PUBLICATIONS SCIENTIFIQUES
DE L'UNIVERSITÉ D' AIGER

SÉRIE A

MATHÉMATIQUES

DÉCEMBRE 1959. — Tome VI.

EXTRAIT

—

M. P. SCHÜTZENBERGER

SUR CERTAINS SOUS-DEMI-GROUPES QUI INTERVIENNENT DANS UN PROBLÈME DE MATHÉMATIQUES APPLIQUÉES

IMPRIMERIE DURAND CHARTRES - 9, RUE FULBERT

Alger, Mathématiques.
Tome VI, 1959.

M. P. SCHÜTZENBERGER (Poitiers)

SUR CERTAINS SOUS-DEMI-GROUPES QUI INTERVIENNENT DANS UN PROBLÈME DE MATHÉMATIQUES APPLIQUÉES

Dans cette note on examine les relations existant entre deux systèmes de conditions qui peuvent caractériser certains sous-demi-groupes intervenant dans un problème d'algèbre appliquée (1).

On fera toujours l'hypothèse que l'élément neutre e du demi-groupe S est contenu dans le sous-demi-groupe P.

Les huit conditions U_x^y sont de la forme :

Si pour un $s \in S$, $U_x^y(s)$ intersecte P, alors s appartient à P, avec :

$$U_d^m(s) = sP \cap Ps; \quad U_r^m(s) = Ps; \quad U_l^m(s) = sP; \quad U_k^m(s) = PsP;$$
$$U_d^f(s) = sS \cap Ss; \quad U_r^f(s) = Ss; \quad U_l^f(s) = sS; \quad U_k^f(s) = SsS;$$

(1) L'intérêt pratique de ces conditions peut être rappelé brièvement comme suit : Soit S demi-groupe libre engendré par un ensemble dénombrable de symboles S_1; P un sous-demi-groupe de S engendré par un ensemble de mots P_1.

La condition U_d^m est nécessaire et suffisante pour que P_1 puisse être utilisé comme un « code » afin de transmettre des messages au moyen des signaux élémentaires en correspondance biunivoque avec les éléments de S_1; U_d^m étant supposée satisfaite, N_d^m devient une condition nécessaire et suffisante pour qu'il existe une distribution de probabilité pour laquelle ce code soit admissible du point de vue de la longueur moyenne des mots. Dans ce cas, N_d^f contrôle la distribution asymptotique du délai au décodage. Les codes unilatéraux (U_r^m) sont les plus importants pratiquement puisque pour eux ce délai est minimal. Et, parmi ceux-ci, les codes satisfaisant U_r^f présentent des caractères optimaux étudiés par B. Mandelbrot qui les a le premier définis. U_k^m signifie donc que le message peut être décodé sans délai aussi bien de droite à gauche que de gauche à droite, etc. (Cf. [8]).

Les huit conditions N_x^y sont de la forme :

Pour tout $s \in S$; $U_{x'}^{y'}(s)$ intersecte P avec $y' = m$ (ou f) quand $y = f$ (ou m) et x' correspondant à x de la façon suivante :

$$d' = k; \qquad r' = l; \qquad l' = r; \qquad k' = d.$$

Par exemple, P satisfait U_r^m et N_d^f si, pour tout $s \in S$, la relation $sp = p'$ avec $p, p' \in P$ entraîne $s \in P$ et si pour tout $s \in S$, il existe au moins une paire $p'', p''' \in P$ telle que $p''sp''' \in P$.

Puisque l'on a supposé que e appartient à P, on a pour $A = U$ ou N :

1) Quelque soit $x = d, r, l$ ou k, A_x^f entraîne A_x^m;

2) Quelque soit $y = m$ ou f, si A_r^y ou A_l^y, alors A_d^y;

3) Quelque soit $y = m$ ou f, si A_r^y et A_l^y, alors A_k^y et réciproquement.

