Séminaire Dubreil. Algèbre et théorie des nombres

Gérard Lallement

Sur les monoïdes finiment présentés

Séminaire Dubreil. Algèbre et théorie des nombres, tome 25, nº 2 (1971-1972), exp. nº J9, p. J1-J4

<http://www.numdam.org/item?id=SD_1971-1972__25_2_A9_0>

Séminaire DUBREIL (Algèbre)
25e année, 1971/72, n° J9, 4 p.
Journées d'Algèbre [1972. Paris]
Demi-groupes. Demi-groupes ordonnés
(M.-L. DUBREIL-JACOTIN)

30 juin 1972

SUR LES MONOÏDES FINIMENT PRÉSENTÉS

par Gérard LALLEMENT

Les groupes présentés par des générateurs et des relations ont retenu l'attention de nombreux algébristes (voir [7]), essentiellement parce qu'ils apparaissent comme groupes de Poincaré de certains espaces topologiques. Plus récemment, les monoïdes présentés par des générateurs et des relations sont apparus de façon naturelle soit comme préliminaires à la résolution de problèmes combinatoires [2], soit comme une façon de construire des exemples [3].

L'objet de cet exposé est de donner, sans démonstration, quelques résultats concernant les monoïdes présentés par une seule relation et ayant des éléments $\neq 1$ d'ordre fini. Nous renvoyons à [5] pour les détails. Les résultats essentiels sont les suivants :

(a) Un monoïde M, présenté par une relation, a un élément $(\neq 1)$ d'ordre fini si, et seulement si, sa présentation est $M = \langle X \; ; \; p^m p' = p^n p' \rangle$, où p est un mot primitif dans le monoïde libre X^*, $m > n \geqslant 0$, et p' est un facteur gauche de p (éventuellement vide).

(b) Pour tous les monoïdes $M = \langle X \; ; \; p^m p' = p^n p' \rangle$, avec p, p', m, n comme en (a), le problème des mots est résoluble (Le cas $n = 0$, $p' = 1$ est dû à ADJAN [1]).

(c) Nous donnons des conditions nécessaires et suffisantes pour que les monoïdes $M = \langle X \; ; \; p^m p' = p^n p' \rangle$ soient résiduellement finis : M est dit résiduellement fini si, pour tout m, $m' \in M$, $m \neq m'$, il existe un homomorphisme

$$\varphi : \; M \dashrightarrow \varphi(M) ,$$

avec $\varphi(M)$ fini et $\varphi(m) \neq \varphi(m')$.

Notations. - Le symbole $=$ indique l'égalité dans M, et le symbole $\equiv$ l'égalité dans X^*.

1. Conditions d'existence d'idempotents $\neq 1$ dans $M = \langle X \; ; \; w = w' \rangle$.

On appelle transition élémentaire, dans X^*, un remplacement dans un mot m d'une occurence de w par w', ou inversement. Une transition est une succession de transitions élémentaires. Deux transitions $\tau_1 : \; m_1 \Rightarrow m_1'$ et $\tau_2 : \; m_2 \Rightarrow m_2'$ sont dites équivalentes si $m_1 \equiv m_2$, $m_1' \equiv m_2'$, et τ_1, τ_2 ont le même nombre de transitions élémentaires. Une transition contient un cycle si elle contient le même mot à deux endroits distincts. Dans les lemmes qui suivent, nous discutons un monoïde M , présenté par

$$\langle X \; ; \; a_1 a_2 \ldots a_r = x_1 x_2 \ldots x_s \rangle , \qquad a_i \in X , \quad x_j \in X .$$

LEMME 1.1. - Supposons $a_1 \not\equiv x_1$, et soit

$$\tau : \; a_1 a_2 \ldots a_r y_1 y_2 \ldots y_t \Rightarrow x_1 x_2 \ldots x_s m$$

une transition qui n'est pas équivalente à une transition contenant un cycle. Alors τ est équivalente à une transition dont le premier pas est

$$a_1 a_2 \ldots a_r y_1 y_2 \ldots y_t \dashrightarrow x_1 x_2 \ldots x_s y_1 y_2 \ldots y_t .$$

La démonstration se fait par récurrence sur la longueur de τ .

