oouvert N°113, p 1-16  
[www.math.unicaen.fr/~dehornoy](http://www.math.unicaen.fr/~dehornoy) Le site de Patrick Dehornoy spécialiste des tresses  
[www.chez.com/alexandrebenoit](http://www.chez.com/alexandrebenoit) Pour débiter  
[www.animath.fr/UE/autres/tresses](http://www.animath.fr/UE/autres/tresses) Une page avec des questions, ce qui est bien dans l'esprit d'Animath