Les tables de Laver

Patrick Dehornoy

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

Tours, avril 2018

• Des objets finis à la description simple, découverts grâce à la théorie des ensembles, dont certaines propriétés combinatoires ne sont (pour le moment) établies qu'à partir d'hypothèses indémontrables, et avec des applications (potentielles) en topologie de basse dimension.

Plan :

- 1. Description combinatoire des tables de Laver
- 2. Tables de Laver et théorie des ensembles
- 3. Tables de Laver et topologie de basse dimension

Plan :

- 1. Description combinatoire des tables de Laver
- 2. Tables de Laver et théorie des ensembles
- 3. Tables de Laver et topologie de basse dimension

• La loi d'autodistributivité (à gauche) :

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

cf. associativité : $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright z$.

• Exemples classiques :

- S quelconque et $x \triangleright y := y$, plus généralement $x \triangleright y = f(y)$;
- E module et $x \triangleright y := (1-\lambda)x + \lambda y$;
- G groupe et $x \triangleright y := xyx^{-1}$.

• Remarque : Ces opérations obéissent à $x \triangleright x = x$ (« idempotence »)

▶ les sous-structures à un générateur sont triviales.

• Q : Conjugaison d'un groupe libre est-elle caractérisée par autodistributivité et idempotence ? Non (Drápal-Kepka-Musilek 1994, Larue 1999), obéit à

$$((x \triangleright y) \triangleright y) \triangleright (x \triangleright z) = (x \triangleright y) \triangleright ((y \triangleright x) \triangleright z), \ldots$$

- Une opération binaire sur $\{1, 2, 3, 4\}$: la table de Laver à quatre éléments

$\triangleright$	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

- Commencer avec $+1 \bmod 4$ dans la 1ère colonne,
et compléter pour obéir à la règle $x \triangleright (y \triangleright 1) = (x \triangleright y) \triangleright (x \triangleright 1)$:

$$\begin{aligned}
4 \triangleright 2 &= 4 \triangleright (1 \triangleright 1) = (4 \triangleright 1) \triangleright (4 \triangleright 1) = 1 \triangleright 1 = 2,\\
4 \triangleright 3 &= 4 \triangleright (2 \triangleright 1) = (4 \triangleright 2) \triangleright (4 \triangleright 1) = 2 \triangleright 1 = 3,\\
4 \triangleright 4 &= 4 \triangleright (3 \triangleright 1) = (4 \triangleright 3) \triangleright (4 \triangleright 1) = 3 \triangleright 1 = 4,\\
3 \triangleright 2 &= 3 \triangleright (1 \triangleright 1) = (3 \triangleright 1) \triangleright (3 \triangleright 1) = 4 \triangleright 4 = 4, \dots
\end{aligned}$$

• La construction marche pour tout entier
et donne une structure autodistributive (« shelf ») pour les puissances de 2 :

• Proposition (Laver) : *Pour tout entier N, il existe une unique opération binaire $\triangleright$ sur $\{1, \ldots, N\}$ vérifiant*

$$x \triangleright 1 = x + 1 \mod N \quad \text{et}$$
$$x \triangleright (y \triangleright 1) = (x \triangleright y) \triangleright (x \triangleright 1).$$

De plus, l'opération ainsi obtenue obéit à la loi

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z) \tag{LD}$$

si, et seulement si, N est une puissance de 2.

► la table de Laver à $1, 2, 4, 8, 16, 32, \ldots$ éléments.

Les tables de Laver : exemples

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

• Pour $n \geqslant 1$, on a $1 \triangleright 1 = 2 \neq 1$ dans A_n : pas idempotent.

▸ très différent de la conjugaison et autres exemples LD classiques

• Proposition (Laver) : *Le shelf A_n est engendré par 1, et admet la présentation $\langle 1 \mid 1_{[2^n]} = 1 \rangle$, où $x_{[k]} = (\ldots((x \triangleright x) \triangleright x) \ldots) \triangleright x$, k termes.*

• Proposition (Drápal) : *Il existe une famille (explicite) de transformations $\mathcal{T}$ (produit direct, ajout d'un élément trivial, ...) telle que tout shelf monogène fini s'obtient à partir des tables de Laver par $\mathcal{T}$.*

▸ Penser à $\mathbb{Z}/p\mathbb{Z}$ dans le monde associatif

• Proposition (Laver) : *Pour chaque* $p \leqslant 2^n$*, il existe un entier* $\pi_n(p)$*, puissance de* 2*, t.q. la* p*-ième ligne de (la table de)* A_n *est*

la répétition de $\pi_n(p)$ *valeurs croissant de* $p+1 \bmod 2^n$ *à* 2^n*.*

• Exemple :

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

- $\pi_3(1) = 4$
- $\pi_3(2) = 4$
- $\pi_3(3) = 2$
- $\pi_3(4) = 4$
- $\pi_3(5) = 2$
- $\pi_3(6) = 2$
- $\pi_3(7) = 1$
- $\pi_3(8) = 8$

- La fonction $x \mapsto x \bmod 2^{n-1}$ est un homomorphisme surjectif de A_n sur A_{n-1}.
  - la limite projective des A_n est un shelf sur les entiers 2-adiques ;
  - on a toujours $\pi_n(p) \geqslant \pi_{n-1}(p)$.

