DES ENSEMBLES AUX TRESSES

DES ENSEMBLES AUX TRESSES

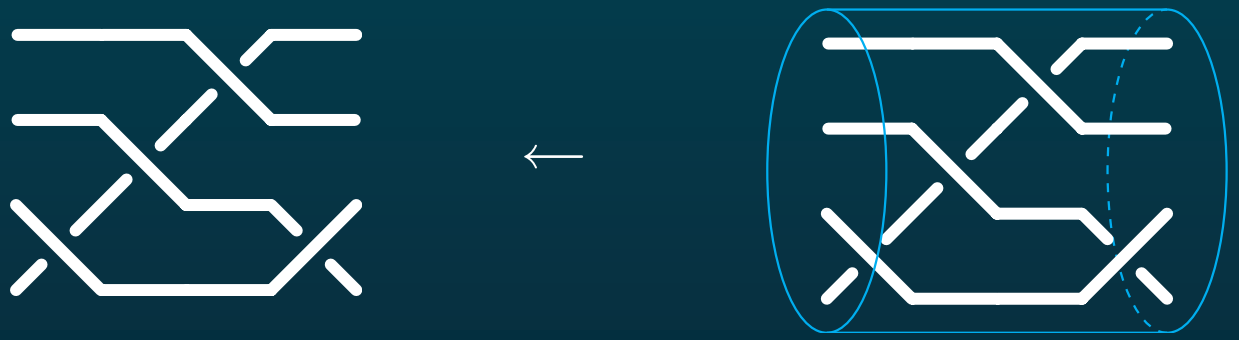
Patrick Dehornoy

Laboratoire de Mathématiques
Nicolas Oresme, Caen

TRESSES

- Un diagramme de tresse à 4 brins

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D



- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

- une tresse = une classe d'isotopie ⇝ représentée par un diagramme 2D,

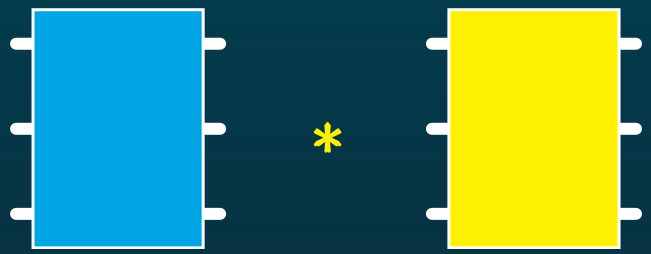
- Un diagramme de tresse à 4 brins = projection 2D d'une figure 3D

- isotopie = bouger les brins de la figure 3D en laissant les extrémités fixes

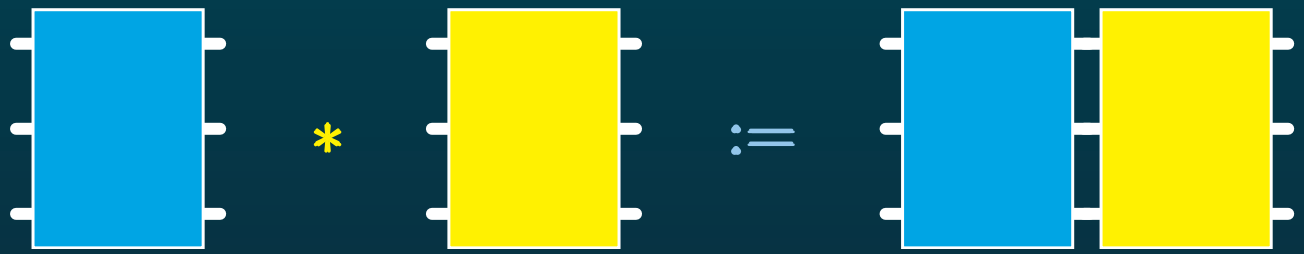
- une tresse = une classe d'isotopie $\rightsquigarrow$ représentée par un diagramme 2D, mais différents diagrammes peuvent correspondre à la même tresse.

GROUPES DE TRESSES

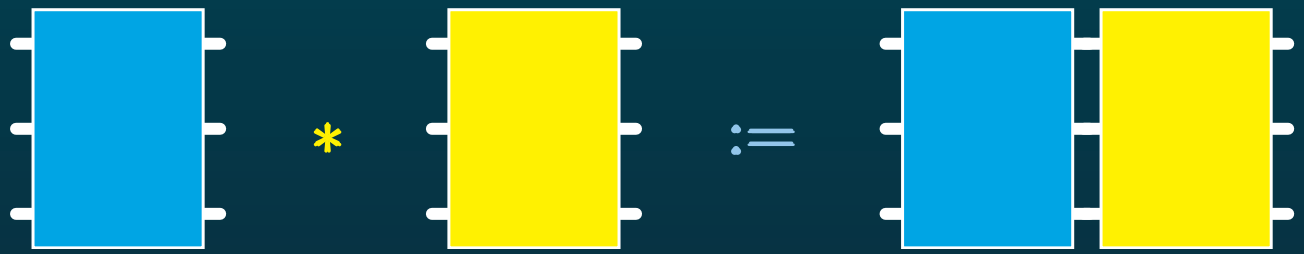
- Produit de deux tresses:



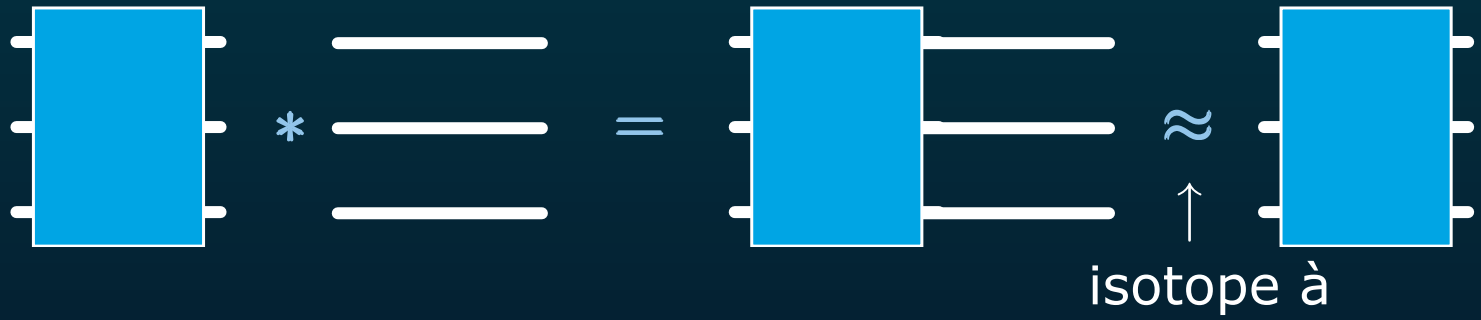
- Produit de deux tresses:



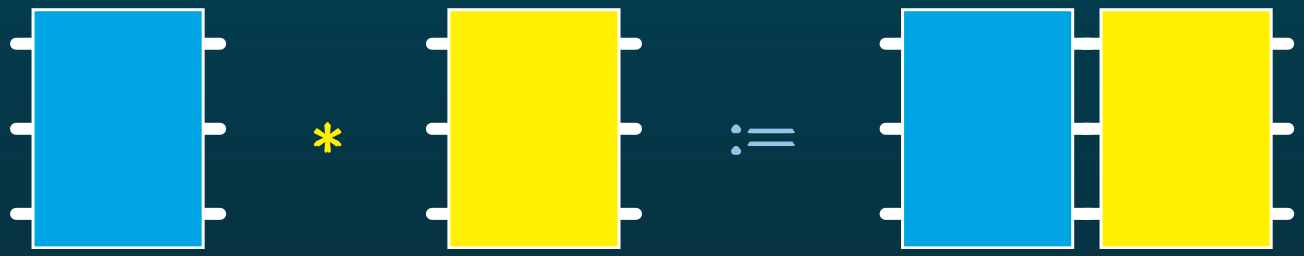
- Produit de deux tresses:



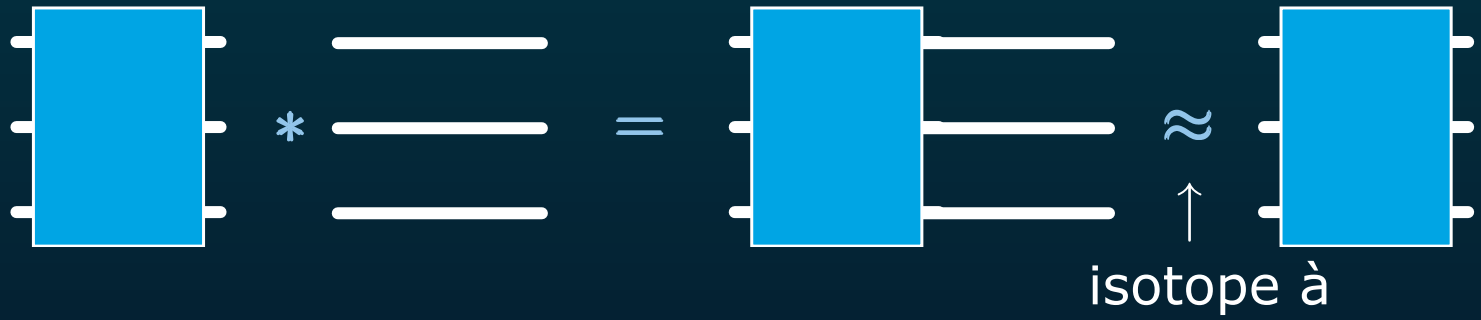
- Alors



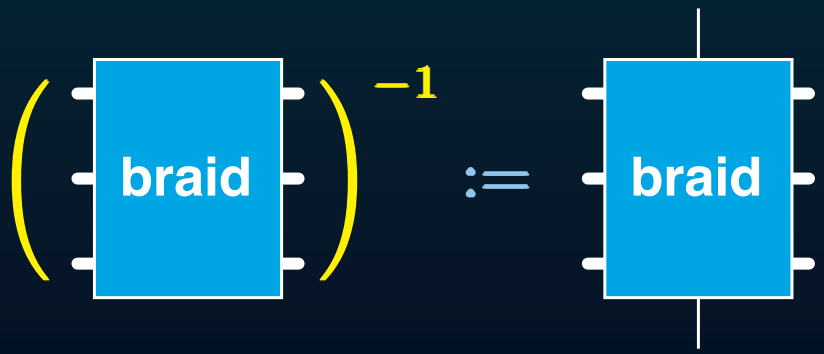
- Produit de deux tresses:



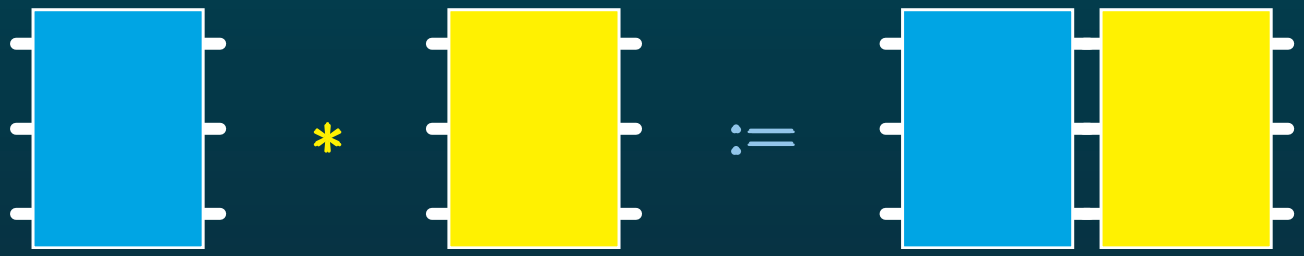
- Alors



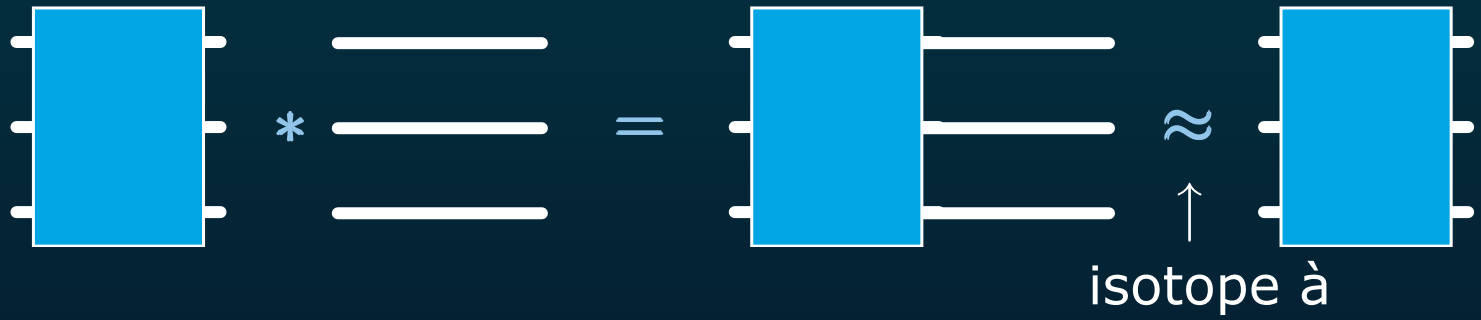
- et



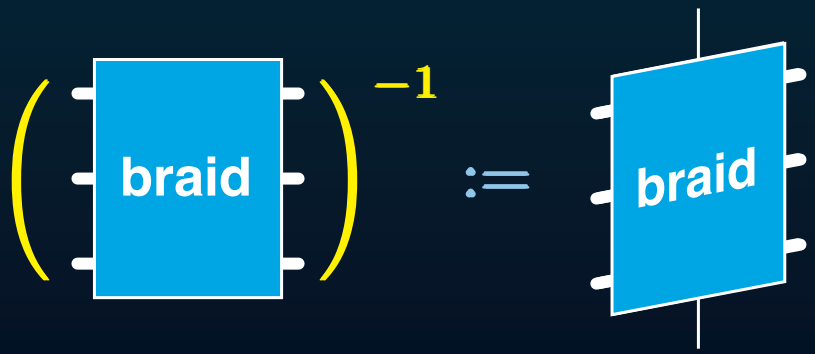
- Produit de deux tresses:



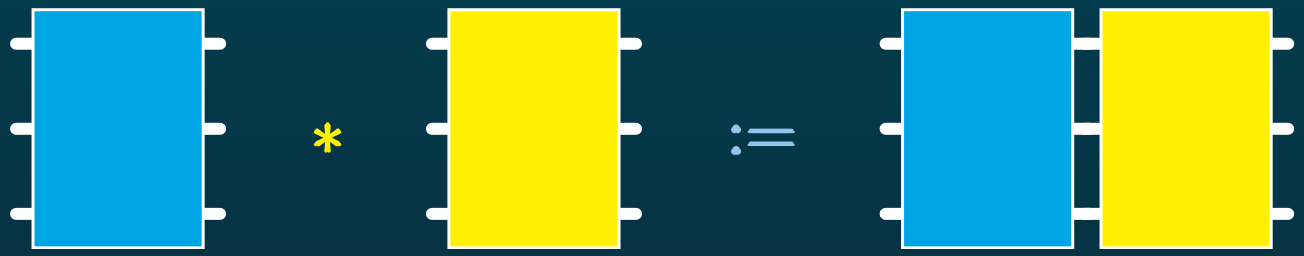
- Alors



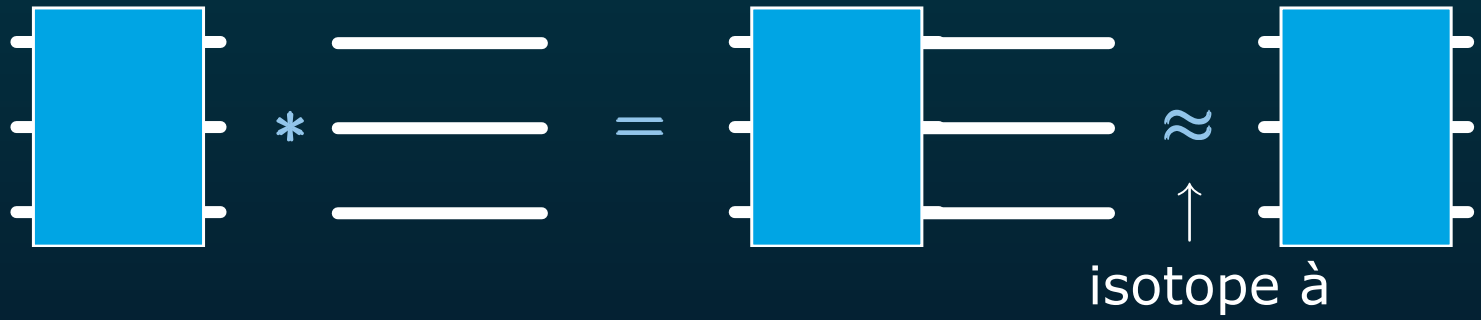
- et



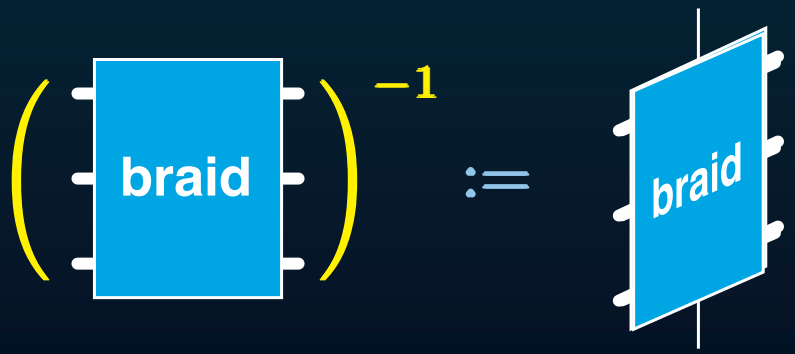
- Produit de deux tresses:



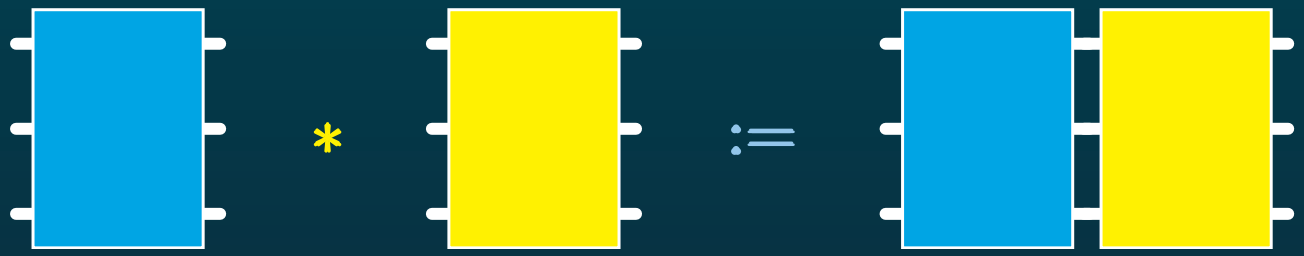
- Alors



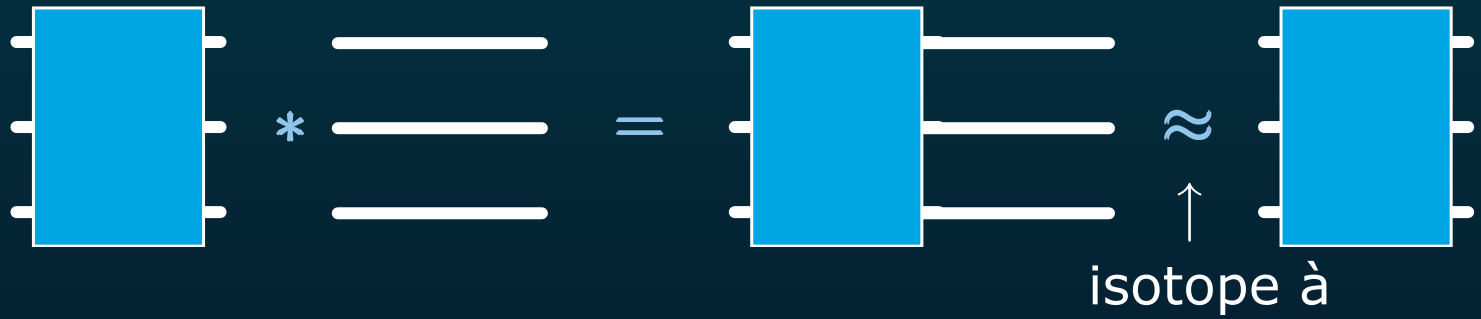
- et



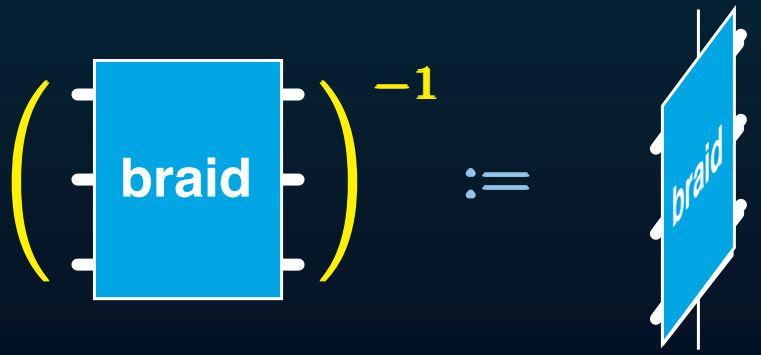
- Produit de deux tresses:



