

Plan :

- 1. **Une** solution au problème d'isotopie des tresses
- 2. **Des** solutions au problème d'isotopie des tresses

- Une **tresse** :



- La théorie des tresses : géométrie (et calcul) des **croisements** ;



C.F. Gauss
1777–1855



A. Hurwitz
1859–1919



E. Artin
1898–1962

- Un **diagramme de tresse** à 3 brins :



- Problème d'**isotopie** : Etant donnés deux diagrammes, peut-on **déformer** l'un en l'autre ?



↑
est isotope à

- Intérêt en coiffure...
- Une **tresse** = une classe d'isotopie de diagrammes
↪ solution au problème d'isotopie
= condition pour parler de tresses de façon non ambiguë.
- En particulier : préliminaire pour **toute** utilisation algorithmique
↪ **cryptographie** (remplacer les entiers par des tresses ?)

- Lien avec la théorie des **nœuds**:
Tout nœud (tout entrelacs) est
clôture d'une tresse.

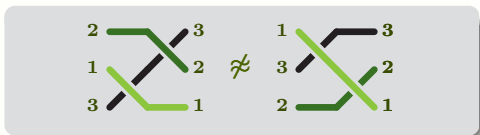


- ↪ isotopie des tresses = première étape vers isotopie des nœuds.
- Liens avec la **physique** (équation de Yang–Baxter), la **chimie**,
et la **biologie** (macromolécules, ADN).

- Deux demi-problèmes :
- Prouver une isotopie : construire la déformation.



- Prouver une non-isotopie : trouver un invariant I
 $I : \{\text{diagrammes}\} \rightarrow \Omega$ t.q. $D \approx D'$ entraîne $I(D) = I(D')$.
- Exemple 1: permutation: $\Omega = \mathfrak{S}_n$.



- Exemple 2: nombre de **croisements**: $\Omega = \mathbb{N}$?

$$2 \text{ } \begin{array}{c} \diagup \diagdown \\ \diagdown \diagup \end{array} \approx \begin{array}{c} \text{---} \\ \text{---} \end{array} 0$$

\rightsquigarrow **parité** nombre de croisements : $\Omega = \mathbb{Z}/2\mathbb{Z}$.

\rightsquigarrow **différence** nombres de croisements dessus-dessous : $\Omega = \mathbb{Z}$.

$$+1 = +2 - 1 \text{ } \begin{array}{c} \diagup \diagdown \\ \diagdown \diagup \end{array} \neq \begin{array}{c} \diagdown \diagup \\ \diagup \diagdown \end{array} +1 - 2 = -1$$

- Exemple 3: **nombre d'enlacement** de deux brins : $\Omega = \mathbb{Z}$.

$$+2 \text{ } \begin{array}{c} \text{---} \\ \text{---} \end{array} \begin{array}{c} \diagup \diagdown \\ \diagdown \diagup \end{array} \neq \begin{array}{c} \text{---} \\ \text{---} \end{array} \begin{array}{c} \diagdown \diagup \\ \diagup \diagdown \end{array} -2$$

plus généralement, supprimer des brins (= projeter)

- **Question** : Obtient-on ainsi une famille **complète** d'invariants ?

↑
qui sépare deux diagrammes
non isotopes quelconques

- Un exemple résistant :



- non isotopes (à démontrer), et pourtant
- même permutation,
- même nombres d'enlacement des brins deux à deux,
- donc même différence dessus-dessous.

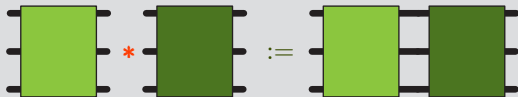


Ce n'est **pas** un problème trivial...

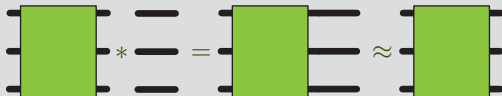
- Le point de départ d'une approche moins naïve :

Les tresses ont une structure de **groupe**.