- Quelques valeurs pour les périodes de 1 et 2 :

n	0	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\pi_n(1)$	1	1	2	4	4	8	8	8	8	16	16	16	$\cdots$
$\pi_n(2)$	–	2	2	4	4	8	8	16	16	16	16	16	$\cdots$

- Question 1 : A-t-on toujours $\pi_n(2) \geqslant \pi_n(1)$?
- Question 2 : Est-ce que $\pi_n(1)$ tend vers ∞ avec n ? Atteint-il la valeur 32 ?

- Théorème (Laver, 1995) : *S'il existe un cardinal de Laver, alors la réponse aux questions ci-dessus est positive.*

Plan :

- 1. Description combinatoire des tables de Laver
- 2. Tables de Laver et théorie des ensembles
- 3. Tables de Laver et topologie de basse dimension

- La théorie des ensembles est une théorie de l'infini.

- Elle a été formalisée et axiomatisée au début du XXe siècle :
  le système ZF de Zermelo-Fraenkel

- Le système ZF est incomplet :
  il existe des énoncés qui ne sont ni prouvables, ni réfutables à partir de ZF …
  … par exemple l'hypothèse du continu :

- Théorème : *Sauf si ZF est contradictoire,*
  - (Gödel, 1938) *l'hypothèse du continu n'est pas réfutable à partir de ZF ;*
  - (Cohen, 1963) *l'hypothèse du continu n'est pas prouvable à partir de ZF.*

  ▶ Continuer l'étude pour découvrir davantage de propriétés de l'infini
  et adjoindre à ZF de nouveaux axiomes...

- Quels nouveaux axiomes ?

- Axiomes de grands cardinaux = des solutions à l'équation

$$\frac{\text{ultra-infini}}{\text{infini}} = \frac{\text{infini}}{\text{fini}}.$$

  - Exemples : cardinaux <u>inaccessibles</u>, <u>mesurables</u>, etc.

- Un principe : « être autosimilaire, c'est être grand ».
  - A est infini ssi $\exists j : A \to A$ injectif non bijectif ;
  - A est ultra-infini («autosimilaire») ssi $\exists j : A \to A$ injectif non bijectif
  et <u>préservant</u> tout ce qui est définissable à partir de $\in$.
  $\uparrow$
  un plongement (élémentaire) de A (dans lui-même)

- <u>Exemple</u> : $\mathbb{N}$ infini, mais pas ultra-infini, car, si $j : \mathbb{N} \to \mathbb{N}$ préserve tout ce qui est définissable à partir de $\in$, alors j préserve $0, 1, 2$, etc. et j est l'identité.

- Définition : Un rang est un ensemble R tel que $f : R \to R$ entraîne $f \in R$.
(il en existe...)

- Supposons qu'il existe un ensemble autosimilaire (i.e. avec un plongement...)
  - alors il existe un rang autosimilaire, soit R ;
  - si i, j sont des plongements de R, alors $i : R \to R$ et $j \in R$,
  donc on peut appliquer i à j ;
  - « être un autoplongement » est définissable à partir de $\in$,
  donc $i(j)$ est un plongement ;
  - « être l'image de » est définissable à partir de $\in$,
  donc $\ell = j(k)$ entraîne $i(\ell)=i(j)(i(k))$, soit $i(j(k))=i(j)(i(k))$: loi LD.

- Proposition : *Si j est un plongement d'un rang R,*
alors les itérés de j forment un shelf $\mathrm{Iter}(j)$.
$\uparrow$
clôture de $\{j\}$ pour l'opération « appliquer » : $j(j)$, $j(j)(j)$...

- Un plongement j envoie tout ordinal α sur un ordinal $j(\alpha) \geqslant \alpha$;
  il existe un plus petit α vérifiant $j(\alpha) > \alpha$: l'ordinal critique de j, noté $\mathrm{crit}(j)$.
- Rappel : $j_{[p]} := j(j)(j)...(j)$, p termes.