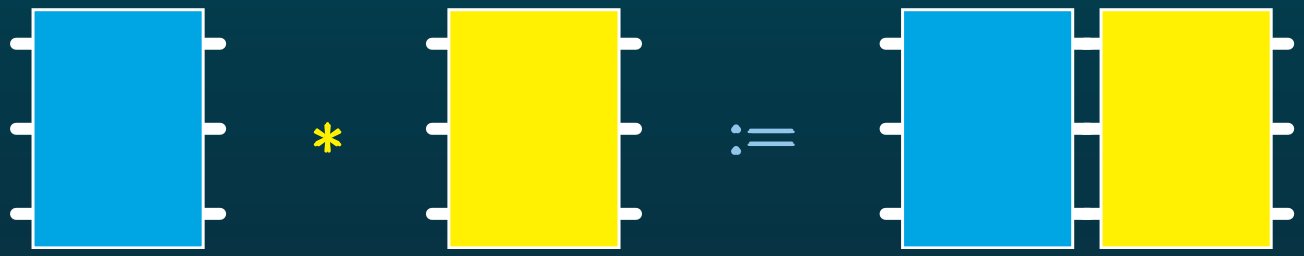
- Alors



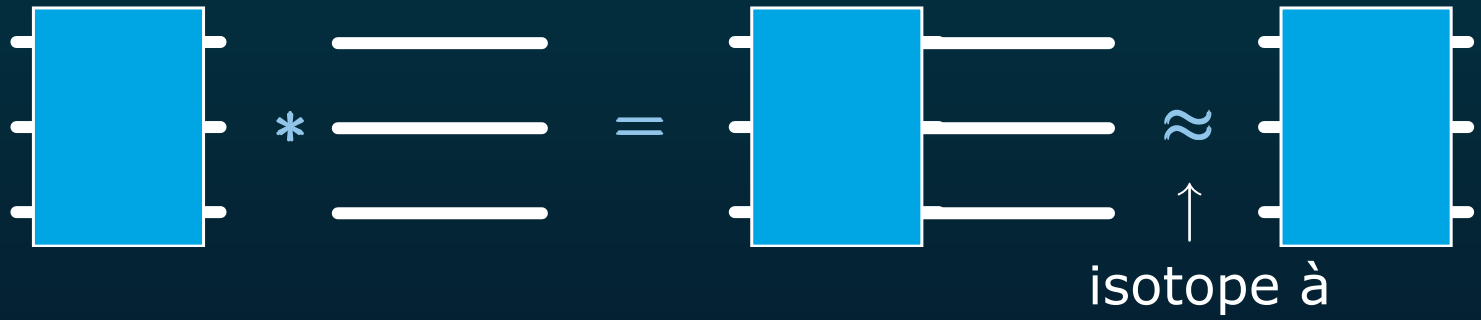
- et



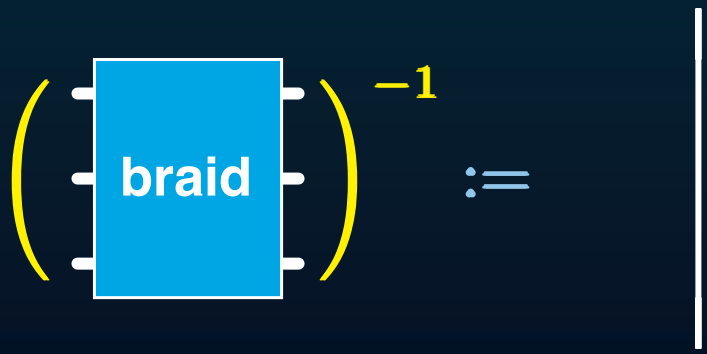
- Produit de deux tresses:



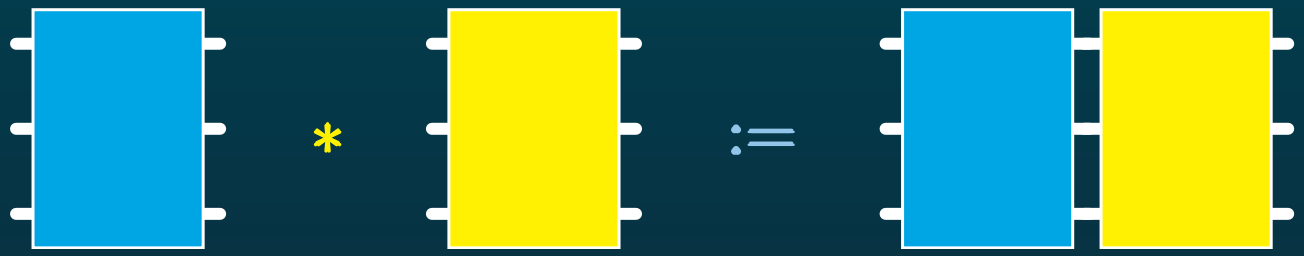
- Alors



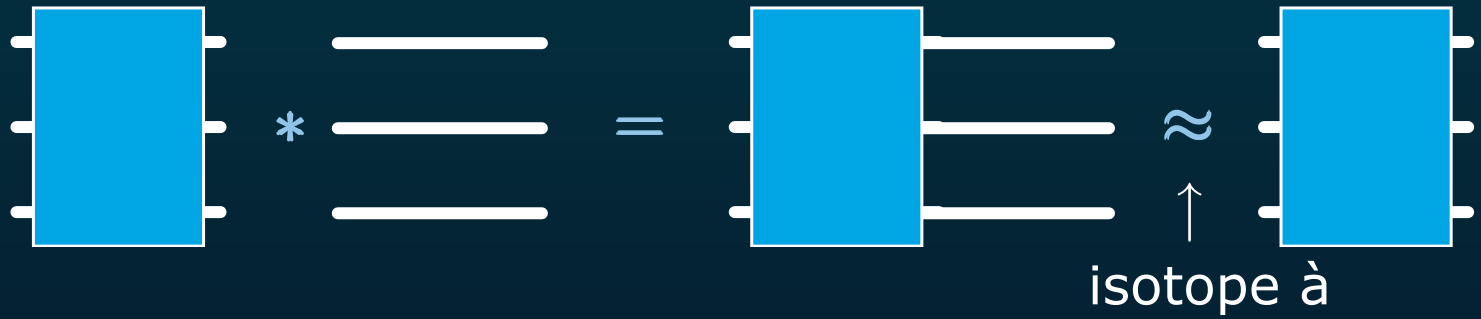
- et



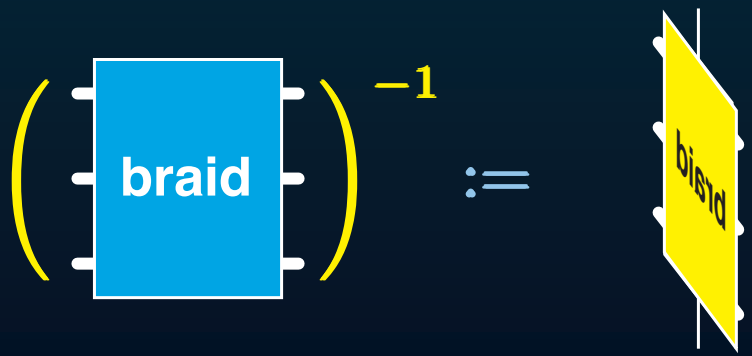
- Produit de deux tresses:



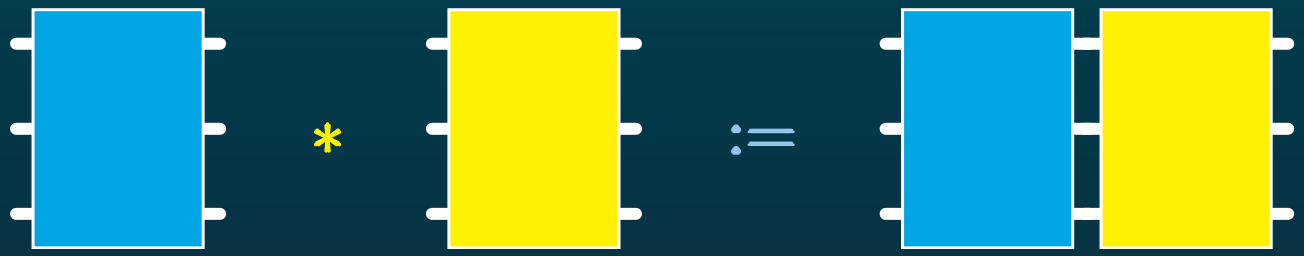
- Alors



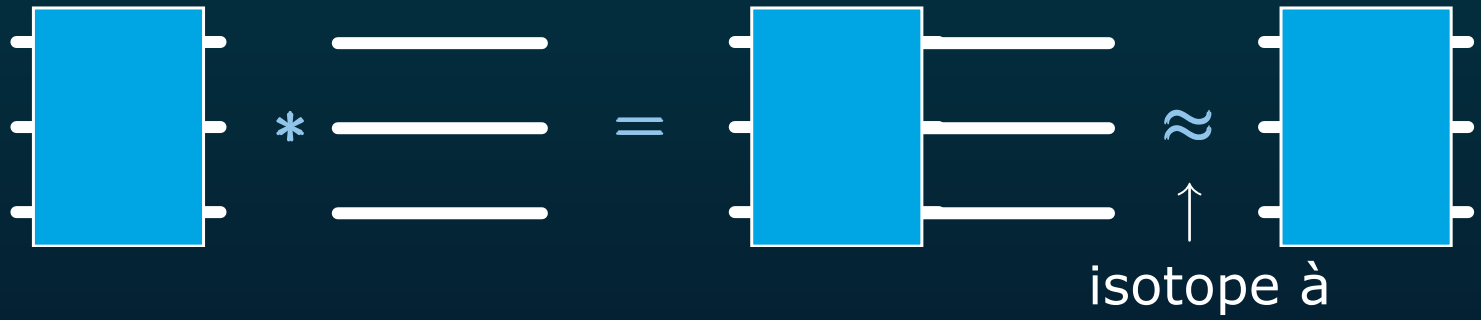
- et



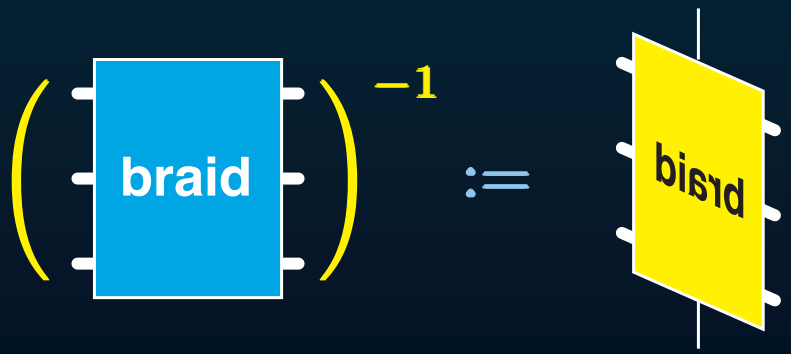
- Produit de deux tresses:



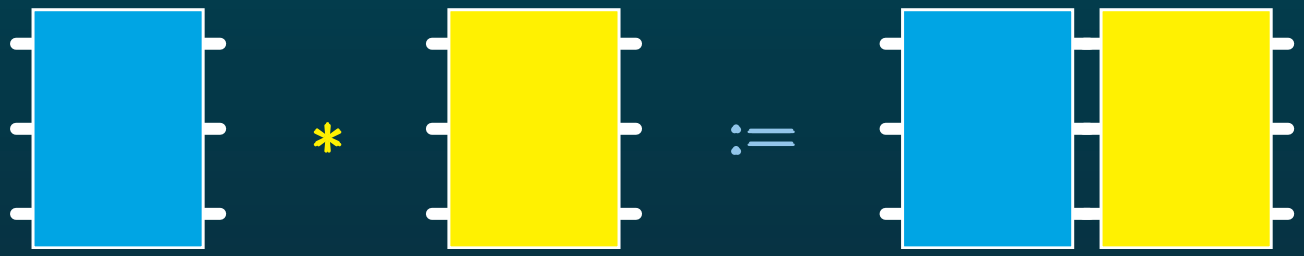
- Alors



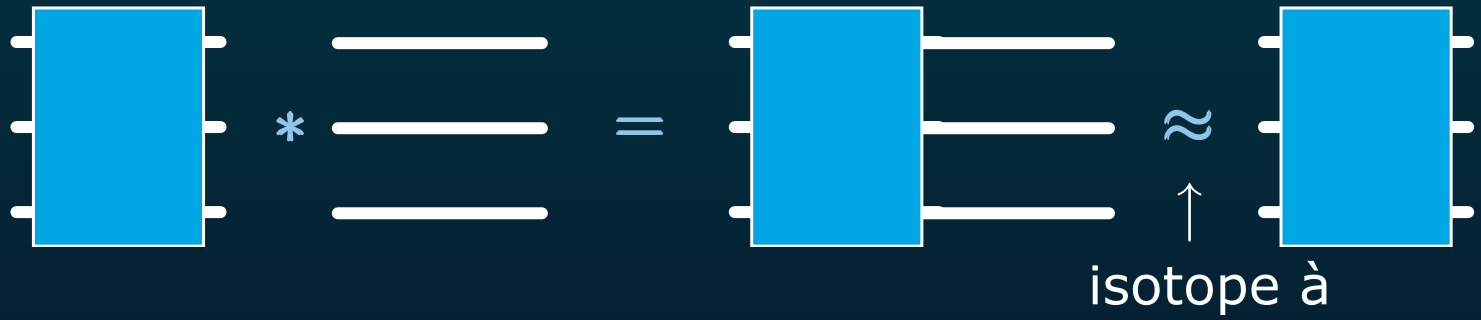
- et



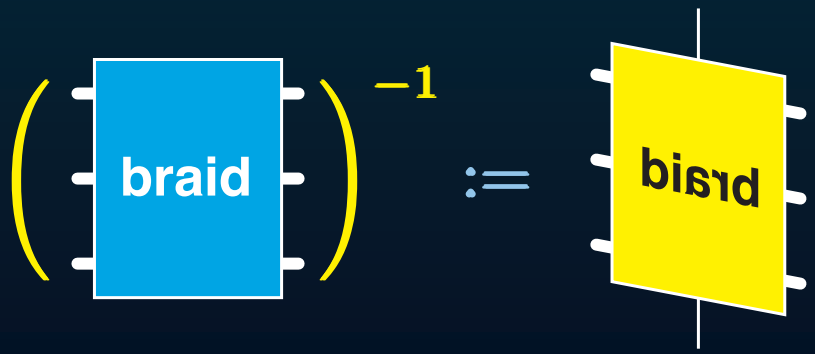
- Produit de deux tresses:



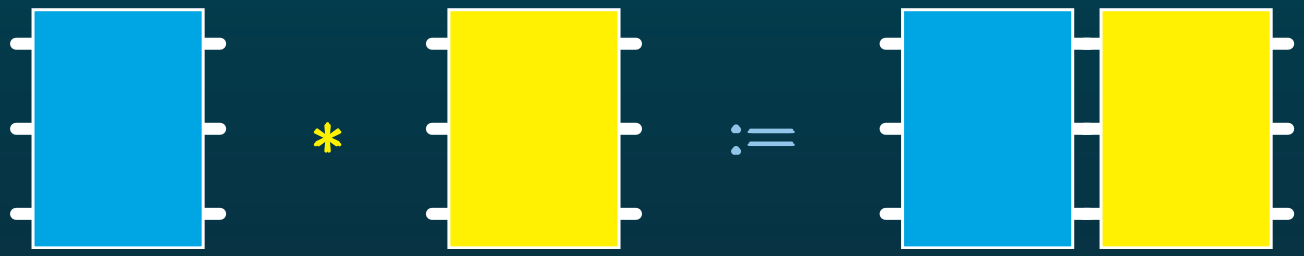
- Alors



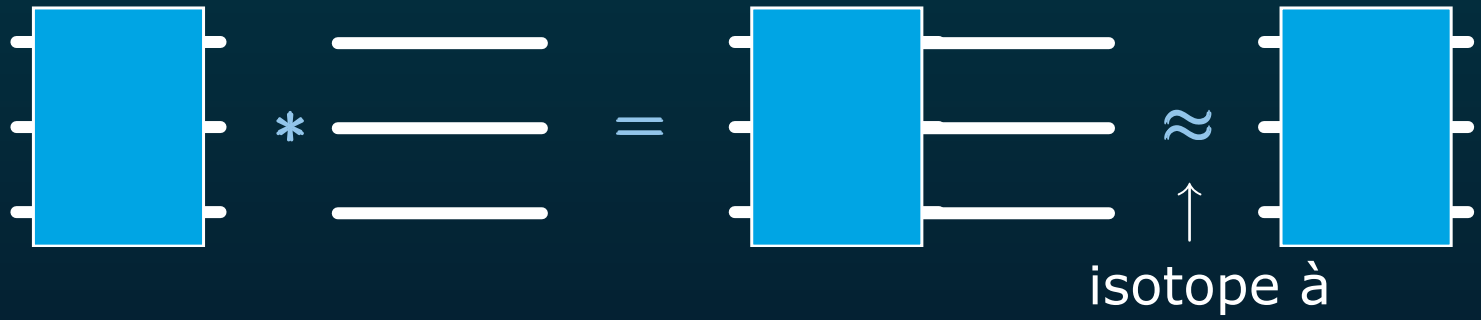
- et



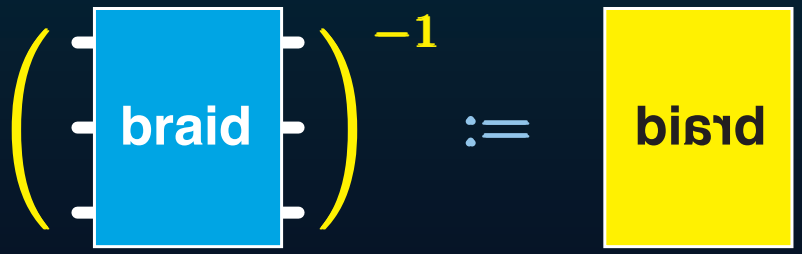
- Produit de deux tresses:



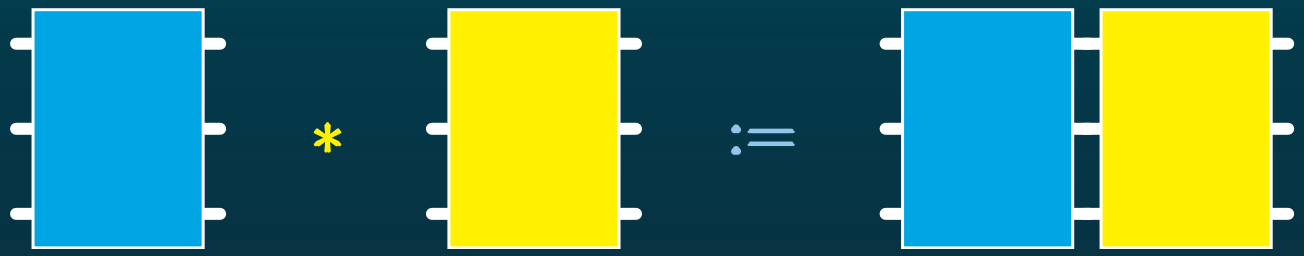
- Alors



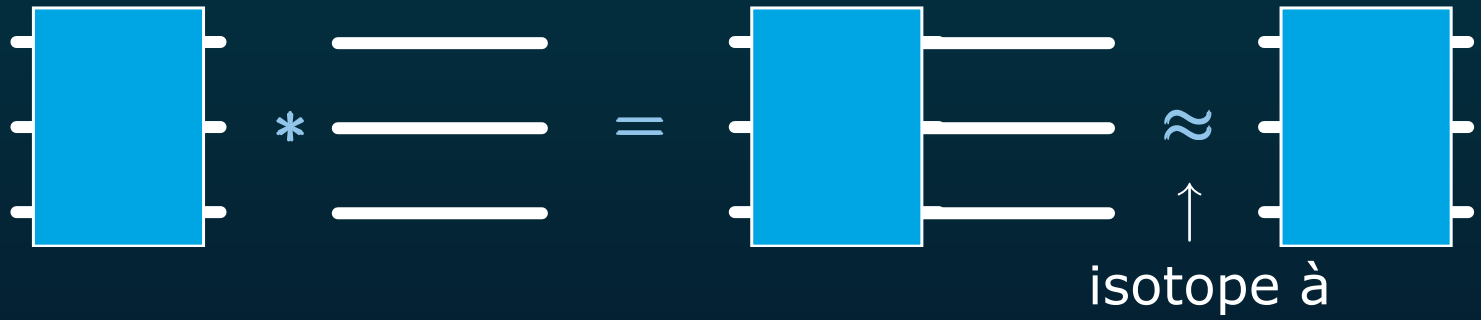
- et



- Produit de deux tresses:

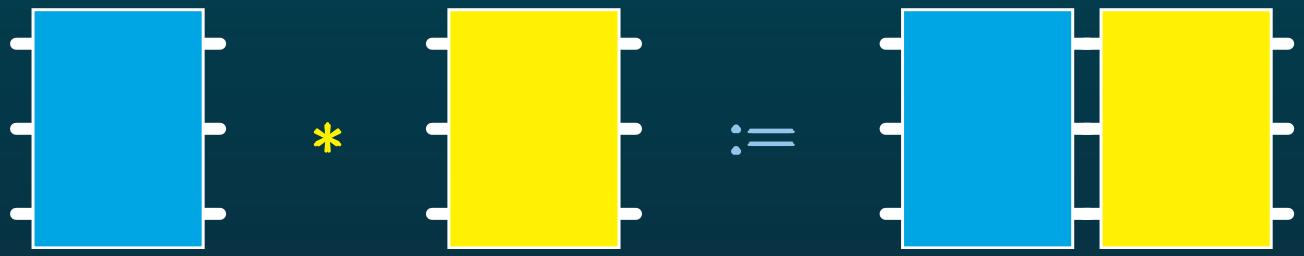


- Alors

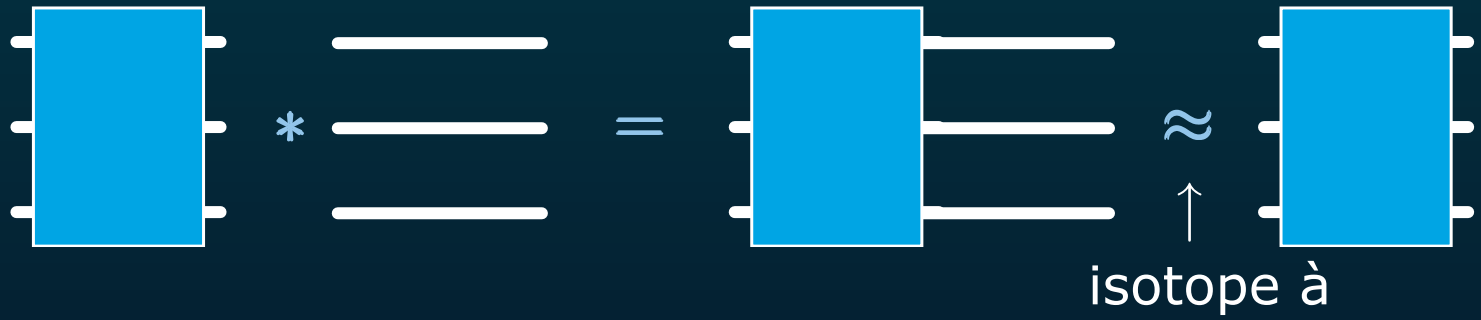


- et

- Produit de deux tresses:

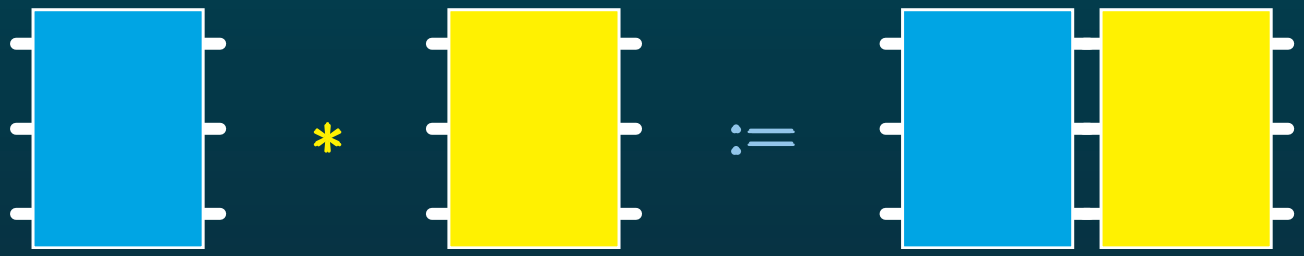


- Alors

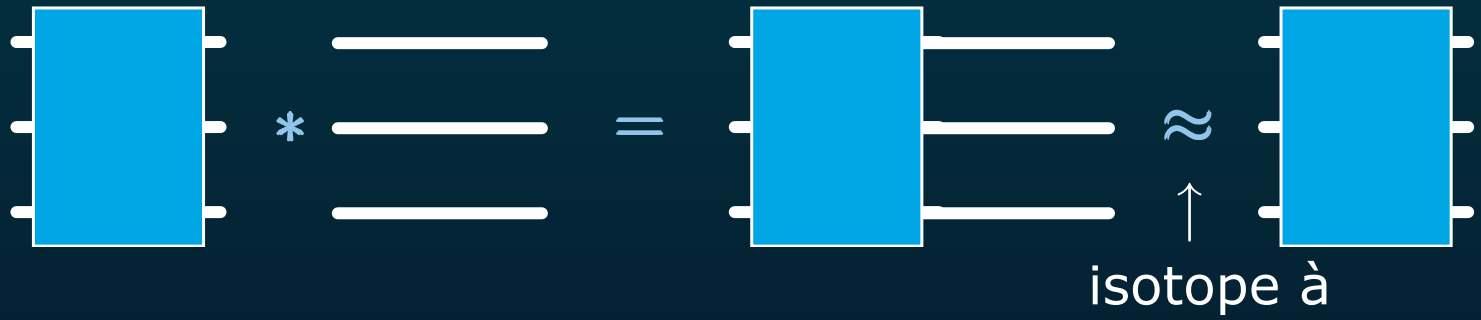


- et

- Produit de deux tresses:

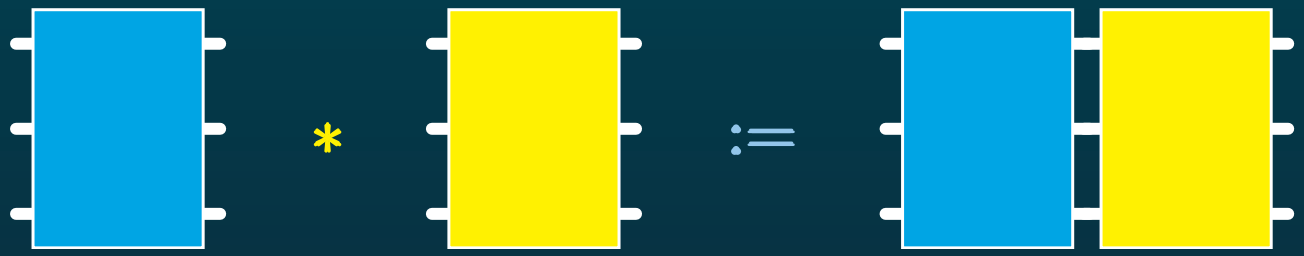


- Alors

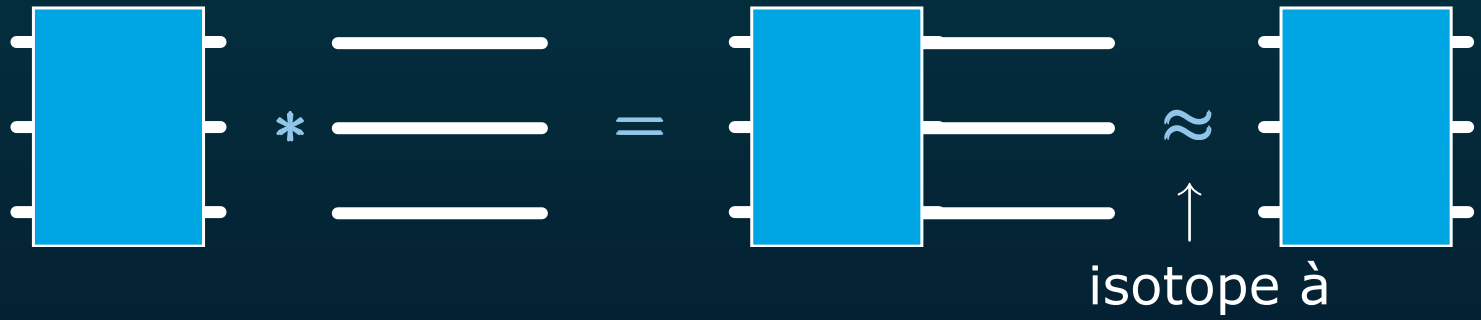


- et

- Produit de deux tresses:

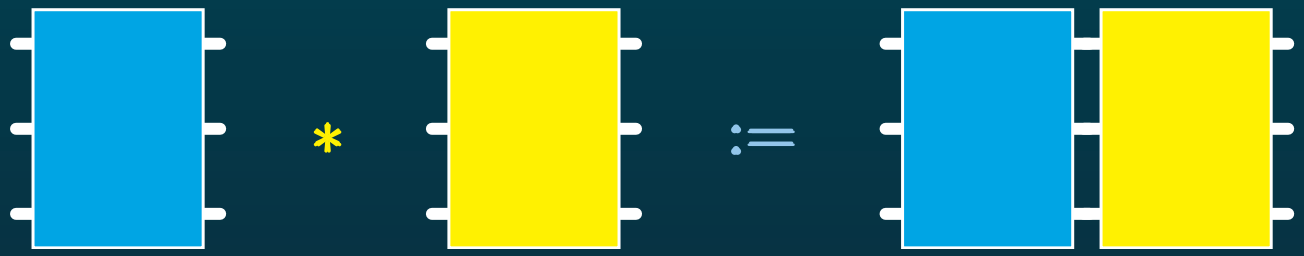


- Alors

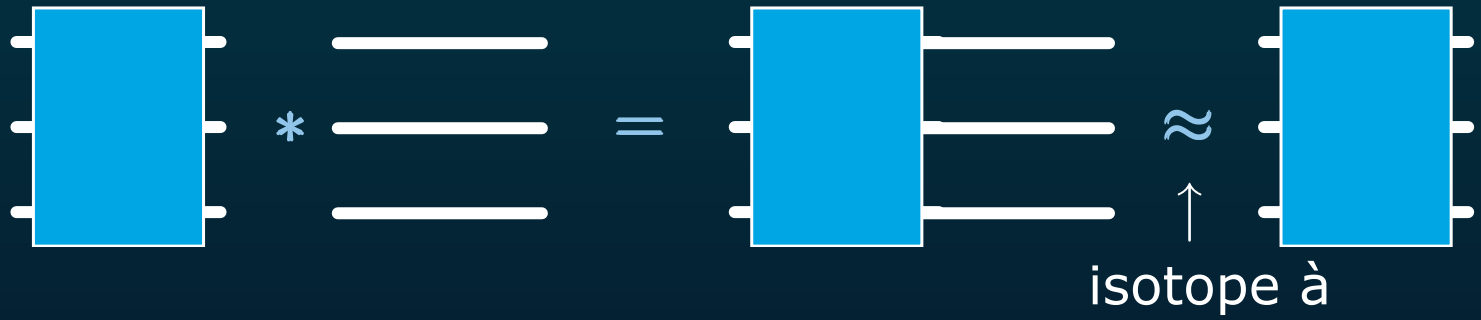


- et

- Produit de deux tresses:

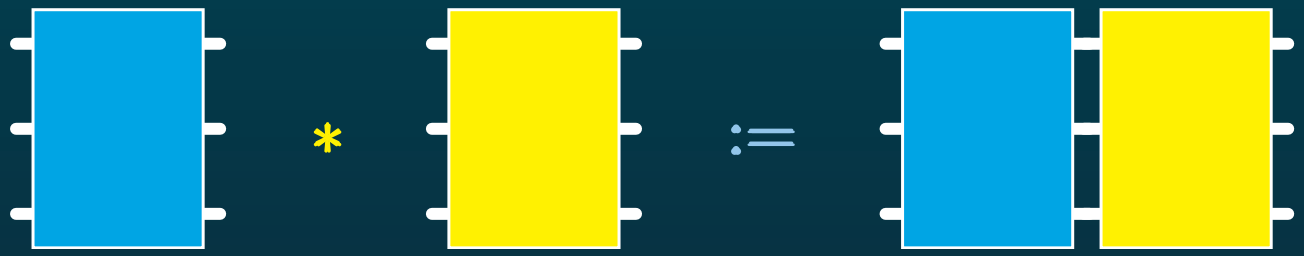


- Alors

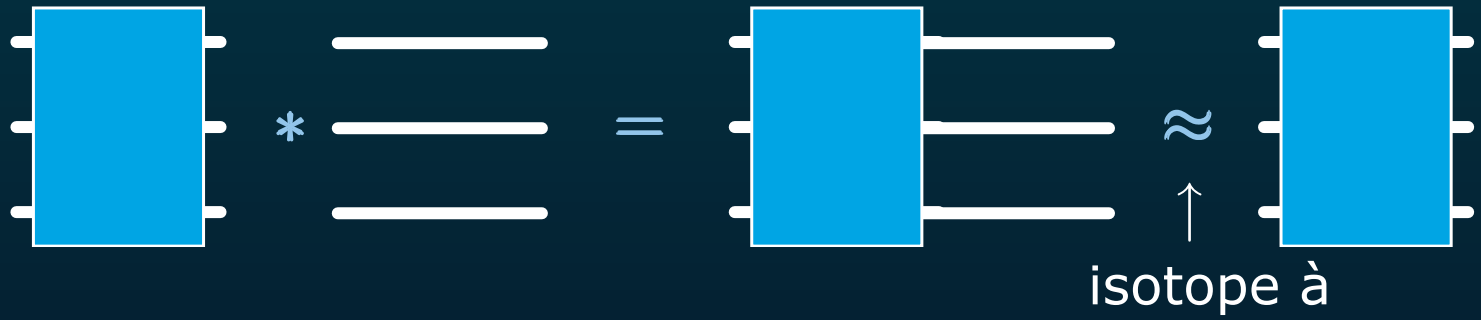


- et

- Produit de deux tresses:

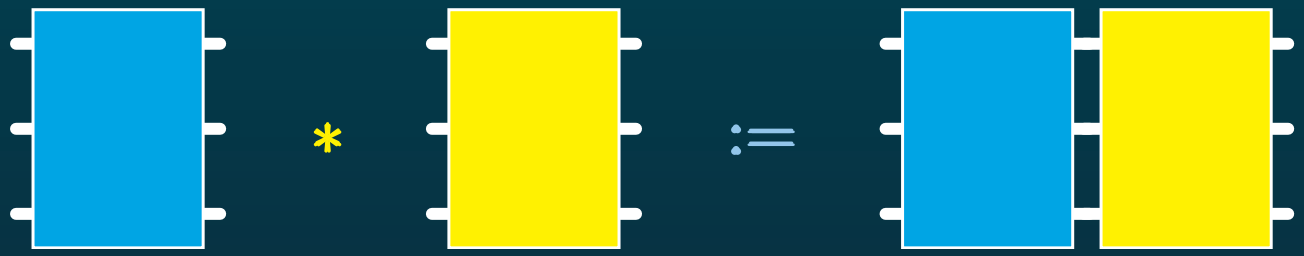


- Alors

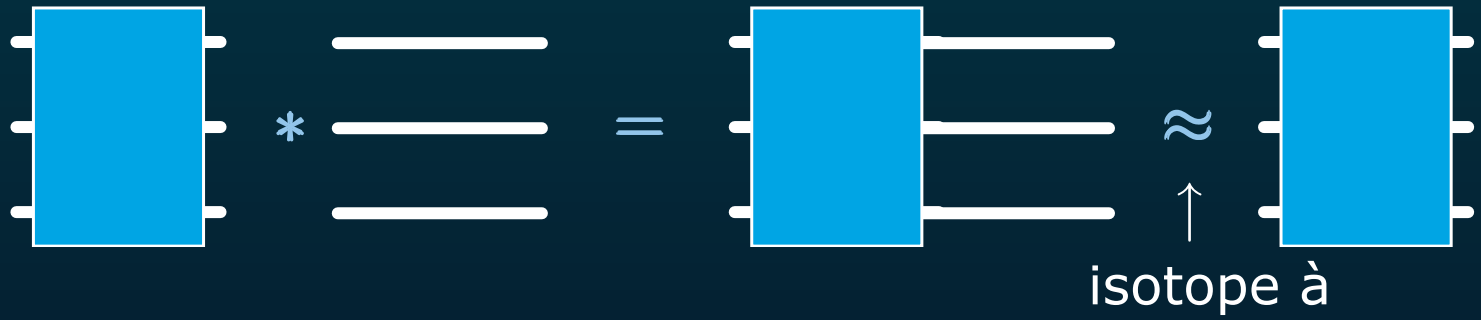


- et

- Produit de deux tresses:

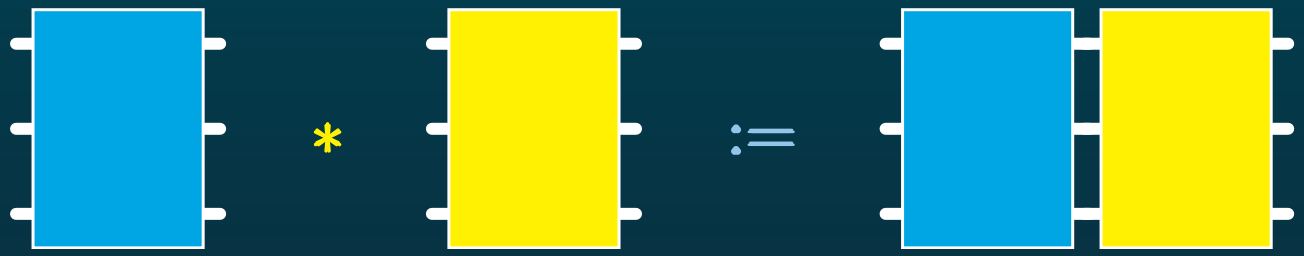


- Alors

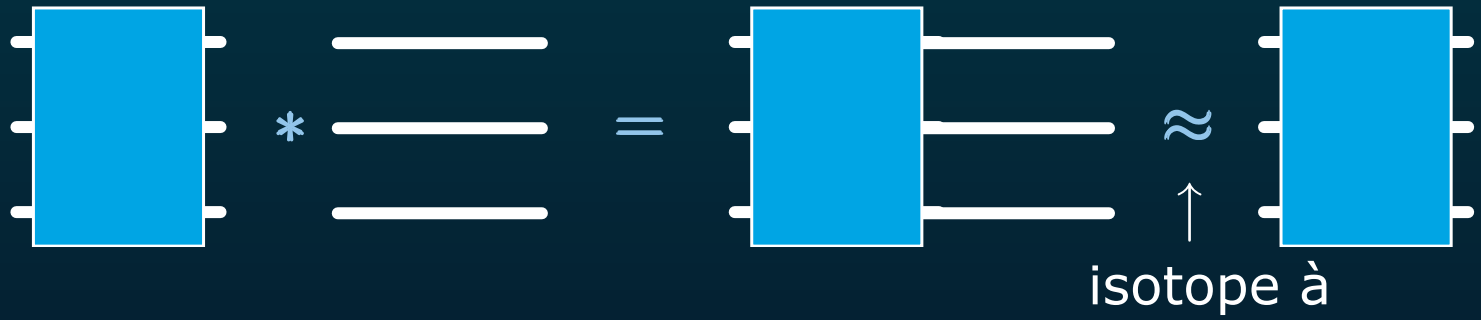


- et

- Produit de deux tresses:

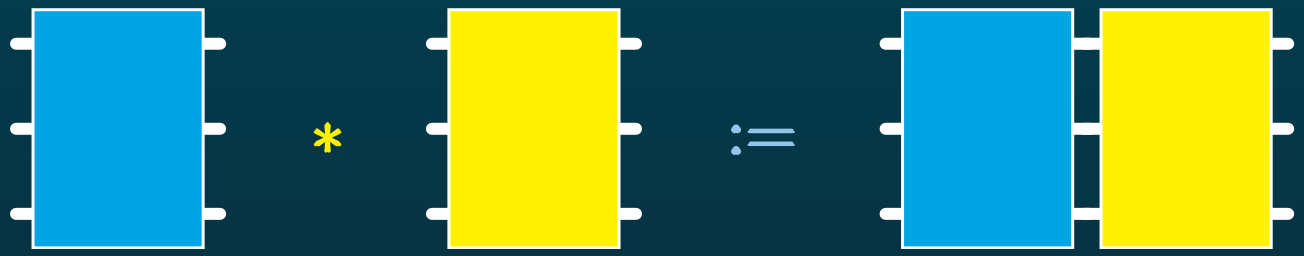


- Alors

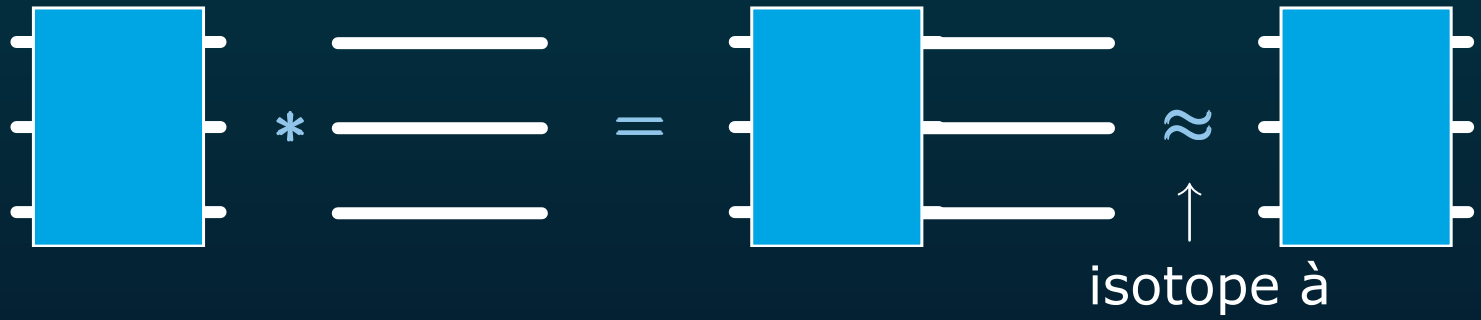


- et

- Produit de deux tresses:

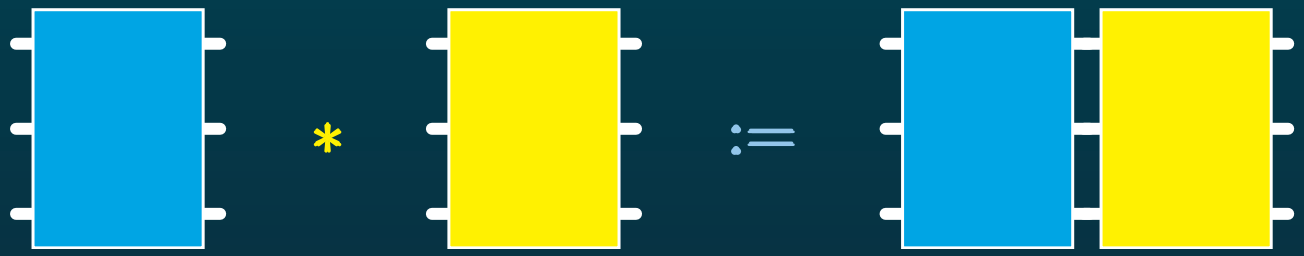


- Alors

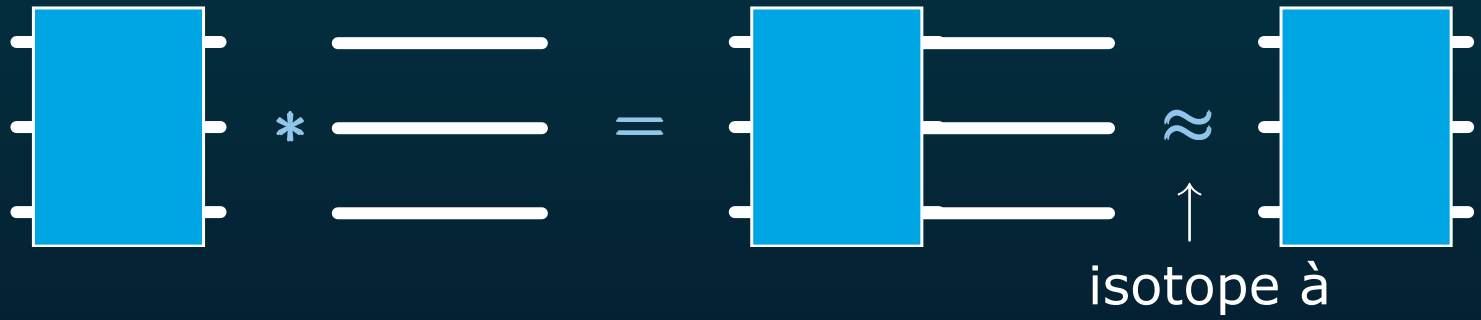


- et

- Produit de deux tresses:

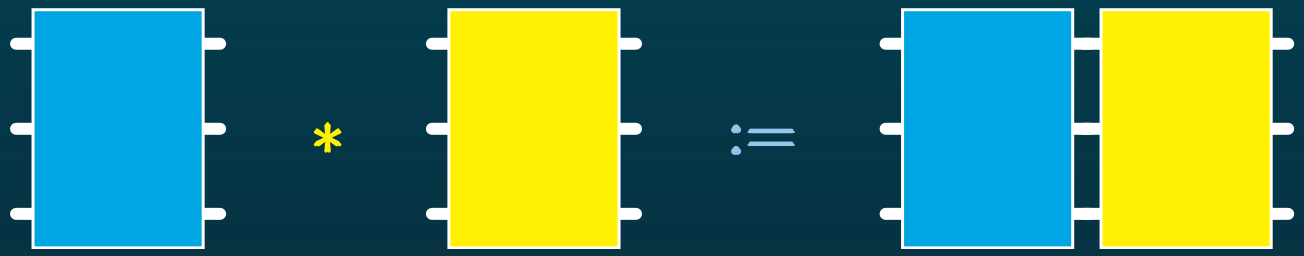


- Alors

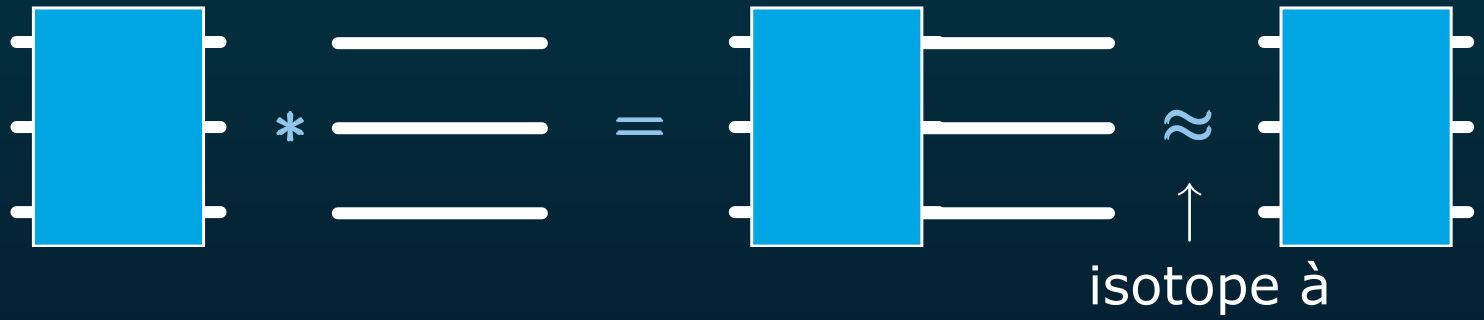


- et

- Produit de deux tresses:

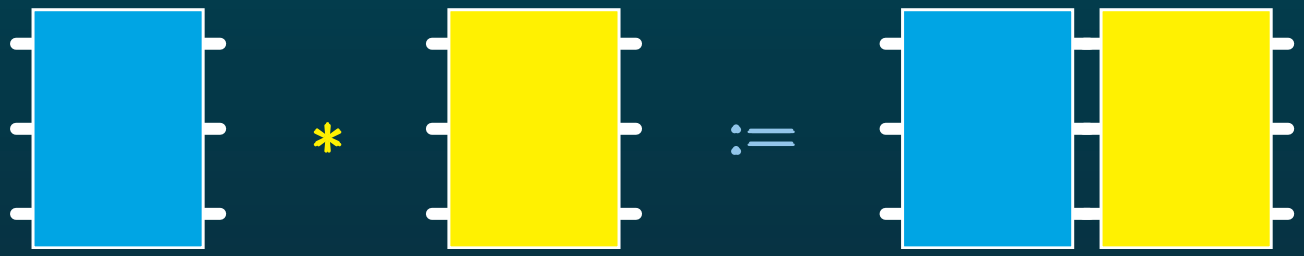


- Alors

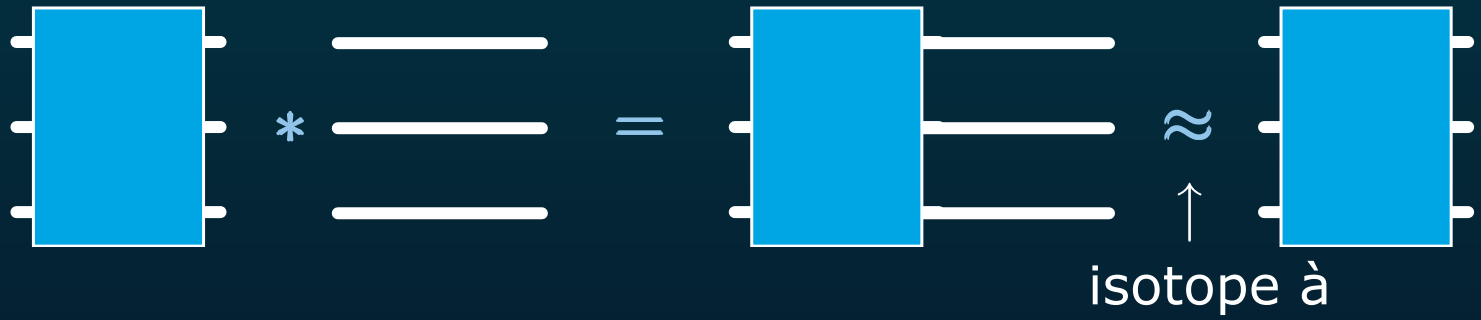


- et

- Produit de deux tresses:



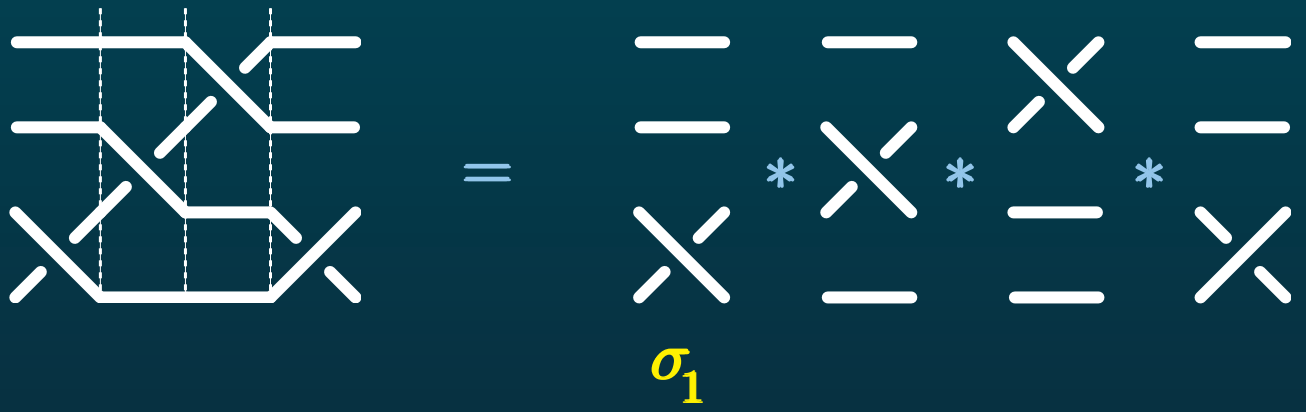
- Alors

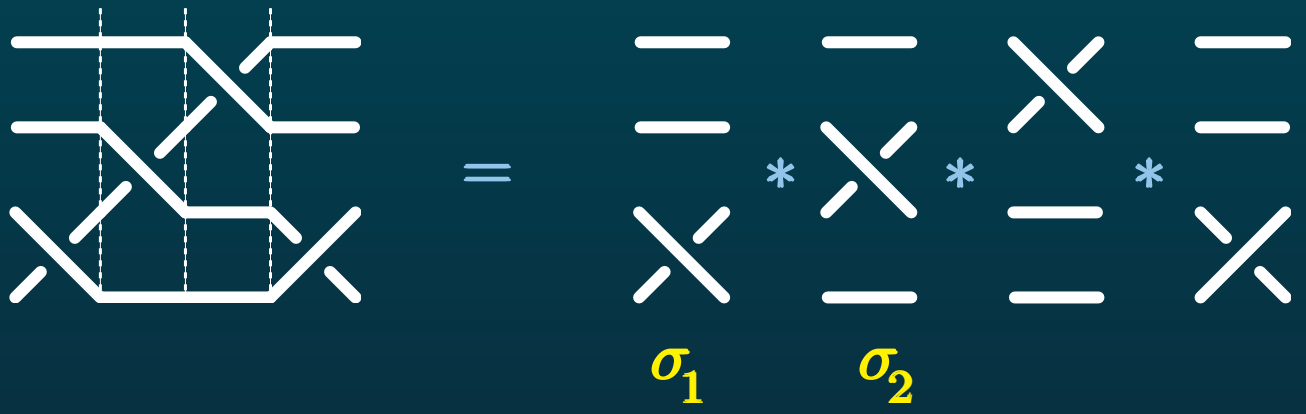


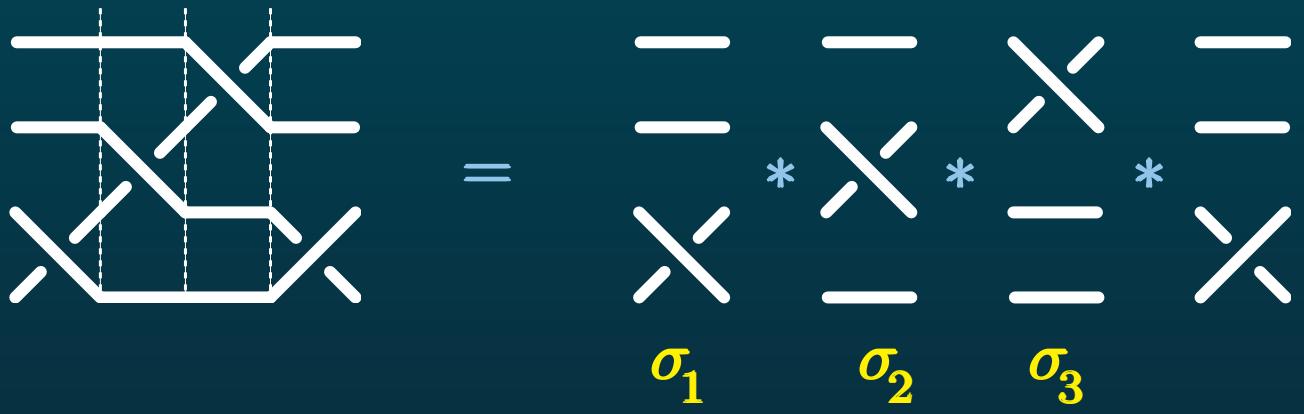
- et

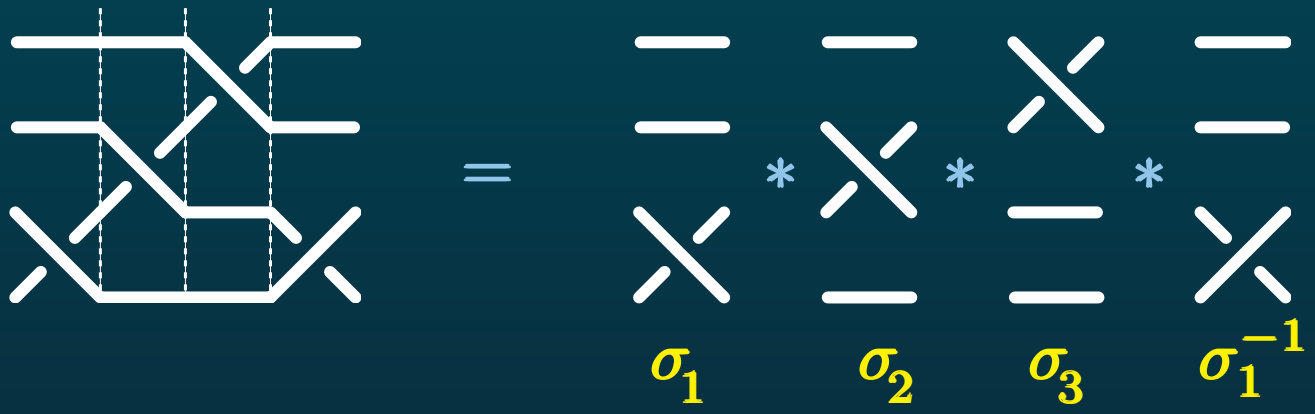
⇝ Pour chaque n, le groupe B_n des tresses à n brins (E. Artin, ∼1925).

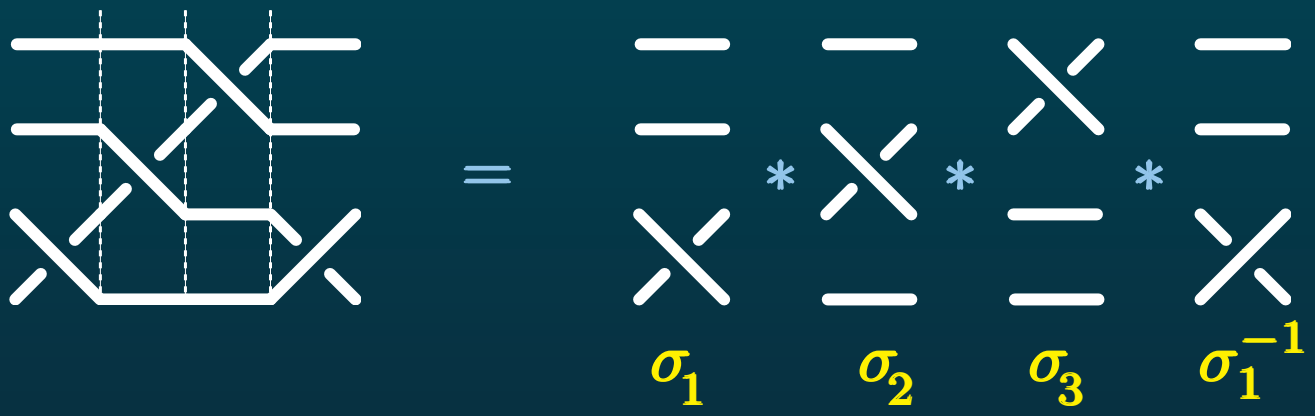
PRESENTATION DE B_n


=
*
*
*
σ_1


=
*
*
*
σ_1
σ_2

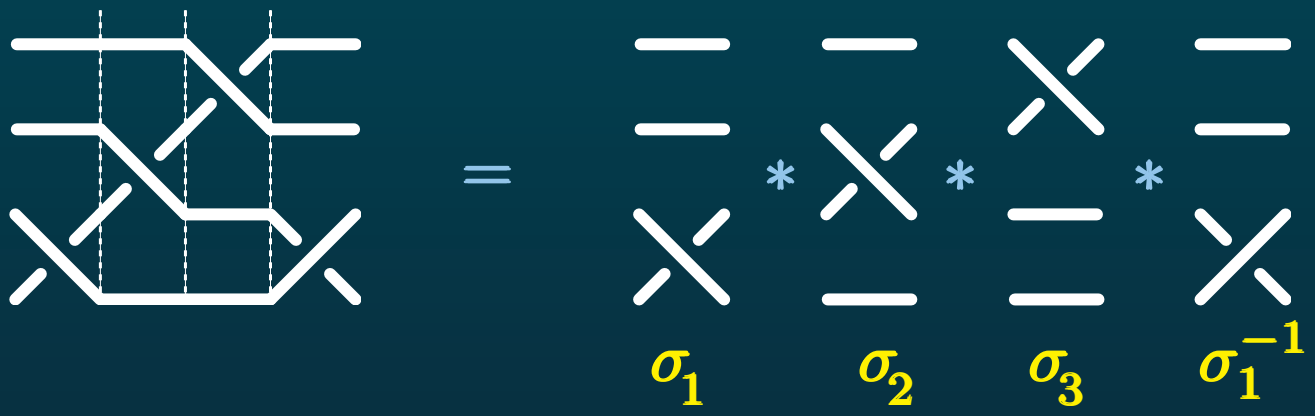

=
*
*
*
σ_1
σ_2
σ_3


=
*
*
*
σ_1
σ_2
σ_3
σ_1^{-1}



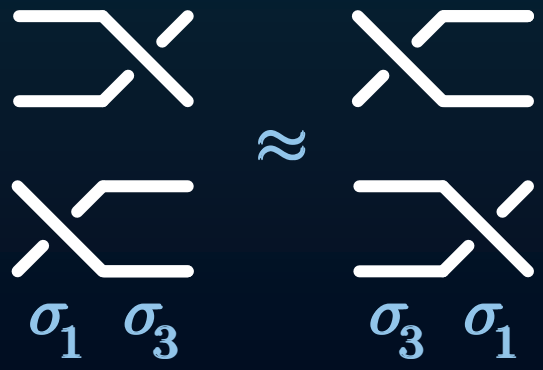
• Théorème (Artin): Le groupe de tresses B_n est engendré par $\sigma_1, \ldots, \sigma_{n-1}$, soumis aux relations

