Séminaire Dubreil.
Algèbre et théorie
des nombres

Marcel-Paul Schützenberger

Sur les monoïdes finis n'ayant que des sous-groupes triviaux

Séminaire Dubreil. Algèbre et théorie des nombres, tome 18, n° 1 (1964-1965), exp. n° 10, p. 1-6

<http://www.numdam.org/item?id=SD_1964-1965__18_1_A9_0>

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1964-1965, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
18e année, 1964/65, n° 10

25 janvier 1965

SUR LES MONOÏDES FINIS N'AYANT QUE DES SOUS-GROUPES TRIVIAUX

par Marcel-Paul SCHÜTZENBERGER

Introduction.

Soit X^* le monoïde libre (demi-groupe libre avec élément neutre e) engendré par un ensemble fixe X . A chaque congruence sur X^* correspond l'algèbre de Boole des parties de X^* saturées par cette congruence ; réciproquement, à chaque algèbre de Boole de parties de X^* correspond de façon unique une congruence qui est la plus fine parmi toutes celles pour lesquelles chacune de ces parties est saturée. Un des problèmes de ce que l'on appelle parfois la théorie des langages formels consiste à étudier les rapports existant entre les familles de congruences sur X^* et les familles de parties de X^* (ou "familles de langages formels") qui leur sont ainsi associées. Soit en particulier $\mathfrak{G}$ une variété de groupes, c'est-à-dire une famille de groupes abstraits contenant tout sous-groupe et tout groupe quotient du produit direct de deux de ses membres. Nous désignerons toujours par $\mathfrak{M}(\mathfrak{G})$ la famille des monoïdes quotient de X^* qui, d'une part sont finis et, d'autre part, ont tous leurs sous-groupes dans $\mathfrak{G}$. On verra plus bas que, de fait, $\mathfrak{M}(\mathfrak{G})$ est une variété de monoïdes ; on l'appellera la variété de monoïdes finis induite par $\mathfrak{G}$.

De même, $\mathfrak{X}^*(\mathfrak{G})$ désignera la famille des parties de X^* saturées par au moins une congruence telle que le monoïde quotient associé appartienne à $\mathfrak{M}(\mathfrak{G})$. On a l'énoncé suivant :

1. - $\mathfrak{X}^*(\mathfrak{G})$ est un sous-gerbier complémenté du gerbier des parties de X^* .

En d'autres termes, si A et B sont deux parties de X^* appartenant à $\mathfrak{X}^*(\mathfrak{G})$, $\mathfrak{X}^*(\mathfrak{G})$ contient $A \cup B$, le complément $X^* \backslash A$ de A dans X^* et le produit $AB = \{ff' \in X^* : f \in A ; f' \in B\}$. Le résultat suivant constitue le théorème fondamental de ce que l'on appelle la théorie des automates finis.

2. THÉORÈME de Kleene. - Quand $\mathfrak{G}$ est la variété de tous les groupes, $\mathfrak{X}^*(\mathfrak{G})$ est le plus petit gerbier de parties de X^* qui contienne toutes les parties X' de X et qui contienne le sous-monoïde A^* engendré par l'un quelconque de ses membres A .

Je me propose ici de donner la vérification de la propriété suivante :

3. - Si $\mathfrak{G}_0$ est la variété de groupes consistant en le seul groupe trivial (c'est-à-dire réduit à un élément neutre), $\mathfrak{X}^*(\mathfrak{G}_0)$ est le plus petit gerbier complémenté contenant toutes les parties X' de X .

Il serait naturellement intéressant d'avoir des caractérisations analogues pour d'autres variétés de groupes que les deux cas extrêmes envisagés ici. Des progrès substantiels ont été réalisés dans cette direction par RHODES et KRON en faisant appel à certaines applications de X^* dans lui-même et à la notion de produit semi-direct (ou de produit en couronne) de monoïdes ; M. NIVAT a exposé ici même cette question et certains des résultats qu'il a obtenus. Je mentionne l'énoncé suivant qui appelle de nouvelles recherches :

4. - Si $\mathfrak{A}$ est la variété des groupes abéliens, $\mathfrak{X}^*(\mathfrak{A})$ contient en même temps que chacun de ses membres B le sous-monoïde engendré par $B \setminus BXX^*$ (ou symétriquement, $B \setminus X^*XB$).