- Proposition (Laver) : *Supposons que j est un plongement d'un rang R. Pour k, k' dans $\mathrm{Iter}(j)$, déclarons $k \equiv_n k'$ si*

  « *k et k' coïncident jusqu'au niveau de $\mathrm{crit}(j_{[2^n]})$* »

  Alors $\equiv_n$ est une congruence sur $\mathrm{Iter}(j)$, elle a 2^n classes, qui sont les classes de $j, j_{[2]}, ..., j_{[2^n]}$, la dernière étant la classe de id.

  ▶ définition exacte de $\equiv_n$: $\forall x \in R_\gamma (\, k(x) \cap R_\gamma = k'(x) \cap R_\gamma \,)$ avec $\gamma = \mathrm{crit}(j_{[2^n]})$

- Corollaire : *Le quotient $\mathrm{Iter}(j)/\equiv_n$ est (isomorphe à) la table A_n.*

  ▶ Démonstration : $\mathrm{Iter}(j)/\equiv_n$ est un shelf qui a 2^n éléments et qui vérifie $j_{[p]} \triangleright j = j_{[p+1 \bmod 2^n]}$ pour tout p. □

- <u>Lemme 1</u> : *Si j est un plongement d'un rang, alors, pour tous $m \leqslant n$ et $p \leqslant 2^n$, la période de p passe de 2^m à 2^{m+1} entre A_n et A_{n+1} si, et seulement si, $j_{[p]}$ envoie $\mathrm{crit}(j_{[2^m]})$ sur $\mathrm{crit}(j_{[2^n]})$.*

- <u>Lemme 2</u> : *Si j est un plongement d'un rang, alors, pour tout ordinal α, on a $j(j)(\alpha) \leqslant j(\alpha)$.*

  ▶ Démonstration : Il existe β vérifiant $j(\beta) > \alpha$, donc il existe un plus petit tel β : on a donc $j(\beta) > \alpha$, et
$$\forall \gamma < \beta \ (j(\gamma) \leqslant \alpha). \tag{$*$}$$
  En appliquant j à $(*)$, on déduit
$$\forall \gamma < j(\beta) \ (j(j)(\gamma) \leqslant j(\alpha)). \tag{$**$}$$
  En prenant $\gamma = \alpha$ dans $(**)$, on obtient $j(j)(\alpha) \leqslant j(\alpha)$. □

- <u>Proposition</u> (Laver) : *S'il existe un ensemble autosimilaire (= un cardinal de Laver), alors, pour tout n, on a $\pi_n(2) \geqslant \pi_n(1)$.*

- Théorème (Steel, Laver) : *Si j est un plongement d'un rang R, alors la suite des ordinaux $\mathrm{crit}(j_{[2^n]})$ est non bornée dans R.*

- Proposition (Laver) : *S'il existe un cardinal de Laver, la suite des périodes $\pi_n(1)$ tend vers l'infini avec n.*

- Corollaire : *S'il existe un cardinal de Laver, le sous-shelf de la limite projective des A_n engendré par $(1, 1, 1, ...)$ est libre.*

- A-t-on répondu aux questions sur les tables de Laver ?
  - Non, car l'existence d'un cardinal de Laver est un axiome de grand cardinal, donc indémontrable à partir de ZF, et dont même la non-contradiction ne peut être établie à partir de ZF.
  - Un cardinal de Laver est beaucoup plus grand qu'un cardinal de Woodin, donc pas (encore) de consensus pour intégrer son existence au système de base...

- L'hypothèse de grand cardinal est-elle nécessaire ?
  - Probablement pas... Pour le moment, on ne sait pas s'en passer, mais rien ne prouve qu'elle soit nécessaire ; et il n'y a pas de méthode systématique pour l'éliminer.

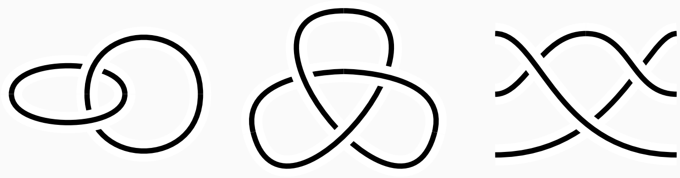
- Une tentative : le programme de Drápal, trois étapes menées à bien...

- Un exemple similaire : l'ordonnabilité des shelves libres et la résolution du problème de mot de LD,
  - d'abord établies à l'aide d'un cardinal de Laver (Laver, 1989),
  - puis par un argument direct (D., 1992) basé sur les groupes de tresses.