La plupart de ces conditions ont déjà été étudiées et définies par P. Dubreil [4, 5, 6] dans le cas plus général d'un sous-ensemble et non pas seulement d'un sous-demi-groupe. U_k^m : « *unitaire* »; U_r^m (U_l^m) « *unitaire à gauche (à droite)*; N_k^m (N_r^m, N_l^m) « *net* » *(à droite, à gauche);* U_r^f (U_l^f) « *consistant à droite* » *(à gauche)*; nous rappelons les propriétés les plus simples qui se déduisent de ces conditions :

U_d^m est une condition nécessaire et suffisante pour que P soit libre quand S est un demi-groupe libre; U_r^m est satisfaite de façon caractéristique par les sous-demi-groupes qui laissent fixe un point dans une représentation à droite de S; U_x^f (avec $x = r, l$) exprime que $S - P$ est un idéal (à droite, à gauche,) et se rattache à des notions de primalité; N_x^m ($x = d, r, l, k$) signifie que P intersecte tous les idéaux (bilatères, à droite, à gauche, *bi*-idéaux); N_x^f ($x = k, l, r, d$) est satisfaite quand P contient un idéal (bilatère, à droite, à gauche *bi*-idéal). Si S est un groupe ou un demi-groupe commutatif, A_x^y est équivalent à $A_{x'}$, pour $A = U$ ou N et y, x et x' quelconques. Plus particulièrement :

Quand S est un groupe, U_x^m est nécessaire et suffisante pour que P soit un sous-groupe et non pas seulement un sous-demi-groupe; N_x^m est satisfaite de façon triviale et A_x^f entraîne $P = S$.

Quand S est un treillis, A_x^m est équivalente à A_y^f; U_x^y est nécessaire et suffisante pour que P soit un idéal dual de S et N_x^y pour que P contienne le zéro de S.

Pour S quelconque, les seules relations qui existent entre ces conditions sont triviales mais pour une classe qui comprend en particulier tous les demi-groupes compacts il est possible de prouver la

PROPOSITION : *S'il existe un homomorphisme* φ *de* S *tel que* $P = \overset{-1}{\varphi}\varphi P$ *et que* φS *admette des bi-idéaux minimaux, toute paire de conditions* $(U_x^y, N_{x'}^{y'})$ *est équivalente à l'une des onze paires suivantes :*

1) (U_x^y, N_x^y) *avec* $y = m$ *ou* f *et* $x = d, r, l$ *ou* k.

2) (U_x^m, N_x^f) *avec* $x = d, r,$ *ou* l.

II. RELATIONS FORMELLES ENTRE LES CONDITIONS.

1° On vérifie directement que les huit paires suivantes — ou toute combinaison plus forte entraînent que P soit égal à S :

$(U_x^y, N_{x'}^{y'})$ avec $y \neq y'$ et (x, x') de la forme (d, k) ou (r, l).

D'autre part, certaines paires entraînent automatiquement une condition plus forte. Tenant compte de la symétrie gauche-droite, il suffit de vérifier les cas suivants :

2° Quand U_r^f, N_d^m est équivalent à N_r^f.

3° Quand N_r^m, U_d^f est équivalent à U_r^f.

4° Quand U_r^m, N_d^f est équivalent à N_r^f.

5° Quand N_r^f, U_d^m est équivalent à U_r^m.

Les démonstrations sont immédiates et le fait qu'aucune autre réduction ne se produit dans le cas général sera établi plus bas par des contre exemples.

III. DÉMONSTRATION DE LA PROPOSITION.

Toujours à cause de la symétrie, il suffira de prouver que sous les hypothèses faites l'on a :

1° Si U_r^m et N_d^m, alors N_r^m.

2° Si N_r^m et U_d^m, alors U_r^m.

3° Si U_d^f et N_d^m, alors N_d^f.

La condition $\overset{-1}{\varphi}\varphi P = P$ implique que φP satisfasse A_x^y dans φS en même temps que P satisfait la même condition dans S. On pourra donc supposer que S admet les *bi*-idéaux minimaux $K_j^i (i \in I, j \in J)$ dont l'union D est l'idéal bilatère minimum de S. On posera $R_j = \bigcup_{i \in I} K_j^i$ et $L^i = \bigcup_{j \in J} K_j^i$ et puisque toutes les conditions considérées sont plus fortes que N_d^m, on pourra supposer que $P \cap D$ contient $q \in K_{j_1}^{i_1}$.

Démonstration de 1°. Soit $s \in S$ quelconque; puisque q appartient à l'idéal à droite minimal R_{j_1}, il existe au moins un s' tel que $qss' = q$. Mais, à cause de U_r^m, cette relation implique que ss' appartienne à P. Donc, à tout $s \in S$ il correspond au moins un s' tel que $ss' \in P$ et c'est là la condition N_r^m.