J'ignore si cette propriété de fermeture suffit à caractériser $\mathfrak{X}^*(\mathfrak{A})$; en utilisant les opérations de RHODES et KRON, elle permet d'obtenir $\mathfrak{X}^*(\mathfrak{G}_{sol})$ à partir des parties de X , où $\mathfrak{G}_{sol}$ est la variété des groupes solvables. Dans tous ces cas, il est impossible de se dispenser d'une hypothèse de finitude (au moins sur les chaînes d'idéaux) sur les monoïdes-quotient envisagés. On peut par contre, compliquer les énoncés pour obtenir des résultats un peu plus généraux. Pour terminer cette introduction et motiver un peu mieux les objets considérés, je signale l'énoncé suivant, inspiré de ce que les ingénieurs appellent les "automates incomplètement spécifiés" :

5. - Soient A , $B \in \mathfrak{X}^*(\mathfrak{G})$ où $\mathfrak{G}$ est la variété de tous les groupes. Il existe une plus petite variété de groupes $\mathfrak{G}'$ telle que $\mathfrak{X}^*(\mathfrak{G}')$ contienne au moins un A' satisfaisant $A \subset A'$; $B \cap A' = \emptyset$.

(Il n'existe pas en général de congruence plus fine que toutes les autres parmi celles qui saturent au moins une partie A' séparant A et B comme ci-dessus.)

Enfin, soit $\mathfrak{X}^{\underset{\sim}{N}}$ l'ensemble des applications dans X de l'ensemble $\underset{\sim}{N}$ des entiers naturels. Pour $f \in \mathfrak{X}^{\underset{\sim}{N}}$ et n , $n' \in \underset{\sim}{N}$, on pose

$$f[n , n'] = e \in X^* \qquad \text{si} \quad n \geqslant n' ,$$

et

$$f[n , n'] = f(n)\ f(n+1) \ldots f(n'-1) \in X^* \qquad \text{si} \quad n < n' .$$

Si $\mathfrak{G}$ est une variété de groupes, $\mathfrak{X}^{\underset{\sim}{N}}(\mathfrak{G})$ sera la famille de toutes les parties de $\mathfrak{X}^{\underset{\sim}{N}}$ qui sont une union finie de parties élémentaires V_M de $\mathfrak{X}^{\underset{\sim}{N}}$ de la forme

$$V_M = \{f \in \mathfrak{X}^N ; \quad M = \bigcap_{n>0} \{\alpha f[0 , n'] : \quad n' > n\}\}$$

où $M \subset \alpha X^*$ et où α est un homomorphisme de X^* dans un monoïde de la variété $\mathfrak{M}(\mathfrak{G})$.

Il est assez remarquable que chaque $A \in \mathfrak{X}^N(\mathfrak{G})$ définisse de façon unique une certaine congruence sur X^* d'une manière qui généralise la construction applicable aux parties de X^* . On a :

6. THÉORÈME de Büchi et McNaughton. - Pour chaque variété de groupe $\mathfrak{G}$, $\mathfrak{X}^N(\mathfrak{G})$ est une algèbre de Boole qui contient toutes les parties de $\mathfrak{X}^N$ de la forme

$$V'_M = \{f \in \mathfrak{X}^N ; \quad M = \bigcap_{n,m>0} \{\alpha f[n' , n' + m'] : \quad n' > n ; \quad m' > m\}\} .$$

où M et α sont pris comme plus haut.

1. Vérification de la propriété 1.

Si les monoïdes M et M' ont tous leurs sous-groupes dans $\mathfrak{G}$, il est clair que tout sous-groupe de tout sous-monoïde de $M \times M'$ est un sous-groupe du produit direct de deux sous-groupes de M et de M' . Pour vérifier que $\mathfrak{M}(\mathfrak{G})$ est une variété de monoïdes, il suffit donc de considérer $M \in \mathfrak{M}(\mathfrak{G})$, un épimorphisme $\alpha : M \to M''$ et de vérifier que si G'' est un sous-groupe de M'' , il existe au moins un sous-groupe G de M tel que $\alpha G = G''$. Soit donc P l'union de l'élément neutre de M et de $\{m \in M ; \ \alpha m \in G''\}$. Comme M est fini, le monoïde $P \subset M$ possède au moins un quasi-idéal minimal H , c'est-à-dire un sous-ensemble non vide H qui satisfait $PH \cap HP = PHP = H$, et H est un sous-groupe de P , donc de M . On a $G''.\alpha H.G'' = \alpha H$, c'est-à-dire $G'' = \alpha H$, et la remarque est établie.

