Patrick Dehornoy au prisme de l'informatique fondamentale

• P.-L. Curien

J'ai commencé à fréquenter Patrick Dehornoy dans son univers mathématique au milieu des années 2000, lorsque, prenant son bâton de pèlerin, il était venu expliquer dans notre séminaire de théoriciens des langages de programmation son approche à la réécriture, nourrie de son expérience avec l'autodistributivité (il en sera question plus loin). Il avait parallèlement soumis par mon intermédiaire un joli article à la revue *Mathematical Structures in Computer Science*, et avait été si heureux des remarques du rapporteur (un « réécrivain » hollandais) qu'il m'avait demandé si je pouvais le mettre en contact avec ce dernier. Et de fil en aiguille, l'article est paru sous les deux noms de Patrick Dehornoy et de Vincent Van Oostrom [4]. Moins d'une dizaine d'années plus tard, à l'issue de son mandat à la direction de l'institut en charge des mathématiques du CNRS (l'INSMI), j'ai été ravi quand Patrick m'a fait part de son souhait de demander un accueil en délégation dans mon laboratoire *Preuves, Programmes et Systèmes* (PPS), à l'université Paris Diderot. Séjour qui a été suivi par un accueil en qualité de chercheur associé. Patrick ne nous a donc plus quittés. Il avait jusqu'à son décès son bureau à l'IRIF [1].

Il participait régulièrement à notre groupe de travail *Catégories supérieures, polygraphes et homotopie*. Il a prêté son concours à plusieurs évènements coorganisés avec nos collègues de Lyon et Marseille. Ainsi, en janvier 2014, il a donné un mini-cours intitulé *Garside calculus* dans le cadre d'une semaine *Algèbre et Calcul* à Lyon. C'est là que j'ai été saisi la première fois, scotché même, par ses talents de conférencier : énergie, précision, clarté lumineuse. Il a aussi été dans le comité scientifique du colloque *Catégories pour la théorie de l'homotopie et la réécriture* qui s'est tenu au CIRM en septembre 2017. Dès les premiers temps de son séjour à Paris Diderot, sous son impulsion, nous avions organisé un groupe de lecture du « livre bleu » (*Foundations of Garside Theory*), qui était alors en voie d'achèvement. Nous avons ainsi baigné dans les « règles de domino » les « retournements », et autres techniques, qui, toujours plus affinées, se retrouvent dans le travail qu'il a mené chez nous avec Yves Guiraud sur la normalisation quadratique [2]. Plus généralement, ces années nous ont permis de bénéficier de son attitude toujours généreuse et à l'écoute, et de sa volonté d'expliquer et de partager ses passions mathématiques, tel un grand chef cuisinier heureux de voir le sourire sur les visages des convives au moment de la dégustation.

Mais revenons en arrière, et tentons de donner un aperçu pouvant éclairer ces liens avec l'informatique. Je laisse d'abord la parole à Matthieu Picantin, mon collègue à l'IRIF, et élève de Patrick. *« Son premier livre de recherche* Braids and self-distributivity*, ou « livre vert »* [2]*, paru en 1999, présente les connexions qu'il a découvertes entre les groupes de tresses et les systèmes autodistributifs, qui sont des ensembles équipés d'une opération binaire satisfaisant à l'équation*

$$x \star (y \star z) = (x \star y) \star (x \star z).$$

Cette identité pourrait sembler presque incongrue, alors qu'en réalité de nombreuses opérations naturelles la vérifient, telle la conjugaison dans un groupe : en définissant $x \star y = xyx^{-1}$*, on a effectivement*

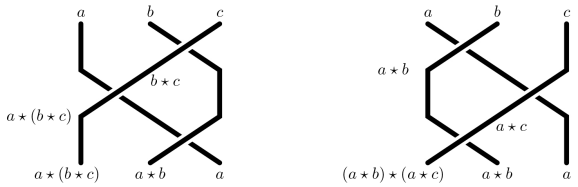
$$x \star (y \star z) = x\,(y \star z)\,x^{-1} = x\,y\,z\,y^{-1}x^{-1}$$
$$(x \star y) \star (x \star z) = (x \star y)\,(x \star z)\,(x \star y)^{-1}$$
$$= x\,y\,x^{-1}\,x\,z\,x^{-1}\,x\,y^{-1}\,x^{-1}.$$

Cette monographie reprend l'ensemble de ses travaux ayant mené à un ordre linéaire invariant à