LEMME 1.2. - S'il existe une transition $m \Rightarrow mm'$, avec $m' \not\equiv 1$, alors $a_1 \equiv x_1$.

Démonstration. - On suppose $a_1 \not\equiv x_1$. En considérant un mot m de longueur minimale tel que $m \overset{\tau}{\Rightarrow} mm'$, et une transition τ de longueur minimale pour un tel mot, on met en évidence une contradiction en s'appuyant sur le lemme 1.1.

Par récurrence sur r (nombre des a_i), on obtient alors le théorème suivant.

THÉORÈME 1.3. - Soit $M = \langle X \; ; \; a_1 a_2 \ldots a_r = x_1 x_2 \ldots x_s \rangle$ avec $r < s$. S'il existe m , $m' \in X^*$, $m' \not\equiv 1$, tels que $m = mm'$, alors $a_i \equiv x_i$ pour tout i , $1 \leqslant i \leqslant r$.

COROLLAIRE 1.4. - Soit $M = \langle X \; ; \; w = w' \rangle$ avec $\ell(w') > \ell(w) > 0$. Alors M a un idempotent $\neq 1$ si, et seulement si, w' admet w comme facteur gauche et comme facteur droit dans X^* .

En utilisant les résultats classiques sur la conjugaison et les mots primitifs dans X^* [6], ainsi que ceux sur l'existence d'éléments d'ordre fini dans un groupe à un relateur [4], on obtient l'énoncé (a) de l'introduction.

2. Le problème des mots.

Soit $M = \langle X \; ; \; w = w' \rangle$, où w est un facteur gauche et droit de w' . On définit

$$S(w) = \{u \in X^* \mid \; uw \equiv wu_1 \; \text{ pour } \; u_1 \in X^*\} .$$

On vérifie que $(uv \in S(w) \; , \; v \in S(w))$ impliquent $(u \in S(w))$. Il s'en suit que $S(w)$ est engendré librement par un code suffixe Σ [8]. En mettant en évidence, dans un mot $m \in X^*$, la première occurence de w , on écrit m de façon unique sous la forme $m = u\omega$, où $\omega \in \Sigma^*$.

LEMME 2.1. - Soient m_1 , $m_2 \in X^*$ et $u_1 \omega_1$, $u_2 \omega_2$ leur décomposition respective par rapport à $S(w)$. Alors $m_1 = m_2$ si, et seulement si, $\omega_1 = \omega_2$ et $u_1 \equiv u_2$.

Ce lemme permet de réduire le problème des mots, aux mots appartenant à l'idéal

wX^* . Dans ce but, on remarque que $w' \equiv w_1 w$ pour un certain $w_1 \in S(w)$. En écrivant $w_1 \equiv \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_s}$ avec $\alpha_{i_K} \in \Sigma$, on obtient un monoïde $L(M)$ présenté par

$$L(M) = \langle \Sigma \; ; \; \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_s} = 1 \rangle$$

appelé le monoïde spécial associé à M .

LEMME 2.2. - Soient ω_1 , $\omega_2 \in wX^*$, et soient $\omega_1 \equiv \overline{\omega}_1 wv_1$, $\omega_2 \equiv \overline{\omega}_2 wv_2$ leur factorisation obtenue en mettant en évidence la dernière occurence de w .

Alors $\omega_1 = \omega_2$ si, et seulement si, $\overline{\omega}_1 = \overline{\omega}_2$ (dans $L(M)$) et $v_1 \equiv v_2$.

Les lemmes précédents, ainsi que le résultat d'ADJAN sur la résolubilité du problème des mots pour les monoïdes ayant une présentation $\langle X \; ; \; w = 1 \rangle$ (cf. [1]), donnent l'énoncé (b) de l'introduction.