Vérifions maintenant que $\mathfrak{M}(\mathfrak{G})$ est un gerbier complémenté, et pour cela considérons deux homomorphismes

$$\alpha_i : X^* \to M_i \quad \text{où} \quad i = 1 , 2 \qquad \text{et} \quad M_1 , M_2 \in \mathfrak{M}(\mathfrak{G}) .$$

Soit R l'ensemble des parties de $M_1 \times M_2$. Pour $m_1 \in M_1$, $m_2 \in M_2$ et

$$r = \{(m'_{1,j} , m'_{2,j}) ; \quad j \in J_r\} \in R ,$$

on pose

$$m_1 . r . m_2 = \{(m_1 \, m'_{1,j} , m'_{2,j} \, m_2) ; \quad j \in J_r\} \in R ,$$

et, e_i étant l'élément neutre de M_i , on définit une multiplication associative

sur $M_1 \times R \times M_2$ en posant, pour toute paire d'éléments de ce produit direct d'ensembles :

$$(m_1 , r , m_2)(m_1' , r' , m_2') = (m_1 m_1' , m_1 r'e_2 \cup e_1 rm_2' , m_2 m_2') .$$

Enfin on définit l'homomorphisme β de X^* sur un monoïde P contenu dans $M_1 \times R \times M_2$ en posant, pour tout $f \in X^*$:

$$\beta f = (\alpha_1 f , \{(\alpha_1 f' , \alpha_2 f'') ; f'f'' = f\} , \alpha_2 f) .$$

Il est clair que si les sous-ensembles A_i de X^* satisfont $\alpha_i^{-1} \alpha_i A_i = A_i$, $(i = 1 , 2)$, on a aussi $B = \beta^{-1} \beta B$ pour

$$B = A_1 \cup A_2 , \quad B = A_1 \backslash A_2 \quad \text{ou} \quad B = A_1 A_2 .$$

Il ne nous reste à vérifier que $P \in \mathfrak{M}(\mathfrak{G})$. Soit $G = \{(m_{1,j} , r_j , m_{2,j}) ; j \in J\}$ un sous-groupe de P . Les sous-ensembles $G_i = \{m_{i,j} ; j \in J\}$ de M_i $(i = 1 , 2)$ sont des images homomorphes de G ; ce sont donc des sous-groupes. Soit u_i l'idempotent contenu dans G_i et soit N l'intersection de G avec $\{(u_1 , r , u_2) ; r \in R\}$. N est un sous-groupe normal de G et le groupe quotient G/N est isomorphe à un sous-groupe du produit direct $G_1 \times G_2$. Il suffit donc de vérifier que N se réduit à l'idempotent $u = (u_1 , r , u_2)$ contenu dans G . Pour cela, prenons deux éléments

$$g = (u_1 , s , u_2) \qquad \text{et} \quad \overline{g} = (u_1 , \overline{s} , u_2)$$

de N inverses l'un de l'autre. La relation $u = u^2$ donne

$$r = u_1 r \cup ru_2$$

et la relation $u = g\overline{g}$ donne

$$r = u_1 \overline{s} \cup su_2 .$$

On a donc

$$u_1 r = u_1 \cup u_1 su_2$$

et, puisque $u_1 r \subset r$, ceci entraîne

$$u_1 su_2 \subset r .$$

Maintenant, on déduit de $g = ugu$ la relation

$$s = u_1 r \cup u_1 su_2 \cup ru_2$$

c'est-à-dire $s = r \cup u_1 su_2$ et enfin $s = r$ ce qui montre que $g = u$, $N = \{u\}$; G est donc isomorphe à un sous-groupe de $G_1 \times G_2$, et $P \in \mathfrak{M}(\mathfrak{G})$ est vérifié.

On peut noter que, de fait, P est un sous-monoïde du produit semi-direct de $M_1 \times M_2$ par le produit direct de $\mathrm{Card}(M_1) \times \mathrm{Card}(M_2)$ copies du monoïde $\{0 , 1\}$ à deux éléments booléens $(0 = 01 = 10 = 00 ; \ 1 = 11)$.

2. Vérification de la propriété 3.

Soit $\Gamma(n)$ la famille des homomorphismes de X^* dans des monoïdes ayant au plus n éléments et dont tous les sous-groupes sont triviaux. Il est clair que pour chaque partie X' de X , on peut trouver un $\gamma \in \Gamma(3)$ tel que $\gamma^{-1} \gamma X' = X'$. Tenant compte de la propriété 1, ceci montre que $\mathfrak{X}^*(\mathfrak{G}_0)$ contient $\mathfrak{F}$, le gerbier complémenté des parties de X^* qui est engendré par tous les $X' \subset X$.