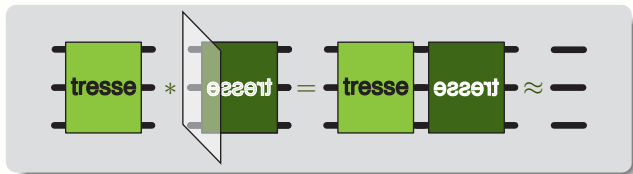
- Produit** de deux diagrammes de tresse :



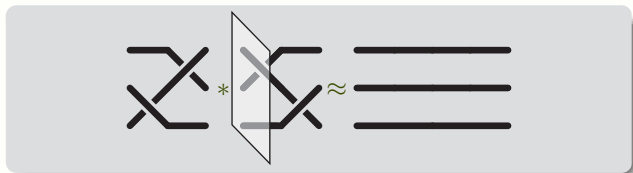
- Associatif** ;
- Compatible** avec l'isotopie \approx induit un produit sur les tresses ;
- Possède un **élément neutre** :



- Le produit possède des **inverses** :



- Exemple :



- Pour chaque n , le groupe B_n des tresses à n brins.

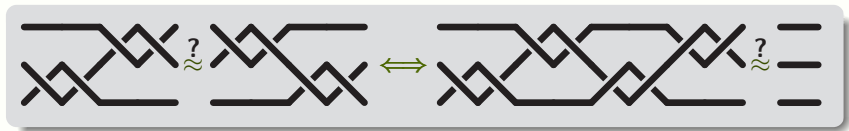
↑
classes d'isotopie de diagrammes

- NB: Une tresse est **représentée** par plusieurs diagrammes.

- Que gagne-t-on avec la structure de groupe ?

- **Réduction** du problème d'isotopie au problème de **trivialité** :

$$D \approx D' \iff D^{-1} * D' \approx 1.$$

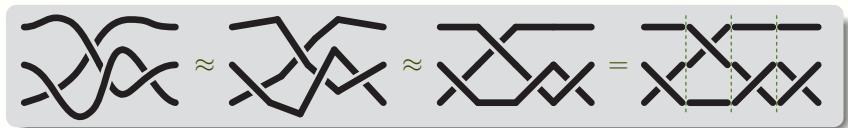


- Possibilité d'utiliser des **méthodes générales** d'algèbre (?)

↪ requiert d'abord une spécification du groupe B_n .

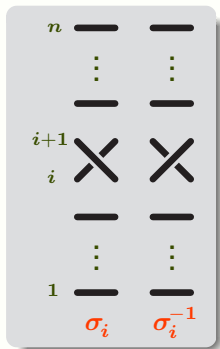
↑
typiquement : une présentation
par générateurs et relations

- **Normalisation** et **décomposition** des diagrammes :

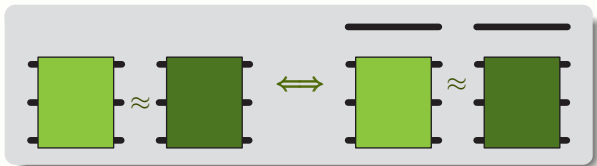


$$\begin{matrix} \uparrow & \uparrow & \uparrow & \uparrow \\ \sigma_1 & \sigma_2 & \sigma_1^{-1} & \sigma_1^{-1} \end{matrix}$$

- **Générateurs d'Artin** :

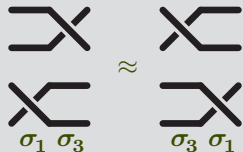
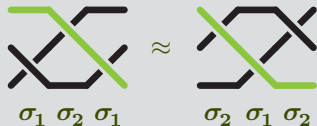


- **Remarque** : B_{n-1} identifié à un sous-groupe de B_n



donc pas d'ambiguïté sur σ_i

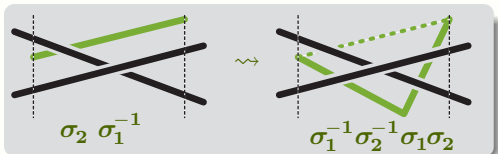
- **Relations** entre les σ_i :