Démonstration du 2°. On observe d'abord que pour tout $j \in J$, l'élément idempotent $e^{i_1}_j$ de $K^{i_1}_j$ appartient à P : en effet, N^m_r implique que pour tout $j \in J$ il existe au moins un élément, $q_j \in P \cap R_j$. On a $q_j q \in P$ et $(e^{i_1}_j q_j)\, q = q_j q = q_j(q e^{i_1}_j)$, c'est-à-dire, $e^{i_1}_j P \cap P e^{i_1}_j \cap P \neq \emptyset$; donc, d'après U^m_d, $e^{i_1}_j \in P$. Pour la même raison, l'inverse $\bar{q}$ de q dans $K^{i_1}_{j_1}$ appartient à P puisque $q\bar{q} = \bar{q}q = e^{i_1}_{j_1}$. Par conséquent, si $s \in R_{j_2}$ satisfait la relation $qs \in P \cap K^{i_2}_{j_1}$, il appartient aussi à P puisque l'on a $s = e^{i_1}_{j_2} e^{i_1}_{j_1} s = e^{i_1}_{j_2} \bar{q} q s$ et que $e^{i_1}_{j_2}$, $\bar{q}$ et qs appartiennent tous à P.

Soit maintenant t, un élément quelconque de S satisfaisant la relation $pt \in P$ pour au moins un élément $p \in P$. Multipliant à gauche par $P \cap D$, on obtient au moins une relation de la forme $q't = q''$ avec q', $q'' \in P \cap D$ et, par exemple $q'' \in K^{i_2}_j$. Puisque $qt = qte^{i_2}_j$, et, en tenant compte de la dernière remarque, $te^{i_2}_j = q'''$ appartient à P et l'on a finalement $(q'''q')t = q'''q'' = t(e^{i_2}_j q'')$ ce qui, d'après U^m_d entraîne $t \in P$. Donc $Pt \cap P \neq \emptyset$ entraîne $t \in P$ et c'est là la condition U^m_r.

Démonstration de 3°. Soit s un élément quelconque de $K^{i_1}_{j_1}$; $\bar{s}$ son inverse. Comme $e^{i_1}_{j_1} = s\bar{s} = \bar{s}s$ appartient à P ainsi que l'on vient de le voir, la condition U^l_d entraîne que s (et $\bar{s}$) appartienne à P. Donc, plus généralement, U^l_d implique que tout bi-idéal minimal qui intersecte P soit contenu dans P. Soit maintenant s quelconque, le produit $e^{i_1}_{j_1} s e^{i_1}_{j_1}$ appartient à $K^{i_1}_{j_1}$, donc à P; Donc, pour tout $s \in S$ $PsP \cap P \neq \emptyset$, ce qui est la condition N^l_d.

IV. Contre exemples.

C'est une conséquence immédiate des définitions que si $P_1 \subset S_1$ satisfait $A^{y_1}_{x_1}$ et $P_2 \subset S_2$ satisfait $A^{y_2}_{x_2}$ le produit direct $P_1 \times P_2 \subset S_1 \times S_2$ satisfait $A^{y_3}_{x_3}$ où y_3 et x_3 dépendent de x_1, x_2, y_1 et y_2 selon les tableaux suivants :

y_1 \ y_2	m	f
m	m	m
f	m	f

si $x_1 = x_2 = x_3$

x_1 \ x_2	d	r	l	k
d	d	d	d	d
r	d	r	d	r
l	d	d	l	l
k	d	r	l	k

si $y_1 = y_2 = y_3$

Avec l'aide de cette remarque, et en notant désormais par S' un demi-groupe anti-isomorphique avec S, il est possible de réduire à six le nombre des contre-exemples nécessaires. On rappelle que e désigne toujours l'élément neutre.

Cas 1. $S = (e, a, b)$; $P = (e, a)$ avec $a = a^2 = ba$; $b = b^2 = ab$.

Cas 2. $S = (e, a, b, ab)$; $P = (e, a)$ avec $e = b^2$; $a = a^2 = ba$.

Cas 3. N'importe quel sous-groupe propre d'un groupe.

Les preuves sont de simples vérifications.

Soit maintenant Z l'ensemble des entiers naturels et S le demi-groupe consistant en l'application identique e et l'ensemble des injections de Z dans lui-même telles que :

$$\text{Card } (Z.s) = \text{Card } (Z - Z.s) = \text{Card } (Z).$$

Il est bien connu que $S - e$ est formé d'un idéal à droite unique et que l'équation en s : $xs = y \neq e$ admet toujours une solution (l); donc, dans les deux cas suivants, N_r^m sera toujours satisfaite.