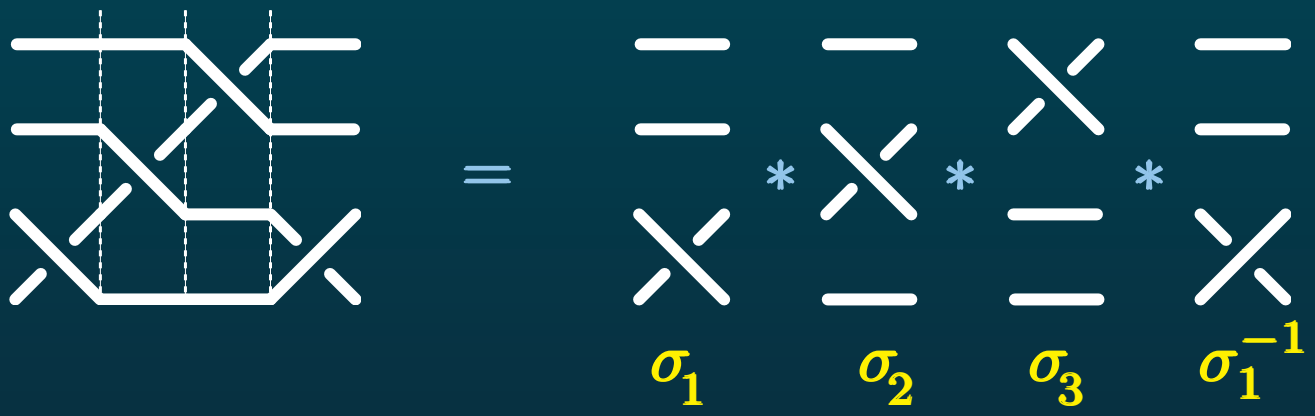
$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ pour } |i-j| \geqslant 2, \text{ et } \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ pour } |i-j| = 1.$$



• Théorème (Artin): Le groupe de tresses B_n est engendré par $\sigma_1, \ldots, \sigma_{n-1}$, soumis aux relations

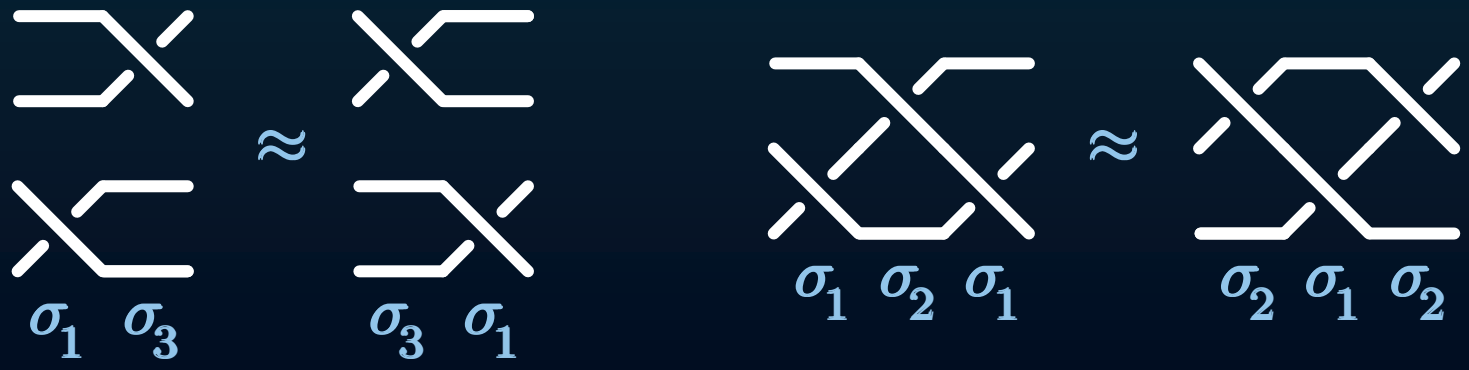
$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ pour } |i-j| \geqslant 2, \text{ et } \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ pour } |i-j| = 1.$$





• Théorème (Artin): Le groupe de tresses B_n est engendré par $\sigma_1, \ldots, \sigma_{n-1}$, soumis aux relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{pour } |i-j| \geqslant 2, \quad \text{et} \quad \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \quad \text{pour } |i-j| = 1.$$



- Le problème d'isotopie des tresses:

- Le problème d'isotopie des tresses:

  Reconnaître si un diagramme de tresse est isotope au diagramme trivial

$\Leftrightarrow$ Reconnaître si un mot de tresse w représente 1 dans le groupe des tresses.

- Le problème d'isotopie des tresses:
  Reconnaître si un diagramme de tresse est isotope au diagramme trivial

$\Leftrightarrow$ Reconnaître si un mot de tresse w représente 1 dans le groupe des tresses.

$\rightsquigarrow$ Problème #0 pour des applications, par ex. cryptographiques

- Le problème d'isotopie des tresses:

  Reconnaître si un diagramme de tresse est isotope au diagramme trivial

$\Leftrightarrow$ Reconnaître si un mot de tresse w représente 1 dans le groupe des tresses.

$\rightsquigarrow$ Problème #0 pour des applications, par ex. cryptographiques

- Dans un groupe libre, w représente 1 ssi

w se réduit au mot vide en détruisant itérativement les motifs xx^{-1} et $x^{-1}x$.

- Le problème d'isotopie des tresses:

  Reconnaître si un diagramme de tresse est isotope au diagramme trivial

$\Leftrightarrow$ Reconnaître si un mot de tresse w représente 1 dans le groupe des tresses.

$\rightsquigarrow$ Problème #0 pour des applications, par ex. cryptographiques

- Dans un groupe libre, w représente 1 ssi

w se réduit au mot vide en détruisant itérativement les motifs xx^{-1} et $x^{-1}x$.

- Ne marche pas dans un groupe non libre:

$\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ représente 1 dans B_n, mais

ne contient aucun $\sigma_i\sigma_i^{-1}$ ou $\sigma_i^{-1}\sigma_i$.

- Le problème d'isotopie des tresses:
  Reconnaître si un diagramme de tresse est isotope au diagramme trivial
  $\Leftrightarrow$ Reconnaître si un mot de tresse w représente 1 dans le groupe des tresses.

$\rightsquigarrow$ Problème #0 pour des applications, par ex. cryptographiques

- Dans un groupe libre, w représente 1 ssi
  w se réduit au mot vide en détruisant itérativement les motifs xx^{-1} et $x^{-1}x$.

- Ne marche pas dans un groupe non libre:
  $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ représente 1 dans B_n, mais
  ne contient aucun $\sigma_i\sigma_i^{-1}$ ou $\sigma_i^{-1}\sigma_i$.

$\rightsquigarrow$ Question: Peut-il exister une réduction pour B_n?

... oui, la réduction des poignées.

... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

... oui, la réduction des poignées.

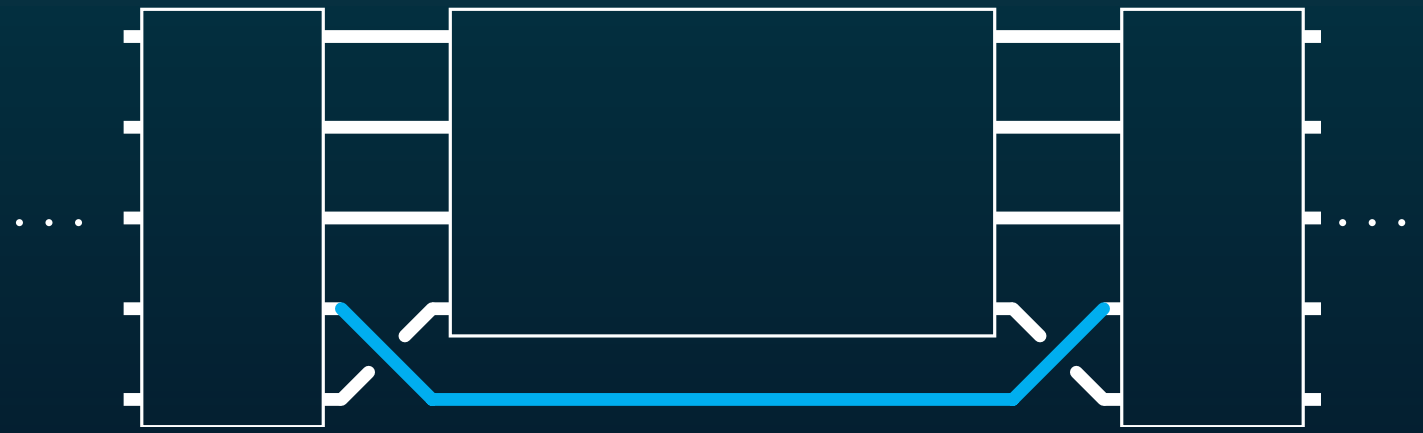
- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.

... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.

... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.

... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.

... oui, la réduction des poignées.

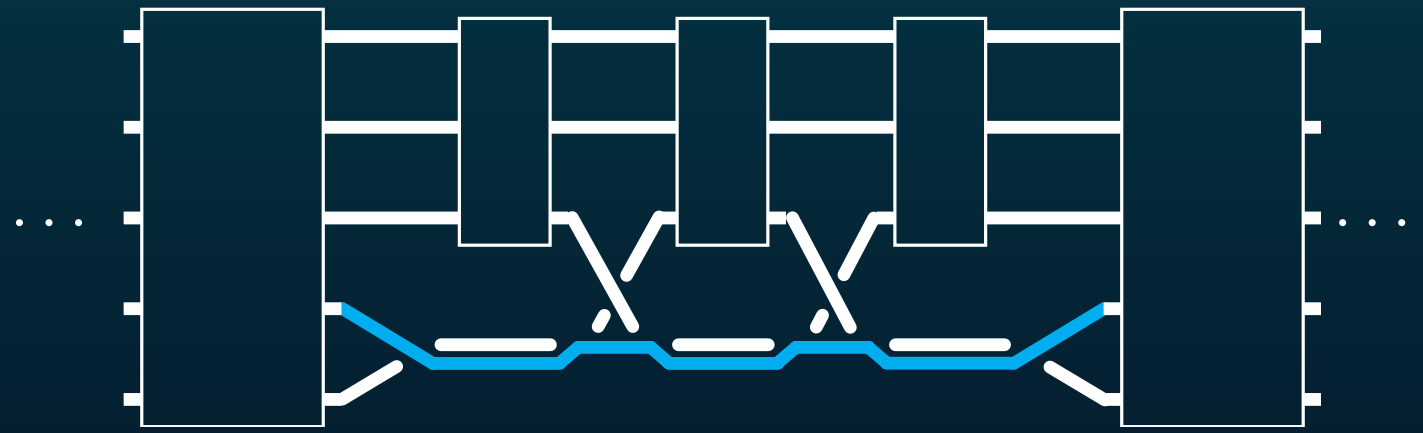
- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.

... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

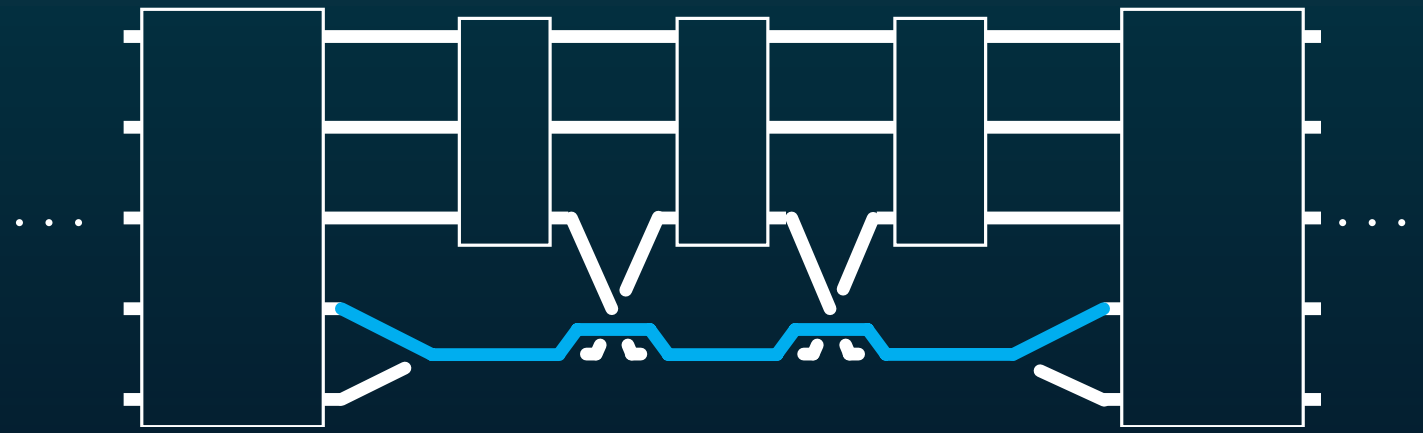
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

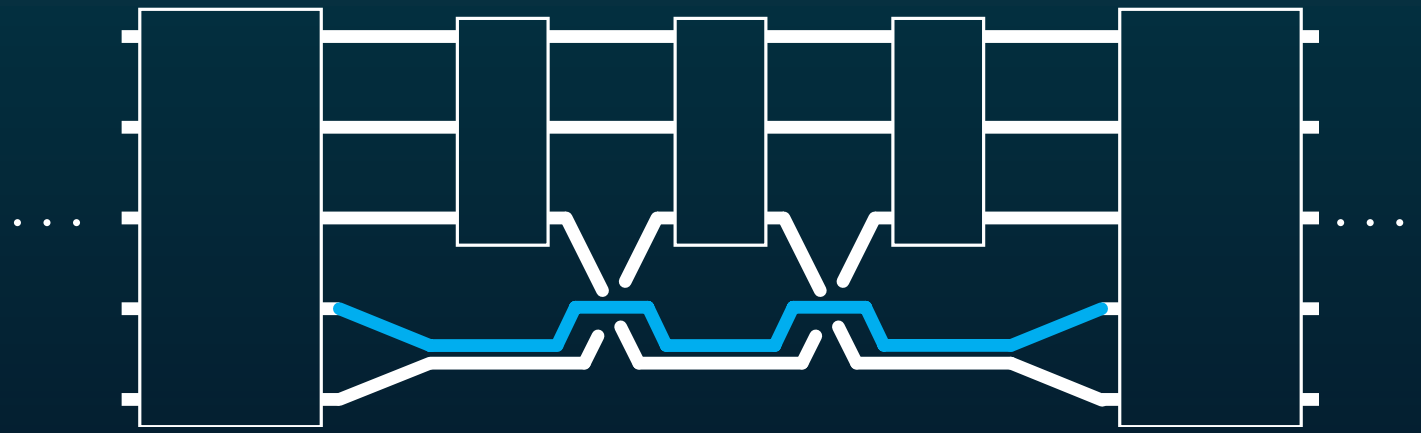
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

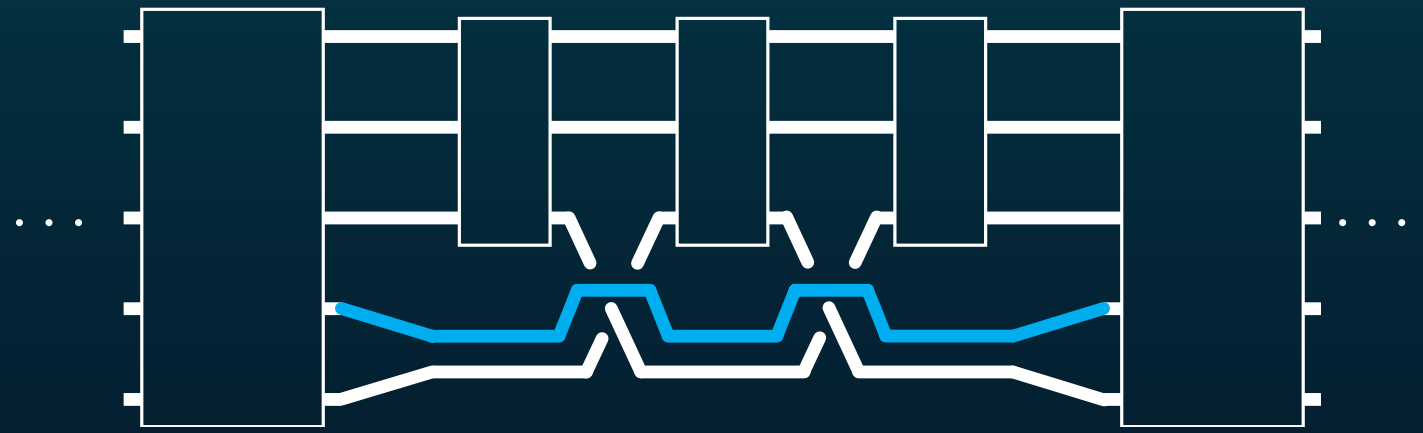
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

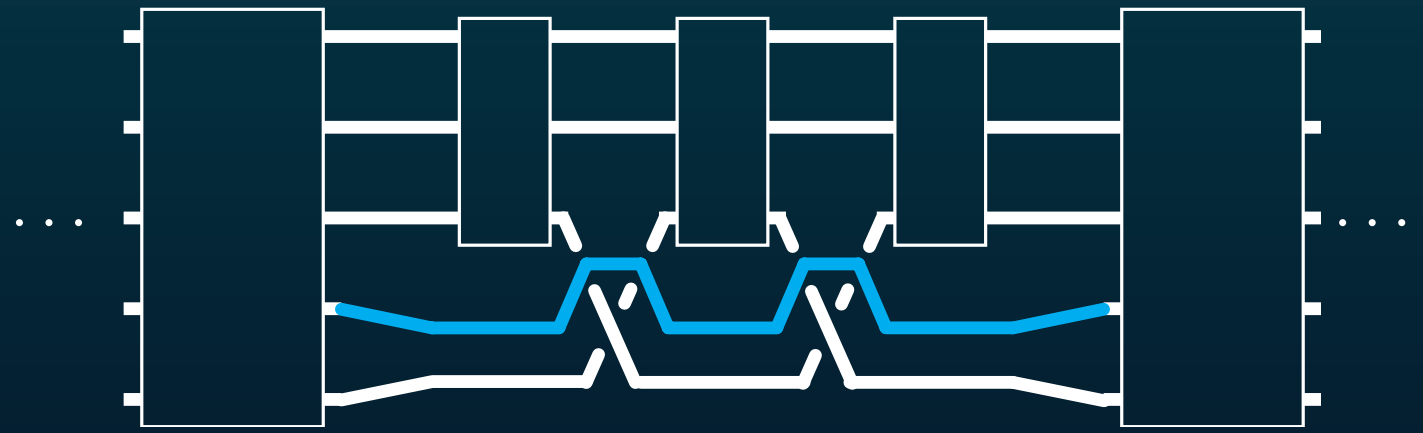
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

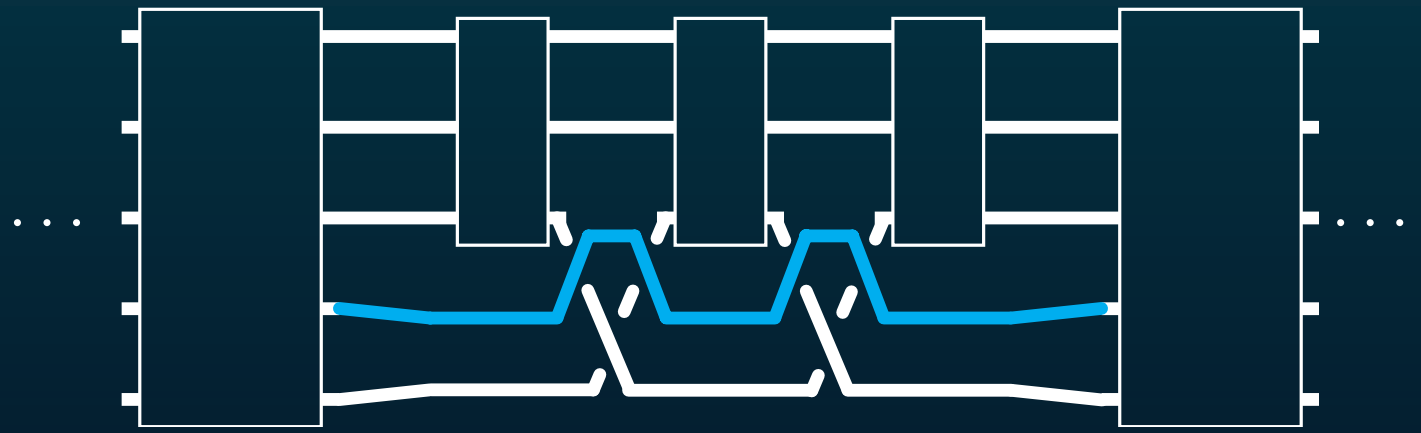
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