Théorème (Artin '25) : Le groupe B_n admet la présentation

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{l} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \text{ pour } |i - j| = 1 \\ \sigma_i \sigma_j = \sigma_j \sigma_i \text{ pour } |i - j| \geq 2 \end{array} \right\rangle.$$

- **Démonstration** :
Isotopie de diagrammes affines par morceaux = Δ -mouvements. \square



- Conséquence : Le problème d'isotopie des tresses est ramené au **problème de mot** du groupe de présentation ...xxx... :

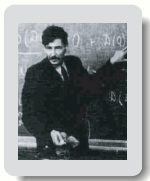
un mot sur les lettres $\sigma_i^{\pm 1}$



- **Problème** : Etant donné un mot de tresse w , déterminer si w représente la tresse triviale dans B_n .

↑
si on a $w \equiv \varepsilon$, où \equiv est la plus petite congruence contenant les paires $(\sigma_i \sigma_j \sigma_i, \sigma_j \sigma_i \sigma_j)$ avec $|i - j| = 1$, et $(\sigma_i \sigma_j, \sigma_j \sigma_i)$ avec $|i - j| \geq 2$, et $(\sigma_i \sigma_i^{-1}, \varepsilon)$ et $(\sigma_i^{-1} \sigma_i, \varepsilon)$.

- Gagné ? **non...**



- **Théorème (P. Novikov '52)** : Il existe une présentation de groupe finie dont le problème de mot est indécidable.

↑
il n'existe pas d'algorithme le résolvant

Solution (Garside) : Utiliser un monoïde.

Définition : On appelle B_n^+ le **monoïde** (= pas d'inverses)

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{l} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \text{ pour } |i - j| = 1 \\ \sigma_i \sigma_j = \sigma_j \sigma_i \text{ pour } |i - j| \geq 2 \end{array} \right\rangle^+.$$

- Etude de $B_n^+ = \text{étude de } \equiv^+, \text{ équivalence de mots positifs associée aux relations ci-dessus (notamment pb. de mot).}$
- (**Markov, Post**) Il existe une présentation finie de monoïde dont le problème de mot est indécidable.

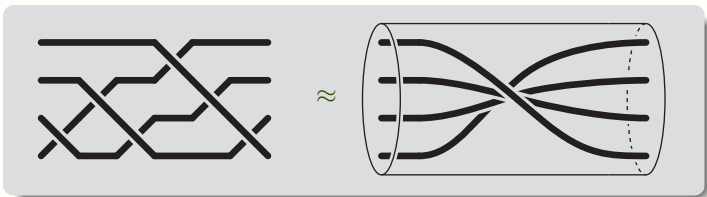
Fait : Le problème de mot pour B_n^+ est décidable.

- **Démonstration :** Comme $w \equiv^+ w'$ entraîne $\lg(w) = \lg(w')$, on peut énumérer exhaustivement les classes d'équivalence. \square

- Qu'a-t-on gagné ? Pour le moment : rien !

Question 1 : Comment ramener le problème $w \equiv \varepsilon$ (w quelconque) à un problème de mots positifs (pas de σ_i^{-1}) ?

- (Mot de) **tresse de Garside** : $\Delta_1 = 1$, $\Delta_n = \Delta_{n-1} \cdot \sigma_{n-1} \dots \sigma_2 \sigma_1$.



Lemme : Pour $1 \leq i \leq n-1$, on a $\sigma_i \Delta_n \equiv \Delta_n \sigma_{n-i}$,
et $\sigma_i^{-1} \Delta_n$ est équivalent à un mot positif.

- Donc, pour **tout** w , il existe $p \geq 0$ et v positifs t.q. $\Delta_n^p w \equiv v$,
... et alors $w \equiv \varepsilon$ équivaut à $\Delta_n^p \equiv v$.