1. Institut de Recherche en Informatique Fondamentale, CNRS et Université Paris Diderot, né de la fusion de PPS et du LIAFA.
2. Ici, « bleu » et « vert » font référence à la couleur des couvertures.

gauche pour les groupes de tresses : l'ordre de Dehornoy. C'est véritablement une somme compacte, d'où s'échappent une multitude de pistes, de variantes, de digressions, toujours parfaitement ciselées et impeccablement présentées pour inviter si possible sans trop de douleur le lecteur ou la lectrice à poursuivre. Patrick était tout à fait conscient qu'il s'agissait bien d'une montagne intrigante que très peu de randonneurs chercheraient à gravir complètement. Dans sa vidéo[3] *– réalisée à l'occasion d'une petite fête pour ses soixante-cinq ans – où lui-même s'imagine s'ennuyant ferme au paradis des mathématiciens, c'est bien un exemplaire du « livre vert » que le chercheur du futur – Cédric Villani en « special guest » avec ses cheveux paillettés et sa combinaison à double cravate argentée – va finalement extraire des sous-sols abandonnés et poussiéreux de l'Institut Henri Poincaré.*

Pour entrevoir un premier lien entre tresses et autodistributivité, certainement le plus accessible, il s'agit de convenir que l'on colorie les brins d'une tresse (positive) en piochant dans un ensemble de couleurs diverses muni d'une opération binaire $\star$, selon la règle qui veut qu'à chaque croisement la couleur a du brin « au-dessous » reste inchangée, tandis que la couleur b du brin « au-dessus » s'étoffe pour devenir la couleur $a \star b$. Il faut imaginer Patrick au tableau, avec son grand sourire, en train de mimer le coloriage des brins – ou plus littéralement le coulage de peinture depuis le haut de chaque brin – avec son pouce renversé, agrémentant l'action de ses glouglous gourmands.



Ce coloriage respecte ainsi les relations de tresses (positives) si et seulement si son opération $\star$ est autodistributive. Superbe! Mais cela n'est que le tout début de l'histoire – en vérité, histoire quelque peu renversée — de ces liens entre tresses et autodistributivité. La suite du traitement requiert alors des trésors d'inventivité et des hectolitres de peinture et de patience. Il s'agit entre autres de concevoir des formes normales pour ces systèmes autodistributifs, des algorithmes pour les calculer, les manipuler, et les transformer en d'autres formes normales, des moyens de contrôle dans la réécriture de termes, avec au passage maints jolis dessins d'arbres toujours explicites. Vient également la construction d'une opération autodistributive sur les tresses elles-mêmes (en ne bornant pas le nombre des brins), en coloriant ces tresses par des tresses pour aboutir à l'opération suivante dite d'exponentiation :

$$a \mathbin{\wedge} b = a\ sh(b)\ \sigma_1\ sh(b^{-1}), \qquad (1)$$

où sh est l'opération consistant à placer tout à gauche de la tresse un brin vertical « frais ».

Cruciale pour obtenir l'ordre de Dehornoy, l'acyclicité de la division pour l'ensemble des tresses muni de cette exponentiation $\wedge$ est alors obtenue via une preuve syntaxique – syntaxique donc évidemment préférable selon Patrick – de cette acyclicité dans les systèmes autodistributifs libres, au prix d'une vérification de la cohérence et de la convergence de l'opération de complément dans le monoïde décrivant la géométrie de la loi d'autodistributivité.

Patrick n'était pas peu fier de cette exponentiation colorée, de sa genèse tortueuse et de sa présentation élégante, et l'on peut noter qu'elle figure en bonne place sur le tableau noir du chercheur du futur argenté! »

Magique, cette double apparition de la loi autodistributive dans le contexte des tresses ? C'est sans compter que le magicien nous dévoile ses tours, et introduit, pour expliquer ce phénomène et le placer dans un contexte beaucoup plus général, l'une de ses méthodes phares, celle du « blueprint ». Pour la présenter, faisons halte un moment chez les réécrivains « pur jus ». Pour eux, le « jackpot », c'est quand un système de réécriture sur des termes, c'est-à-dire une présentation équationnelle avec un choix d'orientation des équations $t = t'$ (on écrit $t \to t'$ pour l'orientation de gauche à droite), est convergent, c'est-à-dire à la fois confluent et noethérien [4]. Alors (modulo des hypothèses d'effectivité), la décidabilité de l'égalité tombe avec une grande facilité : tous les termes ont une forme normale unique [5], et deux termes t, t' sont équivalents par la théorie équationnelle si et seulement s'ils ont la même forme normale. Mieux, on peut rendre