Il est à noter que le problème de la divisibilité (gauche, droite, bilatère) des mots est aussi résoluble. Il en résulte que la question de savoir si dans M , deux éléments sont $\mathcal{K}$-équivalents (où $\mathcal{K}$ est l'une quelconque des équivalences de Green) est décidable. Noter $\mathcal{J} \neq \mathcal{D}$, en général.

3. La condition "résiduellement fini"

PROPOSITION 3.1. - Soit $M = \langle X \; ; \; w = w' \rangle$, où w est un facteur gauche et droit de w' . Si la relation de présentation du monoïde spécial $L(M)$ associé à M n'est pas une relation de présentation d'un groupe, alors M n'est pas résiduellement fini.

On démontre en effet que, dans les conditions de l'énoncé, M contient un sous-monoïde isomorphe au monoïde bicyclique, lequel n'est pas résiduellement fini. Une réciproque de la proposition précédente est la suivante.

PROPOSITION 3.2. - Soit $M = \langle X \; ; \; w = w' \rangle$, où w est un facteur gauche et droit de w' . Si le monoïde spécial $L(M)$ est le produit libre d'un groupe résiduellement fini et d'un monoïde libre, alors M est résiduellement fini.

La démonstration de la proposition 3.2 est assez difficile. Nous proposons la conjecture suivante :

CONJECTURE. - Soit G un groupe à un "relateur" ayant une présentation monoïdale (c'est-à-dire $G = \langle X \; ; \; w = 1 \rangle$, où $\langle X \; ; \; w = 1 \rangle$ est une présentation d'un monoïde). Alors G est résiduellement fini.

Si cette conjecture était vraie, on pourrait énoncer : Un monoïde, présenté par une relation, ayant des éléments $\neq 1$ d'ordre fini, est résiduellement fini si, et seulement si, il ne contient pas un sous-monoïde isomorphe au monoïde bicyclique (ou, de façon équivalente, si son monoïde spécial a une relation de présentation qui est celle d'un groupe).

BIBLIOGRAPHIE

[1] ADJAN (S. I.). - Relations de définition et problèmes algorithmiques pour les groupes et les demi-groupes [en russe], Trudy Matem. Inst. Steklov., t. 85, 1966 ; [en anglais] Proc. Steklov Inst. of Math., t. 85, 1966, p. 1-152.

[2] CARTIER (P.) et FOATA (D.). - Problèmes combinatoires de commutation et réarrangements. - Berlin, Springer-Verlag, 1969 (Lecture Notes in Mathematics, 85).

[3] CLIFFORD (A. H.) and PRESTON (G. B.). - The algebraic theory of semigroups, Vol. 1 and 2. - Providence, American mathematical Society, 1961 and 1967 (Mathematical Surveys, 7).

[4] KARRASS (A.), MAGNUS (W.) and SOLITAR (D.). - Elements of finite order in groups with a single defining relation, Comm. pure and applied Math., t. 13, 1960, p. 57-66.

[5] LALLEMENT (G.). - On monoids presented by a single relation (à paraître).

[6] LYNDON (R. C.) and SCHÜTZENBERGER (M. P.). - The equation $a^m = b^n c^p$ in a free group, Michigan math. J., t. 9, 1962, p. 289-298.

[7] MAGNUS (W.), KARRASS (A.) and SOLITAR (D.). - Combinatorial group theory. - New York, Interscience Publ., 1966 (Pure and applied Mathematics, Interscience, 13).

[8] NIVAT (M.). - Eléments de la théorie générale des codes, "Automata Theory", p. 278-294. - New York, Academic Press, 1966.

Gérard LALLEMENT
Department of Mathematics
Pennsylvania State University
230 McAllister Building
UNIVERSITY PARK, Penn. 16802 (Etats-Unis)