Cas 4. Soit s_0 un élément fixe de $S - e$; $Z_0 = Z.s_0$ et P consistant en les $a \in S$ dont la restriction à Z_0 est une bijection de cet ensemble sur lui-même.

Puisque pour tout sous-ensemble Z' de Z et tout s, $s' \in S$ on a $Z'.ss' \subset Z'.s'$, P ne peut pas satisfaire N_l^m. D'autre part, si $p \in P$, ps (ou sp) ne peuvent appartenir à P que s'il en est de même de s et, par conséquent, P satisfait U_k^m.

Cas 5. On écrit Inv (s) pour représenter le nombre cardinal de paires $(i, j) \in (Z, Z)$ telles que $i < j$ et $i.s > j.s$ et on considère $P = \{s : \text{Inv } (s) = 0\}$. Au moyen de la formule.

$$\text{Inv}(s) - \text{Inv}(s') \leqslant \text{Inv}(ss') \leqslant \text{Inv}(s) + \text{Inv}(s')$$

on vérifie que P satisfait U_l^m et non U_r^m. N_k^m est satisfaite puisque l'on peut trouver pour tout $s \in S$, s' et s'' tels que ss' et $s''s$ appartiennent à P.

Cas 6. Soit S le demi-groupe libre engendré par a et b; T_1, l'ensemble des mots de S de la forme $a^{1+m}b^{1+n}$; T, le sous-demi-groupe engendré par T_1; P_1, l'ensemble des mots de la forme $b^{|t|}ta^{|t|}$ où $t \in T$ et où $|t|$ désigne la longueur de t; P le demi-groupe engendré par P_1.

Quelque soit $s \in S$, le produit xsy où $x = b^{|s|+2}a$ et $y = ba^{|s|+2}$ appartient à P. Donc P satisfait N_d^m. Réciproquement, si $p \in P$ est de la forme $b^m a...$, l'on sait que $p = p'p''$ où $p'' \in P$ et $p' = b^m asba^m$ avec, évidemment, $m = 2 + |s|$. Donc $ps \in P$ et $p \in P$ entraînent $s \in P$ et, par symétrie, U_k^m. Soit maintenant s un élément quelconque de S

tel qu'il existe à la fois x et y satisfaisant $xs \in P$ et $sy \in P$. On peut écrire s sous la forme $ps'p'$ avec $p,p' \in P$ maximaux du point de vue de la longueur. Si s' n'était pas le mot vide, il serait à la fois un diviseur à droite et un diviseur à gauche d'un certain élément $p'' \in P$, c'est-à-dire qu'il aurait la forme $b^n a \ldots b a^{n'}$ avec les conditions mutuellement contradictoires que $n \geqslant n' + 2$ et $n' \geqslant n + 2$. Donc s appartient à P et P satisfait U_d'.

Remarque. — On observera que tous les contre-exemples, sauf le dernier, peuvent être construits au moyen de demi-groupes qui non seulement possèdent un idéal bilatère minimum, mais encore, de façon plus restrictive, consistent en l'union d'un élément unité et d'un demi-groupe d-simple selon la terminologie de Green et Clifford [3, 7].

RÉFÉRENCES

[1] R. Baer et F. Levi, *Sitzber. Heidelberg. Akad. Wiss*, **18**, 19, 1932.
[2] A. H. Clifford, *Am. J. Math.*, **70**, 521-526, 1948.
[3] A. H. Clifford, *Am. J. Math.*, **75**, 547-556, 1953.
[4] P. Dubreil, *Mem. Acad. Sci.*, Inst. France, **2**, 1-52, 1941.
[5] P. Dubreil, *Rend. Circ. Mat. Palermo*, **10**, 1-18, 1951.
[6] P. Dubreil, *Bull. Soc. Math. France*, 289-306, 1953.
[7] J. A. Green, *Ann. Math.*, **54**, 163-172, 1951.
[8] M. P. Schützenberger and R. S. Markus, *I. R. E. Trans. Inf. Theory*. 5, n° 1. 1959, pp. 12-15.

Manuscrit reçu en juin 1959.

M. P. SCHÜTZENBERGER
Maître de conférences
Faculté des Sciences de Poitiers.

ACHEVÉ D'IMPRIMER
SUR LES PRESSES DE
L'IMPRIMERIE DURAND
A CHARTRES
LE 22 JANVIER 1960.

PAPIER OFFSET BLANC VII/I
DES PAPETERIES DE FRANCE

DÉPÔT LÉGAL : 1er TRIMESTRE 1960
N° 3518.