3. `https://dehornoy.users.lmno.cnrs.fr/clips.html`

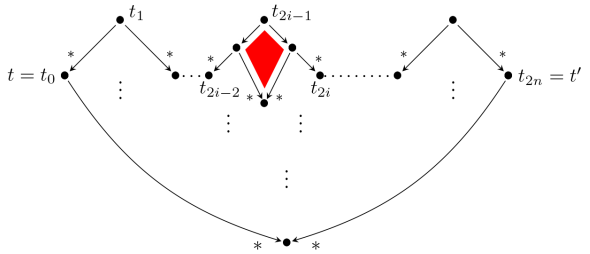
4. On note $\to^*$ la clôture réflexive et transitive de $\to$. La confluence (locale) dit que $t \to^* t_1$ et $t \to^* t_2$ (respectivement $t \to t_1$ et $t \to t_2$) impliquent toujours l'existence de t' tel que $t_1 \to^* t'$ et $t_2 \to^* t'$. La noethérianité dit qu'il n'existe pas de suite infinie (t_n) de termes telle que $t_n \to t_{n+1}$ pour tout n.

5. Un terme t est en forme normale s'il n'est pas réductible, i.e., il n'existe pas t_1 tel que $t \to t_1$.

cet argument complètement constructif, ou géométrique, en exhibant un pavage de l'espace compris entre un zigzag

$$t = t_0 \leftarrow^* t_1 \rightarrow^* t_2 \dots t_{2n-2} \leftarrow^* t_{2n-1} \rightarrow^* t_{2n} = t'$$

et des chemins de t et de t' vers leur forme normale commune. Chaque pavé est un témoin de confluence locale. Les premiers pavés sont posés pour prendre place en haut des pics $t_{2i-2} \leftarrow^* t_{2i-1} \rightarrow^* t_{2i}$, comme suggéré dans la figure ci-dessous :



Cette belle situation est celle rencontrée pour la loi d'associativité

$$(x \star y) \star z = x \star (y \star z),$$

orientée de gauche à droite. Les pavés sont, soit des carrés (correspondant aux cas de confluence locale « triviaux »), soit des instances du célèbre pentagone de Mac Lane : partant du « peigne gauche » $((x \star y) \star z) \star u$, on a deux réductions possibles qui se chevauchent, repérées par l'adresse [6] (notée en indice du symbole $\rightarrow$) du sous-terme auquel elles s'appliquent

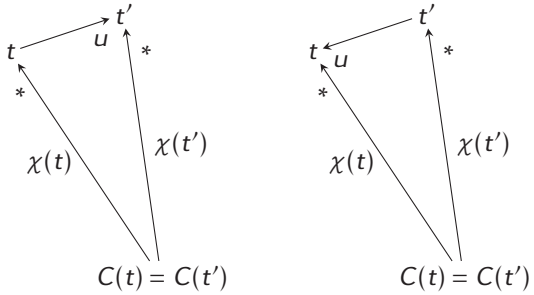
$$((x \star y) \star z) \star u \rightarrow_\epsilon (x \star y) \star (z \star u)$$
$$((x \star y) \star z) \star u \rightarrow_0 (x \star (y \star z)) \star u.$$

Ces deux réductions convergent, en une étape, et en deux étapes, respectivement, vers le « peigne droit » $x \star (y \star (z \star u))$. Comme l'avait remarqué Gérard Huet dans ses notes de cours sur les catégories, au milieu des années 1980, ce pavage fournit une preuve du théorème de cohérence de Mac Lane, qui n'est autre que la preuve originale de Mac Lane, éclairée par la réécriture.