- A-t-on gagné maintenant? toujours pas...
- Problème $w \stackrel{?}{\equiv} \varepsilon$ ramené à $\Delta_n^p \stackrel{?}{\equiv} v$, pas (encore) à $\Delta_n^p \stackrel{?}{\equiv}^+ v$.

Question 2 : Pour v, v' positifs,
 quel rapport entre $v \equiv v'$ et $v \equiv^+ v'$?

- Certainement, $w \equiv^+ w'$ entraîne $w \equiv w'$; mais réciproquement ?
 Penser à $\langle a, b, c \mid ab = ac \rangle^+ \dots$

Théorème (Ore) : Si le monoïde $\langle S \mid R \rangle^+$ est simplifiable et admet des multiples communs à droite, il se plonge dans le groupe $\langle S \mid R \rangle$.

\uparrow
 les relations \equiv_R^+ et \equiv_R sont équivalentes

- **Démonstration** : Le groupe $\langle S \mid R \rangle$ est alors
 groupe de fractions du monoïde $\langle S \mid R \rangle^+$, cf. \mathbb{Q} et \mathbb{Z} . □

Proposition (Garside) : Le monoïde B_n^+ est simplifiable.

$$axb = ax'b \text{ entraîne } x = x'$$

- Démonstration : Propriétés syntaxiques des relations de tresse. \square

Proposition (Garside) : Le monoïde B_n^+ admet des multiples communs.

- Démonstration : Δ_n est multiple de σ_i dans B_n^+ pour tout i ,
déjà vu : [équivalent à] $\sigma_i^{-1} \Delta_n$ positif (...)
- Puis : Δ_n^p est multiple de tout élément de longueur p dans B_n^+ . \square
- Donc : le monoïde B_n^+ satisfait les conditions de Ore,
et le problème d'isotopie des tresses est **décidable**.

Algorithme : Partant de w à n brins et p lettres σ_i^{-1} ,

- (i) Calculer v positif vérifiant $\Delta_n^p.w \equiv v$;
- (ii) Alors $w \equiv \varepsilon$ si et seulement si $\Delta_n^p \equiv^+ v$.

Exemple : $w = \sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$.

Poser $\mathbf{a} = \sigma_1$, $\mathbf{b} = \sigma_2 \dots$ $\mathbf{A} = \sigma_1^{-1} \dots$, d'où $w = \mathbf{BBAAbbbaa}$.

- (i) $\Delta_3^4.w = \Delta_3^4.\mathbf{BBAAbbbaa} \equiv (\mathbf{B}\Delta_3).(\mathbf{A}\Delta_3).(\mathbf{A}\Delta_3).(\mathbf{B}\Delta_3).\mathbf{bbaa}$
 $\equiv (\mathbf{ba}).(\mathbf{ab}).(\mathbf{ab}).(\mathbf{ba}).\mathbf{bbaa}$.
- (ii) $(\mathbf{aba})^4 \equiv^+ \mathbf{baababbabbaa}$? ... non (?), donc $w \not\equiv \varepsilon$.

- Complexité (très) **exponentielle** : calamiteux en pratique.
- Pour l'exemple, il suffit de décider $\sigma_1^2\sigma_2^2 \equiv^+ \sigma_2^2\sigma_1^2$:
 équivalence certainement fautive, car aucune relation ne s'applique.

Solution : Groupe de fractions

- Domaine : algèbre
- Point de vue : tresse = fraction
- Méthode : énumération exhaustive
- Auteur : Garside '67
- Mots-clés : monoïde, théorème de Ore
- Arrière-plan : propriétés spécifiques des tresses Δ_n
- Extensions : groupes de Garside



- On a obtenu **une** solution au problème d'isotopie des tresses.
- Elle est **simple**, mais très **inefficace** en pratique.

Peut-on faire **autre chose** ? Peut-on faire **mieux** ?

— Fin de la partie 1 —