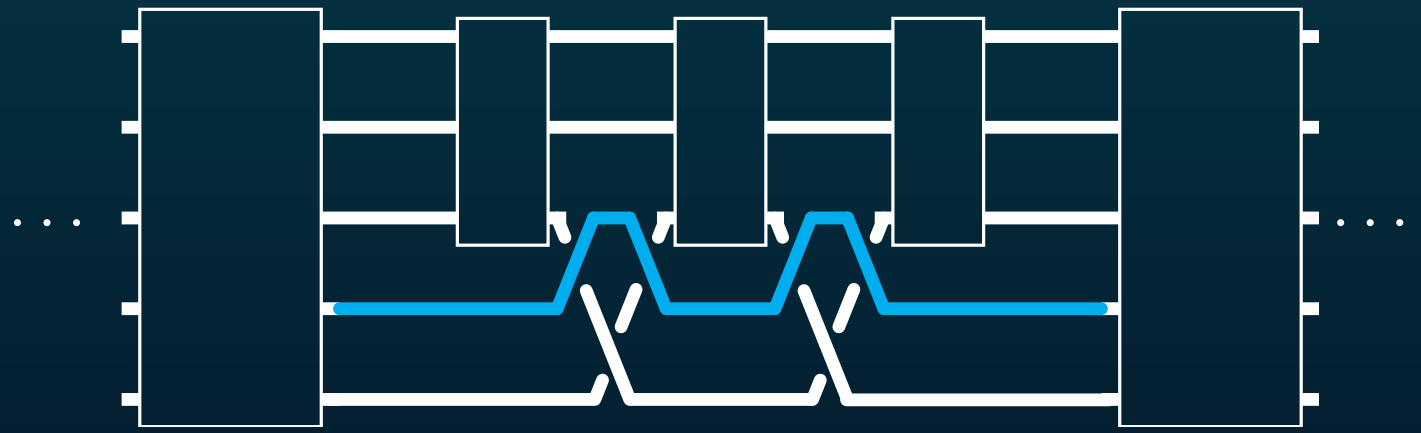
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

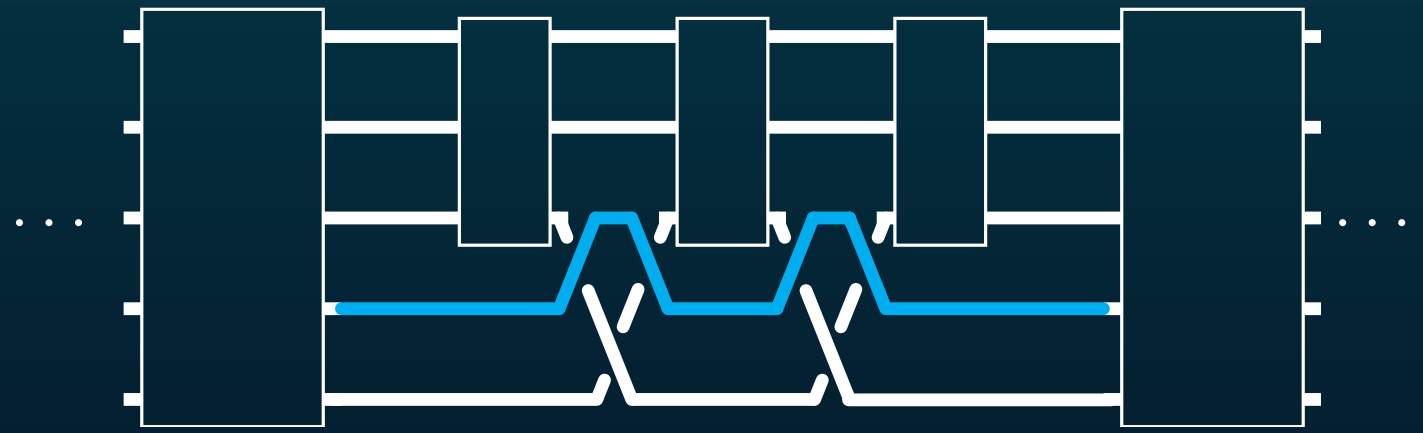
  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



... oui, la réduction des poignées.

- Le mot $\sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ contient $\sigma_1\sigma_2^{-1}\sigma_1^{-1}$

  ⇝ un sous-mot $\sigma_1 \ldots \sigma_1^{-1}$ sans $\sigma_1^{\pm 1}$ au milieu: une σ_1 -poignée.



- Définition: Réduire une σ_1 -poignée $\sigma_1^e w \sigma_1^{-e}$:

  - détruire les $\sigma_1^{\pm 1}$ du début et de la fin,
  - remplacer chaque $\sigma_2^{\pm 1}$ de w par $\sigma_2^{-e}\sigma_1^{\pm 1}\sigma_2^{e}$.

- Faits: - La réduction d'une poignée est une isotopie;

- Faits: - La réduction d'une poignée est une isotopie;
  - Elle étend la réduction des groupes libres;

- Faits: - La réduction d'une poignée est une isotopie;
  - Elle étend la réduction des groupes libres;
  - Les mots irréductibles sont ceux qui ne contiennent pas σ_1 et σ_1^{-1}.

- Faits: - La réduction d'une poignée est une isotopie;
  - Elle étend la réduction des groupes libres;
  - Les mots irréductibles sont ceux qui ne contiennent pas σ_1 et σ_1^{-1}.

- Théorème 1: (D. 1995) La réduction des poignées se termine en un nombre fini d'étapes. Un mot de tresse représente 1 ssi il se réduit au mot vide.

- Faits: - La réduction d'une poignée est une isotopie;
  - Elle étend la réduction des groupes libres;
  - Les mots irréductibles sont ceux qui ne contiennent pas σ_1 et σ_1^{-1}.

- Théorème 1: (D. 1995) La réduction des poignées se termine en un nombre fini d'étapes. Un mot de tresse représente 1 ssi il se réduit au mot vide.

- Règle supplémentaire: réduire d'abord les poignées enchâssées.
- Extrêmement efficace en pratique;

  $\rightsquigarrow$ adapté aux applications cryptographiques.

- Faits: - La réduction d'une poignée est une isotopie;
  - Elle étend la réduction des groupes libres;
  - Les mots irréductibles sont ceux qui ne contiennent pas σ_1 et σ_1^{-1}.

- Théorème 1: (D. 1995) La réduction des poignées se termine en un nombre fini d'étapes. Un mot de tresse représente 1 ssi il se réduit au mot vide.

- Règle supplémentaire: réduire d'abord les poignées enchâssées.
- Extrêmement efficace en pratique;

  ⇝ adapté aux applications cryptographiques.

⇝ Question: D'où vient cette réduction, et pourquoi fonctionne-t-elle?

L'ORDRE DES TRESSES

... à cause de l'ordre des tresses.

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

σ_i apparaît, mais σ_i^{-1} n'apparaît pas

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

σ_i apparaît, mais σ_i^{-1} n'apparaît pas

• Deux ingrédients:

- (A): Un mot de tresse contenant σ_1 et pas σ_1^{-1} ne représente pas 1;

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

σ_i apparaît, mais σ_i^{-1} n'apparaît pas

• Deux ingrédients:

- (A): Un mot de tresse contenant σ_1 et pas σ_1^{-1} ne représente pas 1;
- (C): Toute tresse peut être représentée par un mot sans σ_1 ou sans σ_1^{-1}.

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

σ_i apparaît, mais σ_i^{-1} n'apparaît pas

• Deux ingrédients:

- (A): Un mot de tresse contenant σ_1 et pas σ_1^{-1} ne représente pas 1;
- (C): Toute tresse peut être représentée par un mot sans σ_1 ou sans σ_1^{-1}.

• Théo. 1 vient de Théo. 2:

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

σ_i apparaît, mais σ_i^{-1} n'apparaît pas

• Deux ingrédients:

- (A): Un mot de tresse contenant σ_1 et pas σ_1^{-1} ne représente pas 1;
- (C): Toute tresse peut être représentée par un mot sans σ_1 ou sans σ_1^{-1}.

• Théo. 1 vient de Théo. 2: (C) donne l'idée et (A) la convergence : quelque chose décroît décroît pour $<$ quand une réduction est effectuée.

... à cause de l'ordre des tresses.

• Théorème 2: (D. 1992) Pour a, b dans B_n, déclarons $a < b$ si $a^{-1}b$ peut être représenté par un mot dans lequel le générateur σ_i d'indice minimal apparaît seulement positivement. Alors $<$ est un ordre total sur B_n.

σ_i apparaît, mais σ_i^{-1} n'apparaît pas

• Deux ingrédients:

- (A): Un mot de tresse contenant σ_1 et pas σ_1^{-1} ne représente pas 1;
- (C): Toute tresse peut être représentée par un mot sans σ_1 ou sans σ_1^{-1}.

• Théo. 1 vient de Théo. 2: (C) donne l'idée et (A) la convergence : quelque chose décroît décroît pour $<$ quand une réduction est effectuée.

⇝ Question: D'où vient l'ordre des tresses?

... de l'étude de l'auto-distributivité.

... de l'étude de l'auto-distributivité.

• Colorier les tresses : choisir un ensemble ("couleurs") S, attribuer des couleurs aux extrémités gauches des brins d'un diagramme, propager les couleurs vers la droite. Comparer les couleurs initiales et finales.

... de l'étude de l'auto-distributivité.

• Colorier les tresses : choisir un ensemble ("couleurs") S, attribuer des couleurs aux extrémités gauches des brins d'un diagramme, propager les couleurs vers la droite. Comparer les couleurs initiales et finales.

• Choix 1 : les couleurs ne changent pas lors des croisements.

... de l'étude de l'auto-distributivité.

• Colorier les tresses : choisir un ensemble ("couleurs") S, attribuer des couleurs aux extrémités gauches des brins d'un diagramme, propager les couleurs vers la droite. Comparer les couleurs initiales et finales.

• Choix 1 : les couleurs ne changent pas aux croisements :

$\rightsquigarrow$ permutation des couleurs $\rightsquigarrow$ $B_n \twoheadrightarrow S_n$.

... de l'étude de l'auto-distributivité.

• Colorier les tresses : choisir un ensemble ("couleurs") S, attribuer des couleurs aux extrémités gauches des brins d'un diagramme, propager les couleurs vers la droite. Comparer les couleurs initiales et finales.

• Choix 1 : les couleurs ne changent pas aux croisements :

$\rightsquigarrow$ permutation des couleurs $\rightsquigarrow$ $B_n \twoheadrightarrow S_n$.

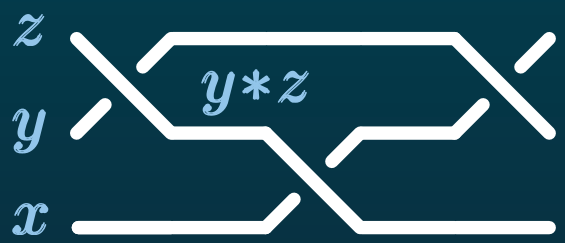
• Choix 2 : (Joyce, Matveev, Brieskorn, ...) Les couleurs changent suivant

où $*$ est une certaine opération binaire sur S

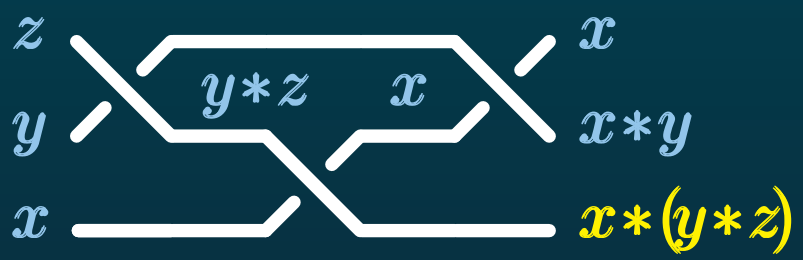
- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:

- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:

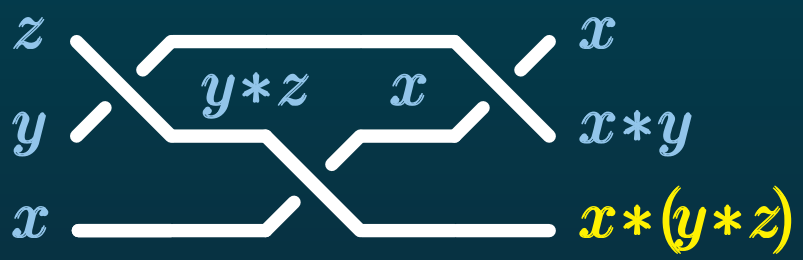
- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:

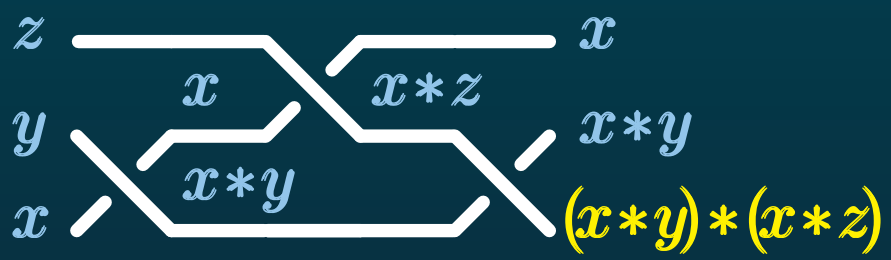


- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:

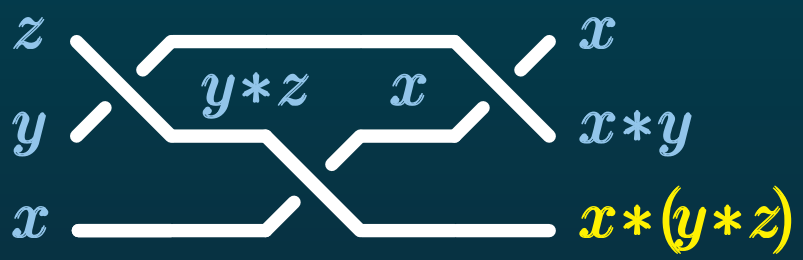


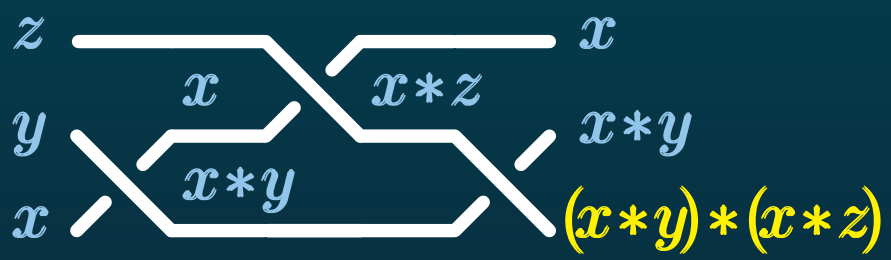
- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:





- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:

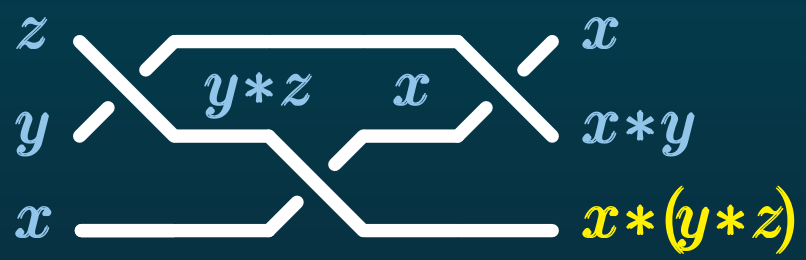


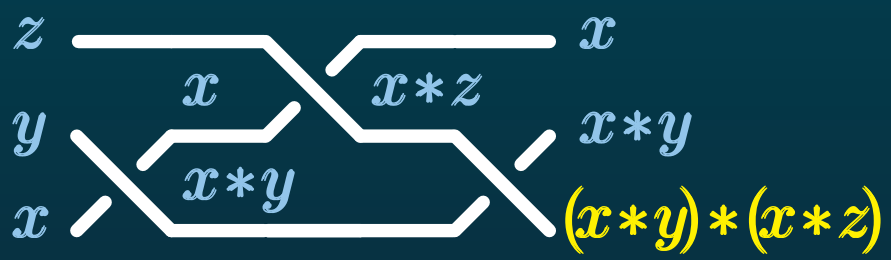


⇝ S doit être un LD-système, c'est-à-dire satisfaire la loi d'autodistributivité:

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(LD)}$$

- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:



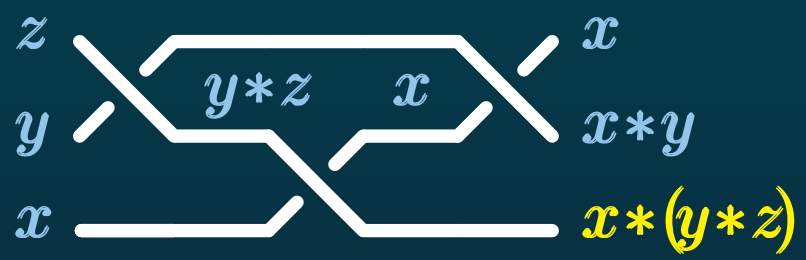


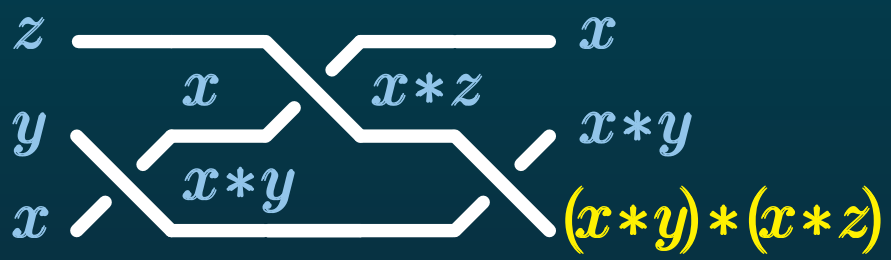
$\rightsquigarrow$ S doit être un LD-système, c'est-à-dire satisfaire la loi d'autodistributivité:

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(LD)}$$

- Exemples standards :
  - $x * y = y$, mène à $B_n \twoheadrightarrow S_n$.

- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:



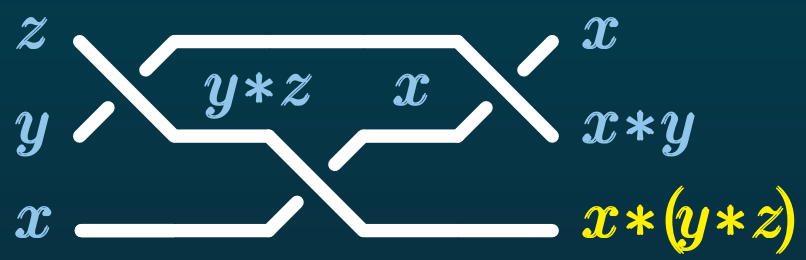


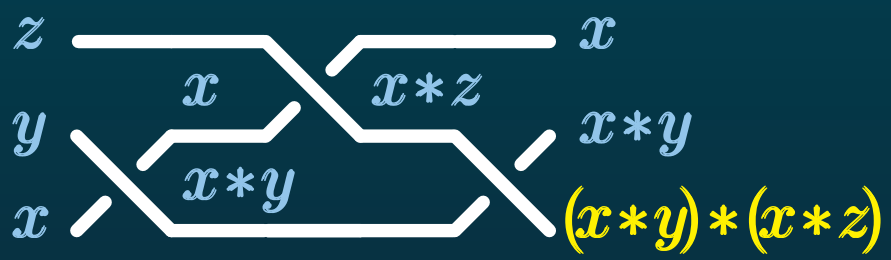
⇝ S doit être un LD-système, c'est-à-dire satisfaire la loi d'autodistributivité:

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(LD)}$$

- Exemples standards :
  - $x * y = y$, mène à $B_n \twoheadrightarrow S_n$.
  - $x * y = xyx^{-1}$, mène à $B_n \hookrightarrow Aut(F_n)$ (Artin)

- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:



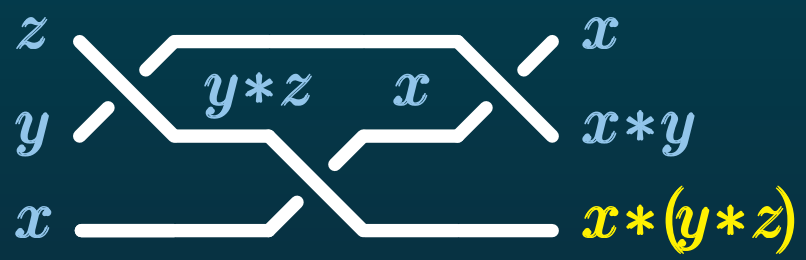


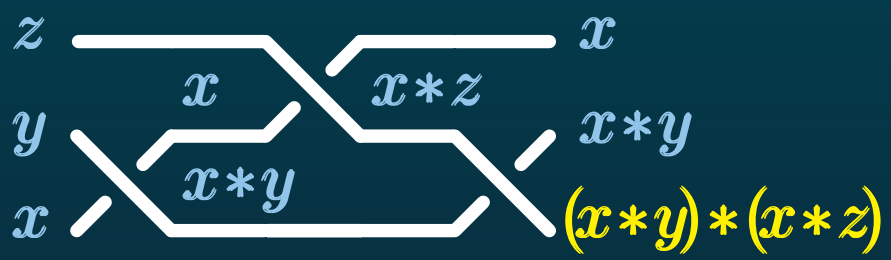
$\rightsquigarrow$ S doit être un LD-système, c'est-à-dire satisfaire la loi d'autodistributivité:

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(LD)}$$

- Exemples standards :
  - $x * y = y$, mène à $B_n \twoheadrightarrow S_n$.
  - $x * y = xyx^{-1}$, mène à $B_n \hookrightarrow Aut(F_n)$ (Artin)
  - $x * y = (1-t)x + ty$, mène à $B_n \to GL_n(\mathbb{Z}[t, t^{-1}])$ (Burau)

- Pour une action de B_n sur S^n, compatibilité avec les relations de tresse:





$\rightsquigarrow$ S doit être un LD-système, c'est-à-dire satisfaire la loi d'autodistributivité:

$$x * (y * z) = (x * y) * (x * z) \qquad \text{(LD)}$$

- Exemples standards :
  - $x * y = y$, mène à $B_n \twoheadrightarrow S_n$.
  - $x * y = xyx^{-1}$, mène à $B_n \hookrightarrow Aut(F_n)$ (Artin)
  - $x * y = (1-t)x + ty$, mène à $B_n \to GL_n(\mathbb{Z}[t, t^{-1}])$ (Burau)

Note: dans ces exemples, on a toujours $x * x = x$.

⇝ Autres exemples?

⇝ Autres exemples?

- Déclarons un LD-système $(S, *)$ ordonnable si
  il existe un ordre total $<$ sur S satisfaisant $x < x * y$ pour tous x, y.
  ⇝ certainement d'un type très différent des précédents : $x < x * x \neq x$.

⇝ Autres exemples?

- Déclarons un LD-système $(S, *)$ ordonnable si
  il existe un ordre total $<$ sur S satisfaisant $x < x * y$ pour tous x, y.
  ⇝ certainement d'un type très différent des précédents : $x < x * x \neq x$.

- Théorème 3: (D. 1991) Il existe des LD-systèmes ordonnables (à savoir les LD-systèmes libres).

⇝ Autres exemples?

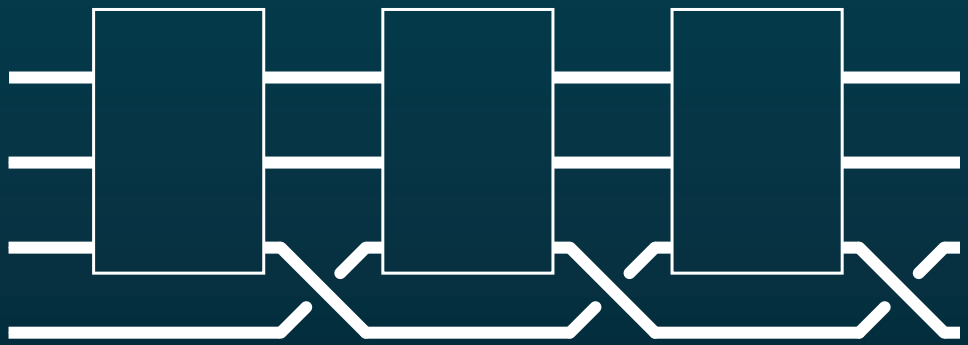
• Déclarons un LD-système $(S, *)$ ordonnable si
il existe un ordre total $<$ sur S satisfaisant $x < x * y$ pour tous x, y.
⇝ certainement d'un type très différent des précédents : $x < x * x \neq x$.

• Théorème 3: (D. 1991) Il existe des LD-systèmes ordonnables (à savoir les LD-systèmes libres).

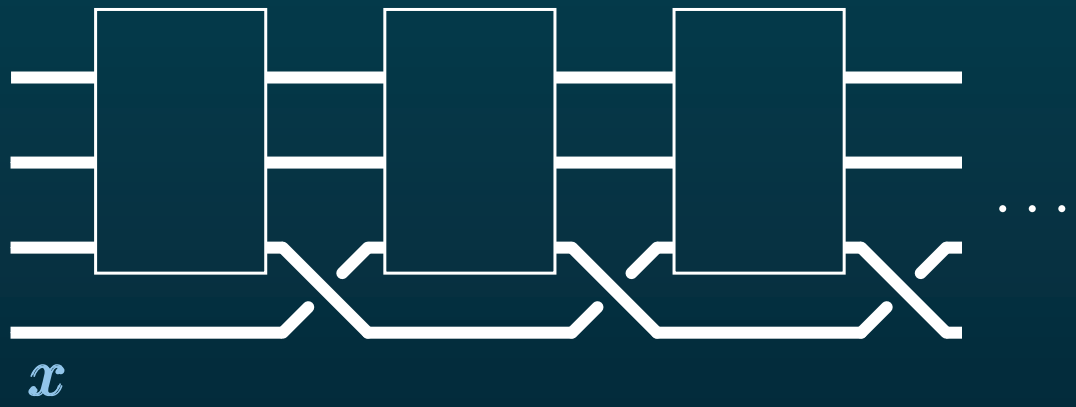
• Théo. 2 vient de Théo. 3 : Utiliser un LD-système ordonnable pour colorier les tresses. Les points importants sont :
- (A): Un mot de tresse contenant σ_1 et pas σ_1^{-1} ne représente pas 1,
- (C): Caractère total de l'ordre.

- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1

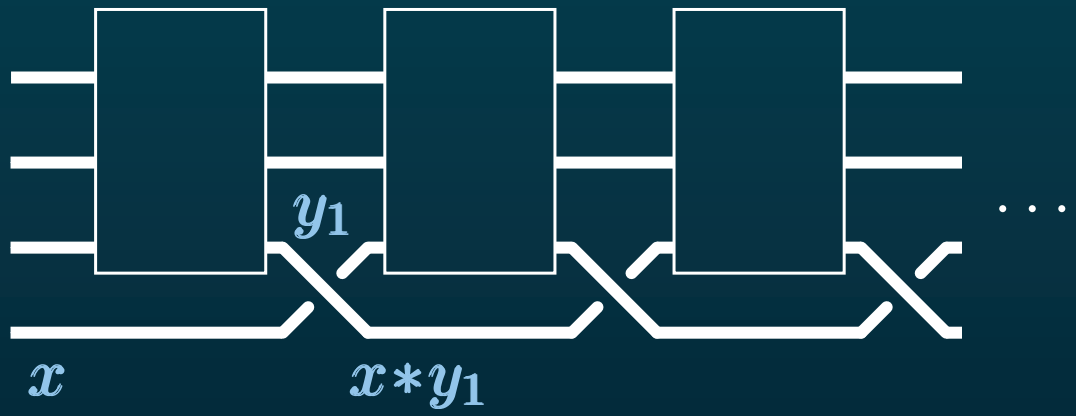
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



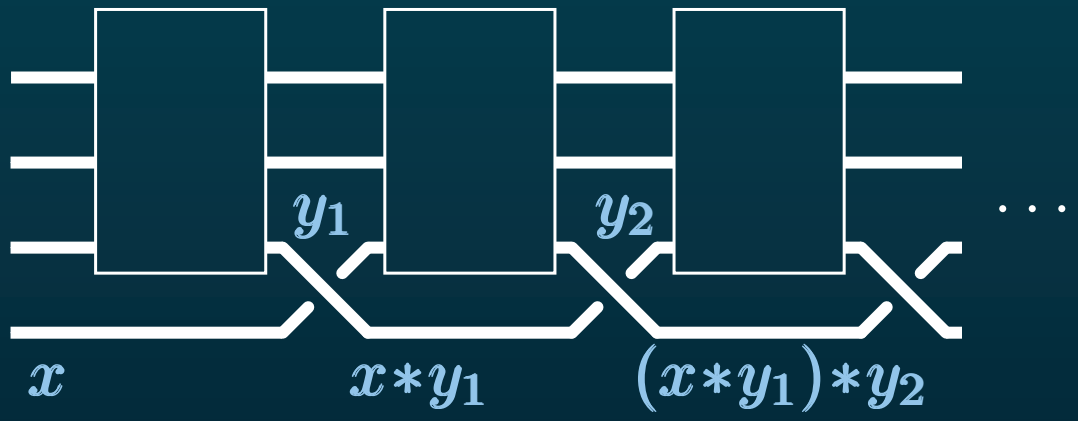
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



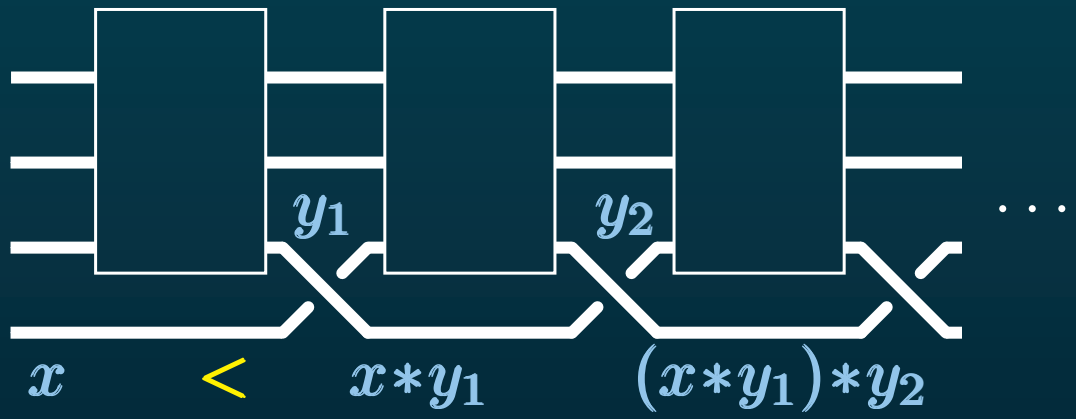
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



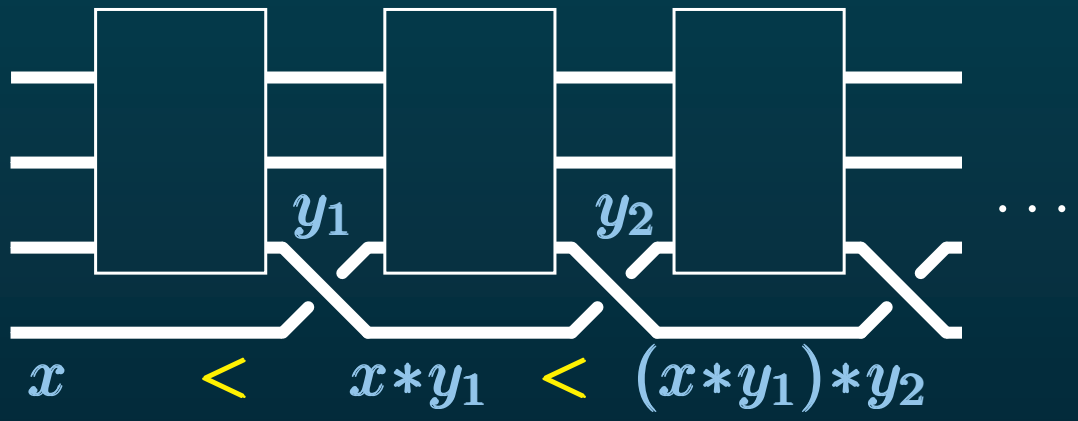
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



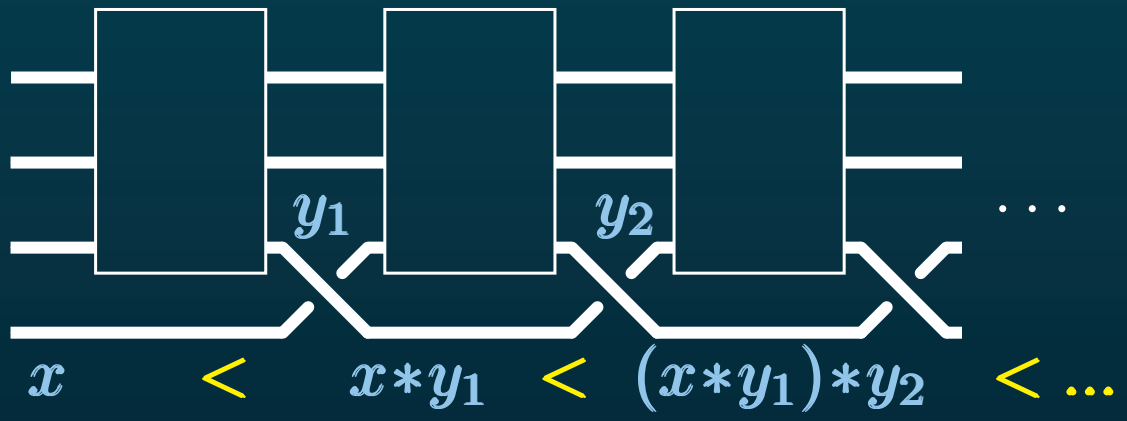
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



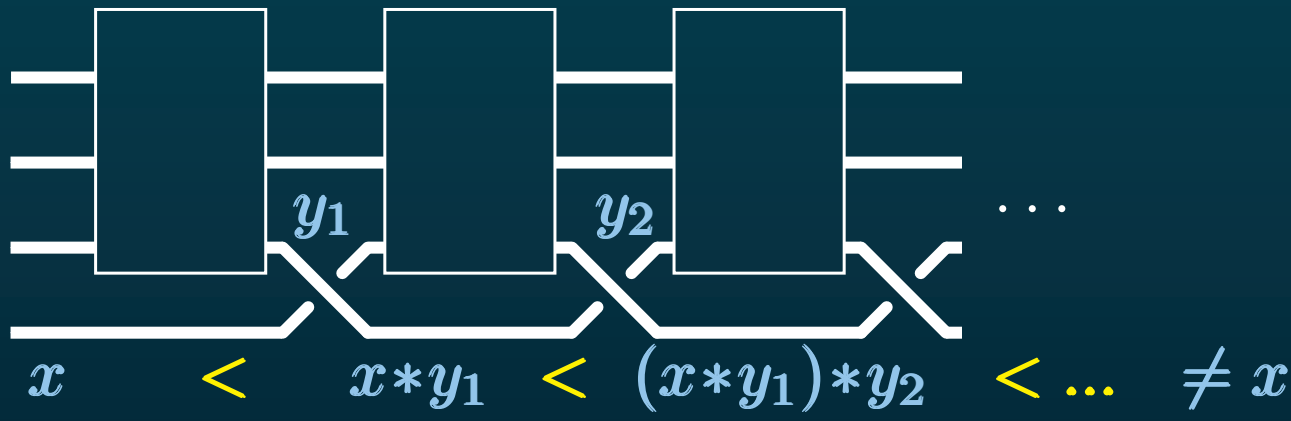
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



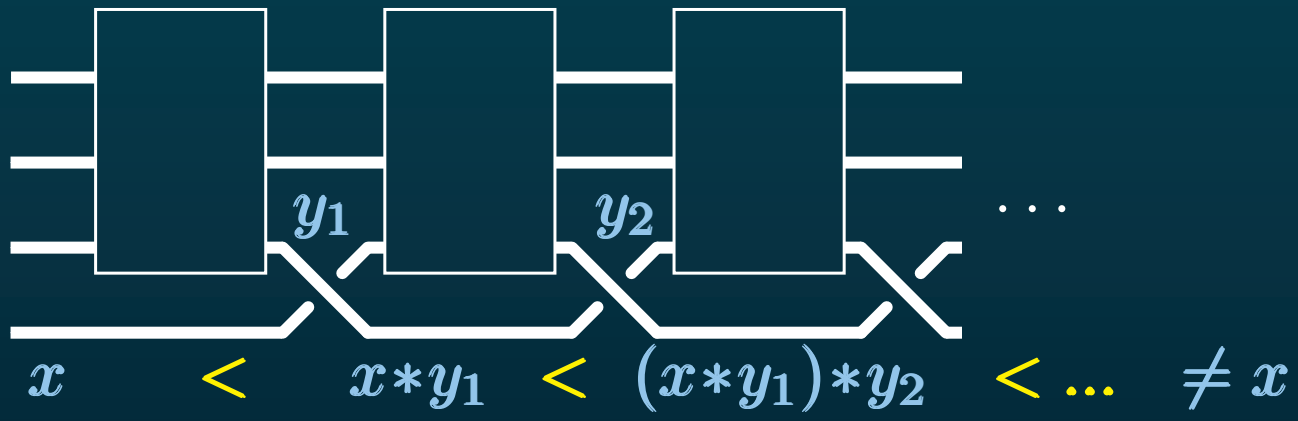
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1

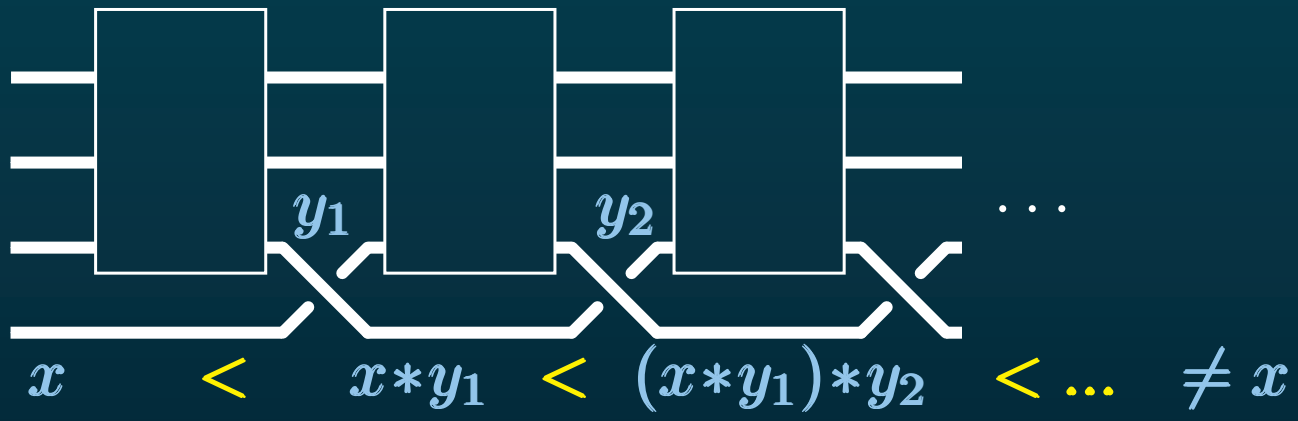


- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1

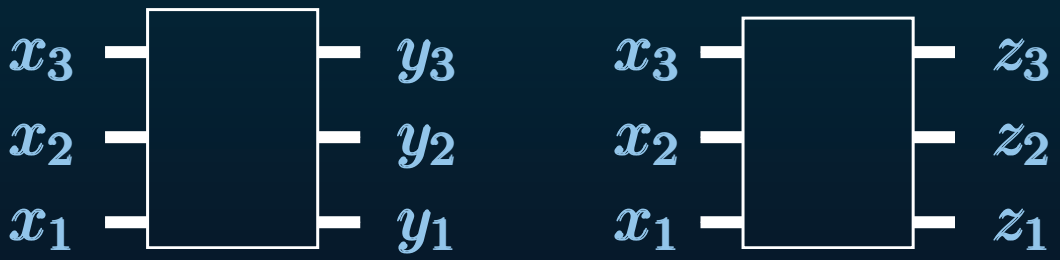


- Propriété (C) : Un ordre total sur les tresses :