Fort bien, mais que faire si l'on n'a pas la noethérianité ou que l'on n'a pas la confluence ? On peut déjà observer que pour ce pavage en carrés et pentagones, on aurait pu utiliser une propriété moins forte que la noethérianité, et simplement spécifier une fonction qui à tout terme t associe l'inverse $\chi(t)$ d'un chemin de réduction menant de t à un terme $C(t)$ (ainsi canoniquement associé à t), ce chemin étant codifié par un mot d'adresses $u_1, \dots, u_t$; soit, pour $\chi(t) = (\rightarrow_{u_1}) \dots (\rightarrow_{u_t})$:

$$C(t) \rightarrow_{u_1} \dots \rightarrow_{u_t} t.$$

La propriété cruciale est alors que si $t \rightarrow_u t'$ ou $t' \rightarrow_u t$, alors $C(t') = C(t)$, et que l'on peut paver l'espace en forme de coin entre $\chi(t)$, $\chi(t')$ et le chemin de longueur 1 reliant t et t' (et ici la preuve utilisera une définition de χ par induction sur la taille des termes) :



Cette approche peut se formaliser en prenant au sérieux l'indexation par des adresses, et en considérant le monoïde libre sur les générateurs $\rightarrow_u$, qui agit sur les termes en posant $t \cdot (\rightarrow_u) = t'$ lorsque $t \rightarrow_u t'$, et en transcrivant les pavés de confluence locale en égalités entre mots sur cet alphabet de mots. Par exemple, le pentagone est transcrit ainsi :

$$\rightarrow_\epsilon \rightarrow_\epsilon \quad = \quad \rightarrow_0 \rightarrow_\epsilon \rightarrow_1 .$$

Le pendant algébrique des coins ci-dessus est alors le fait que, dans le groupe Geom (appelé *groupe géométrique* associé au système de réécriture) présenté par les générateurs $\rightarrow_u$ (augmentés des générateurs $\leftarrow_u$) et par des relations issues de l'heuristique de confluence locale (complétées par les lois $(\leftarrow_u)(\rightarrow_u) = \epsilon$ et $(\rightarrow_u)(\leftarrow_u) = \epsilon$ [7]), on peut prouver l'égalité suivante, pour tout générateur a :

$$\chi(t \cdot a) = \chi(t)\, a,$$

qui transforme, ou internalise, l'action externe du groupe sur les termes en la multiplication interne du groupe.

L'appareillage est alors quasi-prêt pour aborder des théories équationnelles comme celle de l'autodistributivité, dont l'orientation associée $x \star (y \star z) \rightarrow$

6. Il est pratique de dessiner les termes comme des arbres, et de repérer une occurrence d'un sous-terme t' dans un terme t par une spécification du chemin qui mène de la racine de t à la racine de t'. Une telle spécification est fournie par un mot sur l'alphabet $\{0,1\}$. Par exemple, le sous-terme y de $(x \star y) \star z$ est repéré par l'adresse 01 (« gauche », puis « droite »).

7. Le lecteur attentif observera deux niveaux d'usage du symbole ϵ de mot vide : le mot vide comme dans $\rightarrow_\epsilon$, ou le mot *de mots* vide comme ici !

$(x \star y) \star (x \star z)$[8] est violemment non noethérienne (augmentation de la taille des termes!). Mais il faut encore pousser plus loin la généralité du cadre. On ne demande plus $\chi(t)\, a = \chi(t \cdot a)$ mais seulement

$$\chi(t \cdot a) = \chi(t)\phi(a), \tag{2}$$

pour un endomorphisme ϕ du groupe Geom, et le cordon ombilical rattachant $\chi(t)$ à une réduction aboutissant strictement à t est aussi parallèlement relâché.

Par exemple, pour l'autodistributivité, ce qui sert de guide à la définition de $\chi(t)$ est une propriété d'absorption de tout terme t par des peignes droits p_n comme ci-dessus, avec un nombre suffisant n de dents. Plus précisément, on a, modulo la loi d'autodistributivité : $t \star p_{n-1} = p_n$. On définit alors $\chi(t)$ comme un chemin particulier (défini par induction) menant de p_n à $t \star p_{n-1}$, ce qui conduit, pour que l'équation (2) fasse sens, à définir ϕ comme l'opération sh_0 transformant tout générateur $\rightarrow_u$ (resp. $\leftarrow_u$) en $\rightarrow_{0u}$ (resp. $\leftarrow_{0u}$). Et le miracle arrive, car d'une part l'équation (2) est prouvable, d'autre part le groupe des tresses fait son apparition comme quotient du groupe géométrique. Sous cet angle, l'action des tresses sur une structure distributive découle de celle de l'action du groupe géométrique sur la présentation équationnelle autodistributive, et la construction du « blueprint » explique le passage de l'action des tresses à l'opération autodistributive sur les tresses elles-mêmes décrite plus haut. Mieux, elle permet de la *synthétiser* (l'opération sh utilisée pour l'équation définitionnelle (1) étant bien entendu la projection de sh_0). Le magicien est devenu professeur de magie.