Plan :

- 1. Description combinatoire des tables de Laver
- 2. Tables de Laver et théorie des ensembles
- 3. Tables de Laver et topologie de basse dimension

- Diagrammes plans :



▶ projections de courbes plongées en dimension 3

- Question générique : reconnaître si deux diagrammes sont (projections de figures) isotopes

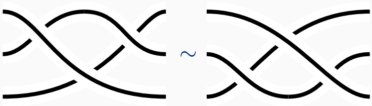
▶ trouver des invariants d'isotopie.

• Deux diagrammes représentent des figures isotopes ssi on peut passer de l'un à l'autre par une suite finie de mouvements de Reidemeister :

- type I :

- type II :

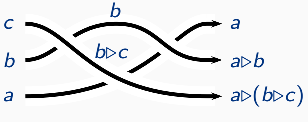
- type III :



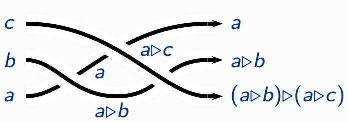
- Fixer un ensemble (de couleurs) S avec deux opérations $\triangleright, \bar{\triangleright}$, et colorier les brins des diagrammes en suivant les règles :

et

- Action des mouvements de Reidemeister III sur les couleurs :

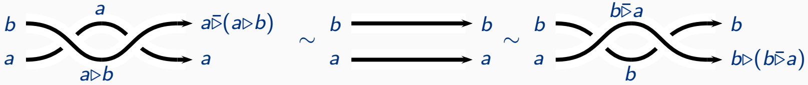


$\sim$



▶ Les S-coloriages sont invariants par Reidemeister III ssi $(S, \triangleright)$ est un shelf.

- Idem pour Reidemeister II :



Il existe $\bar{\triangleright}$ vérifiant $x \triangleright (x \,\bar{\triangleright}\, y) = y$ et $x \,\bar{\triangleright}\, (x \triangleright y) = y$
ssi les translations à gauche de $(S, \triangleright)$ sont bijectives.

  - Les S-coloriages sont invariants par Reidemeister II+III ssi
    $(S, \triangleright)$ est un shelf avec translations à gauche bijectives
    $\uparrow$
    un rack (Fenn–Rourke)

- Idem pour Reidemeister I :

  - Les S-coloriages sont invariants par Reidemeister I+II+III ssi
    $(S, \triangleright)$ est un rack idempotent
    $\uparrow$
    un quandle (Joyce)

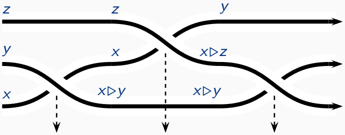
- En théorie (Joyce, Matveev) : Le « quandle fondamental » est
  un invariant complet à symétrie près.

- En pratique (Carter, Kamada) : utiliser la (co)-homologie des shelves
  pour définir des invariants non complets, mais calculables en pratique.

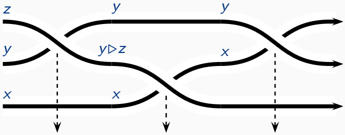
- <u>Définition</u> : Un 2-cocycle sur un shelf $(S, \triangleright)$ est une application $\phi : S^2 \to \mathbb{Z}$ vérifiant

$$\phi(x,z) + \phi(x \triangleright y, x \triangleright z) = \phi(y,z) + \phi(x, y \triangleright z).$$

- <u>Proposition</u> : *Tout* 2*-cocycle donne un invariant pour Reidemeister III (et plus...).*



$\phi(x,y) \quad +\phi(x,z) \quad +\phi(x \triangleright y, x \triangleright z)$



$\phi(y,z) \quad +\phi(x, y \triangleright z) \quad +\phi(x,y)$

- Les tables de Laver sont des shelves mais pas des racks, ni des quandles :
  - pas évident de les utiliser en topologie, mais possible (Przytycki, ...),
  - étape 1 : déterminer les cocycles associés.

- Proposition (D., Lebed) : *Les 2-cocycles sur A_n forment un $\mathbb{Z}$-module libre de rang 2^n, avec une base explicite de cocycles à valeurs dans $\{0, 1\}$.*

$\psi_{1,3}$	1	2	3	4	5	6	7	8
1	1	·	·	·	·	·	·	·
2	1	·	·	·	·	·	·	·
3	1	·	·	·	·	·	·	·
4	1	·	·	·	·	·	·	·
5	1	·	·	·	·	·	·	·
6	1	·	·	·	·	·	·	·
7	1	·	·	·	·	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{2,3}$	1	2	3	4	5	6	7	8
1	·	1	·	·	·	·	·	·
2	1	1	·	·	1	·	·	·
3	1	1	·	·	1	·	·	·
4	·	1	·	·	·	·	·	·
5	1	1	·	·	1	·	·	·
6	1	1	·	·	1	·	·	·
7	1	1	·	·	1	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{3,3}$	1	2	3	4	5	6	7	8
1	1	·	1	·	1	·	·	·
2	·	·	1	·	·	·	·	·
3	1	·	1	·	1	·	·	·
4	·	·	1	·	·	·	·	·
5	1	·	1	·	1	·	·	·
6	1	·	1	·	1	·	·	·
7	1	·	1	·	1	·	·	·
8	·	·	·	·	·	·	·	·