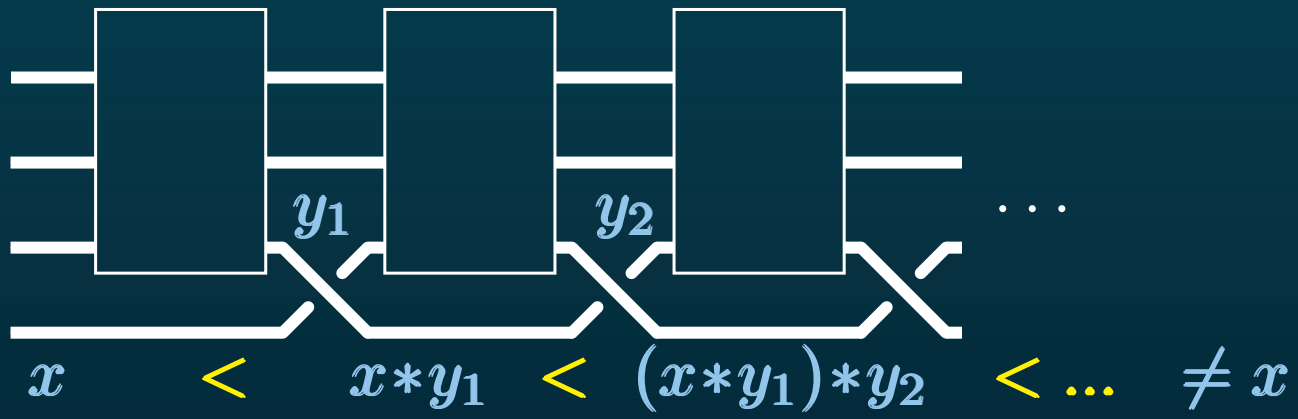
- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



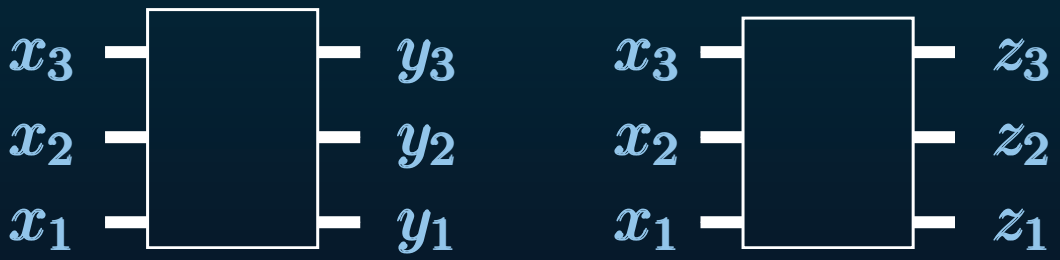
- Propriété (C) : Un ordre total sur les tresses :



- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1

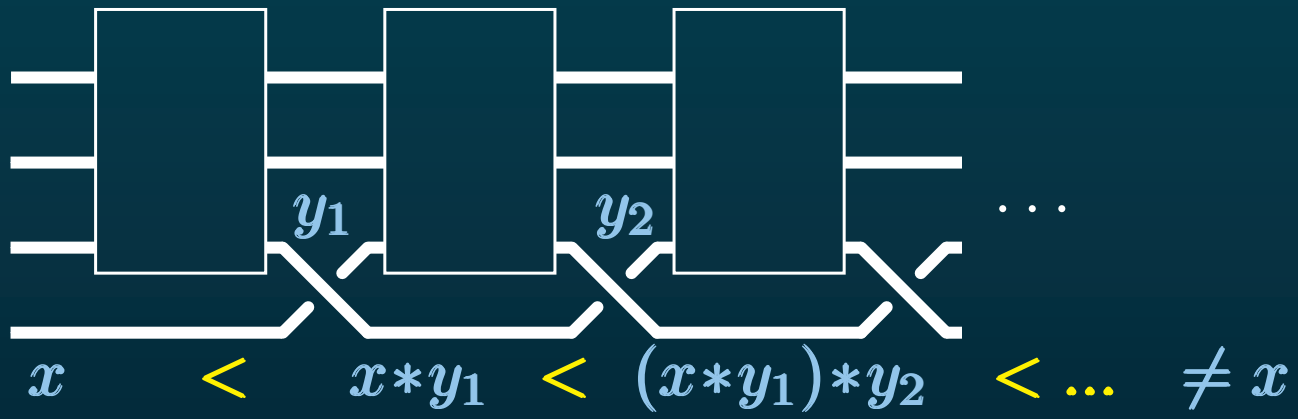


- Propriété (C) : Un ordre total sur les tresses :

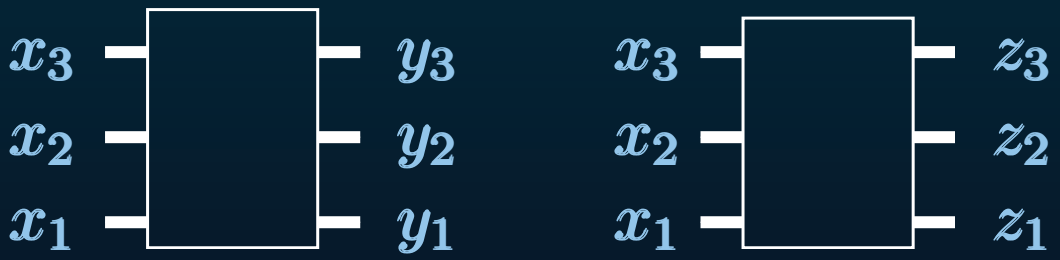


⇝ Comparer $(y_1, y_2, ...)$ et $(z_1, z_2, ...)$ suivant l'ordre lexicographique.

- Propriété (A) : un mot contenant σ_1 et pas σ_1^{-1} ne représente pas 1



- Propriété (C) : Un ordre total sur les tresses :



⇝ Comparer $(y_1, y_2, ...)$ et $(z_1, z_2, ...)$ suivant l'ordre lexicographique.

⇝ Question: Pourquoi étudier les LD-systèmes ordonnables?

... parce que la théorie des ensembles le dit

... parce que la théorie des ensembles le dit

- La théorie des ensembles étudie la notion d'infini. D'après le théorème de Gödel, tout système axiomatique, en particulier ZF, est incomplet.

... parce que la théorie des ensembles le dit

- La théorie des ensembles étudie la notion d'infini. D'après le théorème de Gödel, tout système axiomatique, en particulier ZF, est incomplet.

  ⇝ programme de Gödel : compléter ZF à l'aide d'axiomes affirmant l'existence d'ensembles "hyper-infinis" (grands cardinaux).

... parce que la théorie des ensembles le dit

- La théorie des ensembles étudie la notion d'infini. D'après le théorème de Gödel, tout système axiomatique, en particulier ZF, est incomplet.

  ⇝ programme de Gödel : compléter ZF à l'aide d'axiomes affirmant l'existence d'ensembles "hyper-infinis" (grands cardinaux).

- Renforcer la définition "X est infini ssi $\exists j : X \to X$ injective non surjective" en "X est hyper-infini (auto-similaire) ssi $\exists j$ ... et, de plus, j préserve tout ce qui est définissable à partir de $\in$ (plongement élémentaire)".

... parce que la théorie des ensembles le dit

• La théorie des ensembles étudie la notion d'infini. D'après le théorème de Gödel, tout système axiomatique, en particulier ZF, est incomplet.

⇝ programme de Gödel : compléter ZF à l'aide d'axiomes affirmant l'existence d'ensembles "hyper-infinis" (grands cardinaux).

• Renforcer la définition "X est infini ssi $\exists j : X \to X$ injective non surjective" en "X est hyper-infini (auto-similaire) ssi $\exists j$ ... et, de plus, j préserve tout ce qui est définissable à partir de $\in$ (plongement élémentaire)".

• Comme $j : n \mapsto n+1$ est injective non surjective, $\mathbb{N}$ est infini ;

... parce que la théorie des ensembles le dit

• La théorie des ensembles étudie la notion d'infini. D'après le théorème de Gödel, tout système axiomatique, en particulier ZF, est incomplet.

⇝ programme de Gödel : compléter ZF à l'aide d'axiomes affirmant l'existence d'ensembles "hyper-infinis" (grands cardinaux).

• Renforcer la définition "X est infini ssi $\exists j : X \to X$ injective non surjective" en "X est hyper-infini (auto-similaire) ssi $\exists j$ ... et, de plus, j préserve tout ce qui est définissable à partir de $\in$ (plongement élémentaire)".

• Comme $j : n \mapsto n+1$ est injective non surjective, $\mathbb{N}$ est infini ;
Or j préserve $<$, mais pas $+$: j n'est pas un p.é. ;
En fait, il n'existe pas de p.é. sur $\mathbb{N}$: $\mathbb{N}$ n'est pas auto-similaire.

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

  - “Etre un p.é.” est définissable à partir de $\in$, donc $i(j)$ est un p.é.

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

  - "Etre un p.é." est définissable à partir de $\in$, donc $i(j)$ est un p.é.

    $\rightsquigarrow$ une opération binaire sur les p.é. de R;

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

  - "Etre un p.é." est définissable à partir de $\in$, donc $i(j)$ est un p.é.
    $\rightsquigarrow$ une opération binaire sur les p.é. de R;

  - "Etre l'image de" est définissable à partir de $\in$,
    donc $\ell = j(k)$ implique $i(\ell) = i(j)(i(k))$, i.e., $i(j(k)) = i(j)(i(k))$.

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

  - "Etre un p.é." est définissable à partir de $\in$, donc $i(j)$ est un p.é.
    $\rightsquigarrow$ une opération binaire sur les p.é. de R;

  - "Etre l'image de" est définissable à partir de $\in$,
    donc $\ell = j(k)$ implique $i(\ell) = i(j)(i(k))$, i.e., $i(j(k)) = i(j)(i(k))$.
    $\rightsquigarrow$ l'opération binaire sur les p.é. est auto-distributive.

- Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

- Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

  - "Etre un p.é." est définissable à partir de $\in$, donc $i(j)$ est un p.é.
    $\rightsquigarrow$ une opération binaire sur les p.é. de R;

  - "Etre l'image de" est définissable à partir de $\in$,
    donc $\ell = j(k)$ implique $i(\ell) = i(j)(i(k))$, i.e., $i(j(k)) = i(j)(i(k))$.
    $\rightsquigarrow$ l'opération binaire sur les p.é. est auto-distributive.

$\rightsquigarrow$ Pour chaque p.é. j, un LD-système $I(j)$, les itérés de j : $j(j)$, $j(j)(j)$...

• Un rang est un ensemble R (étrange) t.q. $f : R \to R$ entraîne $f \in R$. (??)

• Si i, j sont des p.é. d'un rang auto-similaire R, on peut appliquer i à j.

- "Etre un p.é." est définissable à partir de $\in$, donc $i(j)$ est un p.é.
  ⇝ une opération binaire sur les p.é. de R;

- "Etre l'image de" est définissable à partir de $\in$,
  donc $\ell = j(k)$ implique $i(\ell) = i(j)(i(k))$, i.e., $i(j(k)) = i(j)(i(k))$.
  ⇝ l'opération binaire sur les p.é. est auto-distributive.

⇝ Pour chaque p.é. j, un LD-système $I(j)$, les itérés de j: $j(j)$, $j(j)(j)$...

• Proposition: (D. 1986) Si j est un p.é. d'un rang autosimilaire, la LD-structure de $I(j)$ entraîne la Π^1_1-détermination. ⇝ "$I(j)$ est non trivial."

UNE SITUATION ETRANGE

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

décider si deux termes sont équivalents modulo LD

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Corollaire: S'il existe un rang autosimilaire, alors le problème de mot de LD est résoluble algorithmiquement.

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Corollaire: S'il existe un rang autosimilaire, alors le problème de mot de LD est résoluble algorithmiquement.

- Mais l'existence d'un rang autosimilaire est un axiome indémontrable

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  ↖ décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Corollaire: S'il existe un rang autosimilaire, alors le problème de mot de LD est résoluble algorithmiquement.

- Mais l'existence d'un rang autosimilaire est un axiome indémontrable

  ⇝ Le corollaire n'est pas une solution au problème de mot de LD

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  ↖ décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Corollaire: S'il existe un rang autosimilaire, alors le problème de mot de LD est résoluble algorithmiquement.

- Mais l'existence d'un rang autosimilaire est un axiome indémontrable
  - ⇝ Le corollaire n'est pas une solution au problème de mot de LD
    - ⇝ Construire un vrai exemple de LD-système ordonnable

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  ↖ décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Corollaire: S'il existe un rang autosimilaire, alors le problème de mot de LD est résoluble algorithmiquement.

- Mais l'existence d'un rang autosimilaire est un axiome indémontrable
  - ⇝ Le corollaire n'est pas une solution au problème de mot de LD
    - ⇝ Construire un vrai exemple de LD-système ordonnable
      - ⇝ Th. 3 ("$\exists$ LD-système ordonnable") via groupe de géométrie de LD

- Théorème: (D. 1989) S'il existe au moins un LD-système ordonnable, alors le problème de mot de LD est résoluble algorithmiquement.

  ↖ décider si deux termes sont équivalents modulo LD

- Théorème: (Laver, 1989) Si j est un p.é. d'un rang autosimilaire, alors le LD-système $I(j)$ est ordonnable.

- Corollaire: S'il existe un rang autosimilaire, alors le problème de mot de LD est résoluble algorithmiquement.

- Mais l'existence d'un rang autosimilaire est un axiome indémontrable
  - ⇝ Le corollaire n'est pas une solution au problème de mot de LD
    - ⇝ Construire un vrai exemple de LD-système ordonnable
      - ⇝ Th. 3 ("∃ LD-système ordonnable") via groupe de géométrie de LD
        - ⇝ Comme G_{LD} est une extension de B_∞, applications aux tresses.

DES APPLICATIONS DE LA THEORIE DES ENSEMBLES?

- Un chemin continu de la théorie des ensembles aux groupes de tresses.

DES APPLICATIONS DE LA THEORIE DES ENSEMBLES?

⇝ Un chemin continu de la théorie des ensembles aux groupes de tresses.

- Question : S'agit-il d'applications de la théorie des ensembles?

DES APPLICATIONS DE LA THEORIE DES ENSEMBLES?

⇝ Un chemin continu de la théorie des ensembles aux groupes de tresses.

- Question : S'agit-il d'applications de la théorie des ensembles?

- Formellement, non : les tresses apparaissent
  quand les ensembles disparaissent :
  - La théorie des ensembles a donné un exemple (hypothétique) d'un objet
    (un LD-système ordonnable),
  - Les tresses et leur ordre apparaissent au cours de la construction
    d'un exemple alternatif (et "vrai").

DES APPLICATIONS DE LA THEORIE DES ENSEMBLES?

⇝ Un chemin continu de la théorie des ensembles aux groupes de tresses.

• Question : S'agit-il d'applications de la théorie des ensembles?

• Formellement, non : les tresses apparaissent
quand les ensembles disparaissent :
- La théorie des ensembles a donné un exemple (hypothétique) d'un objet (un LD-système ordonnable),
- Les tresses et leur ordre apparaissent au cours de la construction d'un exemple alternatif (et "vrai").

• Essentiellement, oui : si la théorie des ensembles n'avait pas montré que la loi LD est impliquée dans des phénomènes profonds et n'avait pas rendu l'existence de LD-systèmes ordonnables plausible, il est douteux qu'on ait cherché à construire de tels objets...

UNE ANALOGIE

• En physique : à partir d'une intuition ou d'une évidence physique, deviner un énoncé, puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables;

• En physique : à partir d'une intuition ou d'une évidence physique, deviner un énoncé, puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables;

• Ici : à partir d'une intuition logique (existence d'un rang autosimilaire), deviner un énoncé (existence d'un LD-système ordonnable), puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables.

• En physique : à partir d'une intuition ou d'une évidence physique, deviner un énoncé, puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables;

• Ici : à partir d'une intuition logique (existence d'un rang autosimilaire), deviner un énoncé (existence d'un LD-système ordonnable), puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables.

• Un argument en faveur de la théorie des ensembles : pour cet usage de la théorie, l'important n'est pas qu'un axiome soit plausible, mais qu'il soit puissant.

UNE ANALOGIE

• En physique : à partir d'une intuition ou d'une évidence physique, deviner un énoncé, puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables;

• Ici : à partir d'une intuition logique (existence d'un rang autosimilaire), deviner un énoncé (existence d'un LD-système ordonnable), puis le passer au mathématicien pour une démonstration formelle, débarrassée d'hypothèses indémontrées/ables.

• Un argument en faveur de la théorie des ensembles : pour cet usage de la théorie, l'important n'est pas qu'un axiome soit plausible, mais qu'il soit puissant.

⇝ Même si on ne croit pas à l'existence d'ensembles (hyper)-infinis, on doit reconnaître que, dans ce cas au moins, de tels objets ont pu mener à des mathématiques concrètes.

- Davantage sur l'ordre des tresses...

- Davantage sur l'ordre des tresses...
- Une autre application simillaire de la théorie des ensembles?

- Davantage sur l'ordre des tresses...
- Une autre application simillaire de la théorie des ensembles?
- Partir de

	1	2	...	N
1	2			
2	3			
$\vdots$				
$N-1$	N			
N	1			

et essayer de construire un LD-système.

- Davantage sur l'ordre des tresses...
- Une autre application simillaire de la théorie des ensembles?
- Partir de

	1	2	...	N
1	2			
2	3			
$\vdots$				
$N-1$	N			
N	1			

et essayer de construire un LD-système.

  - au plus une solution pour chaque N;

- Davantage sur l'ordre des tresses...
- Une autre application simillaire de la théorie des ensembles?
- Partir de

	1	2	...	N
1	2			
2	3			
$\vdots$				
$N-1$	N			
N	1			

et essayer de construire un LD-système.

- au plus une solution pour chaque N;
- en fait, un LD-système ssi N est une puissance de 2, par exemple

	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

- Davantage sur l'ordre des tresses...
- Une autre application simillaire de la théorie des ensembles?
- Partir de

	1	2	...	N
1	2			
2	3			
$\vdots$				
$N-1$	N			
N	1			

et essayer de construire un LD-système.

- au plus une solution pour chaque N;
- en fait, un LD-système ssi N est une puissance de 2,

par exemple

	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

⇝ Définir la n-ème table de Laver A_n comme le LD-système à 2^n éléments.

- Faits: - Toute ligne de A_n est périodique;

- Faits: - Toute ligne de A_n est périodique;
  - A_n est la projection de A_{n+1} mod. 2^n.

- Faits: - Toute ligne de A_n est périodique;
  - A_n est la projection de A_{n+1} mod. 2^n.

  $\rightsquigarrow$ période de la première ligne dans A_{n+1}

  $\geqslant$ période de la première ligne dans A_n.

- Faits: - Toute ligne de A_n est périodique;
  - A_n est la projection de A_{n+1} mod. 2^n.
  - $\rightsquigarrow$ période de la première ligne dans A_{n+1}
  - $\geqslant$ période de la première ligne dans A_n.

- Théorème: (Laver, 1995) Supposons qu'il existe un rang autosimilaire. Alors la période de la première ligne dans A_n tend vers l'infini avec n.

- Faits: - Toute ligne de A_n est périodique;
  - A_n est la projection de A_{n+1} mod. 2^n.
  $\rightsquigarrow$ période de la première ligne dans A_{n+1}
  $\geqslant$ période de la première ligne dans A_n.

- Théorème: (Laver, 1995) Supposons qu'il existe un rang autosimilaire. Alors la période de la première ligne dans A_n tend vers l'infini avec n.

- Problème ouvert :

Démontrer que la période de la première ligne dans A_n tend vers l'infini avec n...

- Faits: - Toute ligne de A_n est périodique;
  - A_n est la projection de A_{n+1} mod. 2^n.

  $\rightsquigarrow$ période de la première ligne dans A_{n+1}

  $\geqslant$ période de la première ligne dans A_n.

- Théorème: (Laver, 1995) Supposons qu'il existe un rang autosimilaire. Alors la période de la première ligne dans A_n tend vers l'infini avec n.

- Problème ouvert :

Démontrer que la période de la première ligne dans A_n tend vers l'infini avec n...

↑

sans utiliser une hypothèse non démontrable
comme l'existence d'un rang autosimilaire

- Faits: - Toute ligne de A_n est périodique;
  - A_n est la projection de A_{n+1} mod. 2^n.

  $\rightsquigarrow$ période de la première ligne dans A_{n+1}

  $\geqslant$ période de la première ligne dans A_n.

- Théorème: (Laver, 1995) Supposons qu'il existe un rang autosimilaire. Alors la période de la première ligne dans A_n tend vers l'infini avec n.

- Problème ouvert :

Démontrer que la période de la première ligne dans A_n tend vers l'infini avec n...

↑

sans utiliser une hypothèse non démontrable
comme l'existence d'un rang autosimilaire

- Seul résultat négatif connu (Dougherty 1995): non démontrable dans l'arithmétique primitive récursive (récurrence double nécessaire).

- P. Dehornoy, Braids and self-distributivity,
  Progress in Math. vol. 192, Birkhauser (2000)

- P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, Why are braids orderable?
  Panoramas & Syntheses vol. 14, Soc. Math. France (2002)

- http://www.math.unicaen.fr/∼ dehornoy