Ceci fait l'objet du chapitre VIII du « livre vert »– je me suis contenté ici de montrer comment arriver, en partant du cadre rêvé des réécrivains, à la vraie vie du « working algebraist », et par là-même rendre patent tout ce que nous avons à apprendre des méthodes de Patrick.

La liste des outils ciselés par Patrick ne s'arrête pas là. Il a poussé le calcul des compléments (opération naturelle dans une structure algébrique admettant assez de plus petits communs multiples pour l'ordre de division), retrouvant ainsi (de manière indépendante) une contrepartie algébrique de la théorie des résidus en réécriture développée originellement dans la thèse de Jean-Jacques Lévy dans le cas du λ-calcul au milieu des années 1970. Ce calcul lui a permis de construire une résolution élégante des monoïdes gaussiens – qui retiennent une partie de l'axiomatique des monoïdes de Garside [1]. Dans cet article en collaboration avec Yves Lafont (issu comme moi de l'univers des preuves et des programmes), d'autres résolutions plus générales sont également construites, réalisant ainsi une extension importante, avec des techniques nouvelles, du travail pionnier de Squier sur l'homologie des groupes d'Artin-Tits.

La dimension syntaxique et algorithmique est omniprésente dans le travail de Patrick. Il s'est intéressé aux questions d'automaticité (extension aux groupes de Garside des résultats de Thurston sur les groupes de tresses). Ceci n'est pas sans lien avec la théorie des germes développée originellement par Bessis, Digne et Michel, et figurant en bonne place dans le « livre bleu ».

Ainsi, le fil d'Ariane est continu, comme le lecteur pourra s'en rendre compte en mettant bout à bout le présent texte et les hommages réunis dans le numéro d'avril 2020 de la *Gazette* : grands cardinaux → structures autodistributives → tresses → ordre sur les tresses et calcul de Garside.

Mais Patrick était furieusement curieux, et a emprunté aussi maints chemins de traverse! Ses liens avec l'informatique ne se limitent pas à la réécriture, à l'algorithmique des mots, ou aux automates. Il a aussi voulu explorer les applications des tresses en cryptographie. Je laisse Hervé Sibert, qui a fait sa thèse avec Patrick sur ces sujets, en parler.

« Toujours soucieux de relier les objets mathématiques qu'il étudiait à des applications concrètes, Patrick remarqua les premiers articles proposant d'utiliser les groupes de tresses en cryptographie[9]*. Dans tous ces exemples, le problème de conjugaison dans le groupe de tresses – déterminer si deux éléments sont conjugués et, dans l'affirmative, exhiber un élément conjuguant – constituait le fondement des protocoles cryptographiques proposés. En collaboration avec la R&D de France Telecom (aujourd'hui Orange), Patrick contribua à l'élaboration de schémas d'authentification basés sur ce même problème. Il me revint d'écrire l'article en question et les preuves de sécurité qui reposaient sur la difficulté du problème de conjugaison, c'est-à-dire qu'il*

8. L'orientation inverse est fortement déconseillée par la profession, à cause de la non-linéarité du terme $(x \star y) \star (x \star z)$, où x apparaît deux fois, car l'implémentation de ce type de règle nécessite de l'unification et non pas du simple filtrage, i.e., pour appliquer la règle ainsi orientée, il faudrait repérer un sous-terme de la forme $(t_1 \star t_2) \star (t_1' \star t_3)$ et *en plus* savoir reconnaître que t_1 et t_1' sont le même terme.

9. Sidelnikov, Cherepnev et Yashchenko (1993), Anshel, Anshel et Goldfeld (1999) et enfin Ko, Lee, Cheon, Han, Kang et Park (2000).

était trivial de construire une instance du problème en choisissant une tresse et un conjuguant, tandis qu'il n'y avait pas à notre connaissance d'algorithme permettant de retrouver efficacement un tel conjuguant étant donné deux tresses conjuguées quelconques.