$\psi_{4,3}$	1	2	3	4	5	6	7	8
1	·	·	·	1	·	·	·	·
2	·	·	·	1	·	·	·	·
3	·	1	·	1	·	1	·	·
4	·	·	·	1	·	·	·	·
5	·	1	·	1	·	1	·	·
6	·	1	·	1	·	1	·	·
7	1	1	1	1	1	1	1	·
8	·	·	·	·	·	·	·	·

$\psi_{5,3}$	1	2	3	4	5	6	7	8
1	1	·	·	·	1	·	·	·
2	1	·	·	·	1	·	·	·
3	1	·	·	·	1	·	·	·
4	·	·	·	·	·	·	·	·
5	1	·	·	·	1	·	·	·
6	1	·	·	·	1	·	·	·
7	1	·	·	·	1	·	·	·
8	·	·	·	·	·	·	·	·

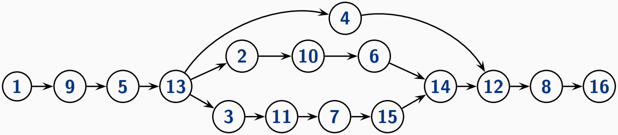
$\psi_{6,3}$	1	2	3	4	5	6	7	8
1	·	1	·	·	·	1	·	·
2	·	1	·	·	·	1	·	·
3	1	1	1	·	1	1	1	·
4	·	·	·	·	·	·	·	·
5	·	1	·	·	·	1	·	·
6	·	1	·	·	·	1	·	·
7	1	1	1	·	1	1	1	·
8	·	·	·	·	·	·	·	·

$\psi_{7,3}$	1	2	3	4	5	6	7	8
1	1	·	1	·	1	·	1	·
2	·	·	·	·	·	·	·	·
3	1	·	1	·	1	·	1	·
4	·	·	·	·	·	·	·	·
5	1	·	1	·	1	·	1	·
6	·	·	·	·	·	·	·	·
7	1	·	1	·	1	·	1	·
8	·	·	·	·	·	·	·	·

- Ces cocycles ne sont pas triviaux : par exemple, le cocycle « période » ψ_n
t.q. $\psi_n(x, y) = 1$ ssi y multiple de la période de x dans A_n.

$\exists z\,(y = z \triangleright x)$

▶ Démonstrations: Reposent sur la divisibilité à droite de A_n, qui est un ordre.



- Question : Que comptent tous ces nouveaux invariants de tresse positive ?

- Résultats analogues pour n-cocycles pour tout n (Lebed, 2016).

- Conclusion : Espoir raisonnable d'application topologique des tables de Laver.

- Les propriétés des périodes dans les tables de Laver sont-elles
  une application de la théorie des ensembles ?
  - Pour le moment, oui ;
  - Dans le futur, formellement non si on découvre des démonstrations
    sans hypothèse de grand cardinal.
  - Mais, dans tous les cas, c'est la théorie des ensembles qui aura permis
    de découvrir les propriétés : même si on ne croit pas que ces objets existent,
    ils fournissent des intuitions et des arguments simples.

- Une analogie :
  - En physique : partir d'une intuition physique, deviner des énoncés,
    puis les passer au mathématicien pour une preuve formelle.
  - Ici : partir d'une intuition logique (existence d'un ensemble autosimilaire),
    deviner des énoncés (les périodes tendent vers l'infini dans les tables de Laver),
    puis les passer au mathématicien pour une preuve formelle.

Richard Laver
(1942-2012)

- R. Laver, *On the algebra of elementary embeddings of a rank into itself*, Adv. Math. 110 (1995) 334–346
- P. Dehornoy, Braids and self-distributivity, Progress in math. vol 192, Birkhaüser (1999), chapters X and XIII
- P. Dehornoy & V. Lebed, *Two- and three-cocycles for Laver tables*, J. Knot Theory Ramifications 23-4 (2014)
- V. Lebed, *Cohomology of Finite Monogenic Self-Distributive Structures*, J. Pure Appl. Algebra 220 (2016) 711–734

www.math.unicaen.fr/∼dehornoy