Réciproquement, si $\gamma \in \Gamma(2)$ et si $A = \gamma^{-1} \gamma A$, on a $A = \phi$ ou $A = \{e\}$ ou $A = X^*$, et par conséquent, $A \in \mathfrak{F}$. Pour établir la propriété, il suffit donc de prendre $\gamma \in \Gamma(n)$ fixe et de vérifier que $\gamma^{-1} \gamma A = A$ entraîne $A \in \mathfrak{F}$ sous l'hypothèse d'induction que $A' \in \mathfrak{F}$ pour tous les A' tels que $\gamma'^{-1} \gamma' A' = A'$ pour au moins un $\gamma' \in \Gamma(n-1)$. De fait, comme $M = \gamma X^*$ est fini, il suffit même de vérifier ce résultat pour chaque sous-ensemble A de la forme $\gamma^{-1} m$ $(m \in M)$.

On a :

(i) $\gamma^{-1} m \in \mathfrak{F}$ si le résiduel $W_m = \{m' \in M ; \ m \notin Mm'M\}$ de m a deux éléments ou plus.

En effet, il existe un homomorphisme ρ de M sur un monoïde M' tel que ρW_m soit un zéro de M' et que la restriction de ρ à $M \backslash W_m$ soit bijective. On a $\gamma^{-1} m = (\rho\gamma)^{-1} m$ et $\rho\gamma \in \Gamma(n-1)$, et par conséquent, $(\rho\gamma)^{-1} m \in \mathfrak{F}$ résulte de l'hypothèse d'induction.

(ii) Quel que soit $m \in M$, $\gamma^{-1}(MmM) \in \mathfrak{F}$.

Soit $f \in \gamma^{-1}(MmM)$. Le mot f possède au moins un facteur g de longueur minimale tel que γg appartienne à la même $\mathfrak{D}$-classe que m . Si $g \notin \{e\} \cup X$, on peut écrire $g = xg'x'$ où $x , x' \in X$ et $g' \in X^*$. Comme M est un monoïde fini, la théorie de Green et l'hypothèse qu'aucun des facteurs propres de g n'appartient à la $\mathfrak{D}$-classe de γg impliquent que $\gamma xg'$, $\gamma g'x'$ et γg appartiennent au résiduel de $\gamma g'$ et qu'au moins deux de ces trois éléments sont distincts. D'après ce que l'on vient de voir, $\gamma^{-1} g'$ appartient donc à $\mathfrak{F}$. Il en résulte que $\gamma^{-1} MmM$ est une union finie d'ensembles de la forme $X^*X_1 \times \gamma^{-1} g' \times X_2 X^*$ où X_1 et X_2 sont des parties de X et où $\gamma^{-1} g' \in \mathfrak{F}$ pour chacun des g' .

(iii) Quel que soit $m \in M$, $\gamma^{-1}(mM)$ et $\gamma^{-1}(Mm)$ appartiennent à $\mathfrak{F}$.

Soit encore $f \in \gamma^{-1}(mM)$, et soit g le facteur gauche de longueur minimale de

f tel que γg et m appartiennent à la même $\mathcal{R}$-classe. On peut écrire $g = g'x$ où $x \in X$ et $g' \in X^*$, et tenant compte de ce que M est fini, on voit que, comme plus haut, la $\mathcal{Q}$-classe de m appartient au résiduel de $\gamma g'$. Utilisant encore (i), on en conclut que $\gamma^{-1} g' \in \mathfrak{F}$ quand la $\mathcal{Q}$-classe de m contient deux éléments ou plus (si cette $\mathcal{Q}$-classe ne contenait qu'un seul élément, et si le résiduel de m ne contenait pas deux éléments, on aurait $mM = MmM$). Le même raisonnement que dans (ii) achève la vérification de (iii).

Ceci termine aussi la vérification de la propriété 3, car l'hypothèse que tous les sous-groupes de M sont triviaux équivaut à l'identité

$$\{m\} = (mM \cap Mm) \backslash W_m \qquad \text{pour tout } m \in M .$$

BIBLIOGRAPHIE

[1] KLEENE (S. C.). - Representation of events in nerve nets and finite automata, Automata studies, p. 1-41. - Princeton, Princeton University Press, 1956 (Annals of Mathematics Studies, 34).

[2] McNAUGHTON (R.). - Symbolic logic and automata. - Washington, Wright Air Development Center, 1960 (W. A. D. C. Technical Report).