Un coup d'arrêt fut rapidement donné à la cryptographie à base de tresses, quand plusieurs algorithmes probabilistes permettant de résoudre efficacement le problème de conjugaison furent proposés indépendamment par différents auteurs [10]*. Tous les protocoles n'étaient cependant pas impactés de la même manière, certains d'entre eux reposant sur des instances du problème de conjugaison particulièrement simples à résoudre. Les protocoles sur lesquels nous avions travaillé n'avaient pas ce travers, nous permettant de proposer des heuristiques de choix d'instances plus robustes, mais la confiance en la cryptographie basée sur les groupes de tresses était trop profondément ébranlée.*

Patrick continua à regarder le sujet de loin, proposant d'une part un état des lieux de la cryptographie à base de tresses, et d'autre part des idées et de nouveaux problèmes réputés difficiles pour la construction de protocoles plus sûrs. Si le sujet semble s'être quelque peu tari, la menace que fait peser l'avènement redouté des ordinateurs quantiques sur les protocoles de cryptographie asymétrique couramment utilisés dans des milliards de transactions quotidiennes pourrait bien justifier de se replonger dans la cryptographie basée sur les groupes de tresses. »

Citons un autre exemple d'excursion logico-algébrique. Avec son étudiant Abderrahim Marzouk, Patrick a établi un dictionnaire entre la méthode de Wu pour la résolution d'équations polynomiales et la logique propositionnelle, et en a déduit des stratégies de résolution efficaces. Un pont naturel après coup, mais il fallait y penser, et avoir la culture pour.

L'héritage de Patrick est plus que vivant dans notre champ scientifique. Dans la thèse de doctorat de Maxime Lucas, dirigée par Yves Guiraud, tout comme dans mon travail en collaboration avec Samuel Mimram sur les présentations cohérentes de catégories monoïdales, les techniques de retournement, qui partent de l'idée de transformer une équation de la forme $u'v = v'u$ en une réécriture $uv^{-1} \to v'^{-1}u'$, jouent un rôle clé. Dans une autre direction, le cadre des familles de Garside laisse espérer de pouvoir unifier les généralisations par Gaussent, Guiraud et Malbos du résultat de Deligne montrant l'existence d'une présentation cohérente des monoïdes d'Artin-Tits sphériques (i.e., dont le groupe de Coxeter associé est fini). Utilisant des méthodes purement syntaxiques, ces auteurs ont étendu le résultat de Deligne dans deux directions : les monoïdes d'Artin-Tits généraux, et les monoïdes de Garside – formant deux sous-classes de la classe des monoïdes avec famille de Garside. Mentionnons enfin la normalisation quadratique comme nouveau chantier à développer !

Ces dernières années, ma relation avec Patrick avait pris un tour de plus en plus amical. J'ai eu la chance de les voir régulièrement, son épouse Arlette et lui, jusque dans les dernières semaines [11]. Son besoin d'activité était intact, qu'il s'agisse de corriger des pages Wikipedia sur les tresses, de fignoler des détails de finition dans la chambre d'ami qu'il avait refaite peu avant de tomber malade, ou de confectionner un cake délicieux : perfectionniste en toutes choses ! Le 17 juillet, il m'écrivait ceci : « Je prends un grand plaisir à rédiger un article sur les "règles de domino" qui unifie des types de normalisation divers. J'aime toujours autant mettre au point des lemmes esthétiques et compliqués. » C'est tout lui !

Références

[1] P. Dehornoy et Y. Lafont. « Homology of Gaussian groups ». *Ann. Inst. Fourier (Grenoble)* **53**, n° 2 (2003), p. 489-540. ISSN : 0373-0956. URL : http://aif.cedram.org/item?id=AIF_2003__53_2_489_0.

[2] P. Dehornoy et Y. Guiraud. « Quadratic normalization in monoids ». *Internat. J. Algebra Comput.* **26**, n° 5 (2016), p. 935-972. ISSN : 0218-1967. DOI : 10.1142/S0218196716500399. URL : https://doi.org/10.1142/S0218196716500399.

[3] P. Dehornoy et A. Marzouk. « Theorem proving by chain resolution ». *Theoret. Comput. Sci.* **206**, n° 1-2 (1998), p. 163-180. ISSN : 0304-3975. DOI : 10.1016/S0304-3975(97)00128-X. URL : https://doi.org/10.1016/S0304-3975(97)00128-X.

[4] P. Dehornoy et V. van Oostrom. « Using groups for investigating rewrite systems ». *Math. Structures Comput. Sci.* **18**, n° 6 (2008), p. 1133-1167. ISSN : 0960-1295. DOI : 10.1017/S0960129508007160. URL : https://doi.org/10.1017/S0960129508007160.

10. Hugues (2000), Franco et Gonzales-Meneses (2001), Hofheinz et Steinwandt (2002), Lee et Lee (2002), pour ne citer que ceux-là.
11. Son décès est survenu le le 4 septembre 2019.