BULLETIN DE LA S. M. F.

M.P. SCHÜTZENBERGER

Sur certains sous-monoïdes libres

Bulletin de la S. M. F., tome 93 (1965), p. 209-223

<http://www.numdam.org/item?id=BSMF_1965__93__209_0>

Bull. Soc. math. France,
93, 1965, p. 209 à 223.

(Au Professeur A. D. WALLACE, en hommage respectueux)

SUR CERTAINS SOUS-MONOÏDES LIBRES ;

PAR

MARCEL PAUL SCHÜTZENBERGER.

Soit A une partie finie non vide fixe du monoïde libre X^* engendré par l'ensemble fini X. Nous supposerons toujours que A satisfait les deux conditions suivantes :

($\mathfrak{U}'_d$). *A engendre librement un sous-monoïde de X^*.*

(C'est-à-dire qu'il existe un ensemble Y et une bijection de Y sur A pouvant être étendue à un monomorphisme dans X^* du monoïde libre engendré par Y.)

($\mathfrak{M}'_d$). *A est maximal parmi les parties de X^* qui satisfont* ($\mathfrak{U}'_d$).

La première condition équivaut à l'hypothèse que chaque mot de X^* a au plus une factorisation comme produit de mots de A, et nous aurons à considérer les conditions plus restrictives :

($\mathfrak{U}'_r$) [resp. ($\mathfrak{U}'_l$)]. *Chaque mot de X^* a au plus un facteur gauche* (resp. *droit*) *dans A.*

On verra plus loin que ($\mathfrak{U}'_d$) et ($\mathfrak{M}'_d$) entraînent l'existence d'un polynôme $T \in \mathbf{Z}[X]$ tel qu'on ait

$$(\bigstar) \qquad 1 - \sum_{a \in A} \alpha a = \left(1 - \sum_{x \in X} \alpha x\right) T,$$

où α dénote l'homomorphisme naturel de X^* dans le monoïde multiplicatif de l'anneau $\mathbf{Z}[X]$. On peut vérifier que l'ensemble $\mathfrak{T}$ des polynômes T associés aux parties finies A, qui satisfont ($\mathfrak{U}'_r$) [ou ($\mathfrak{U}'_l$)] et ($\mathfrak{M}'_d$), est la plus petite famille de polynômes contenant 1 qui soit telle que

$$\sum_{x \in X} \alpha x . T_x \in \mathfrak{T}$$

pour toute application $x \to T_x$ de X dans $\mathfrak{T} \cup \{0\}$. Ceci indique que les polynômes de $\mathfrak{T}$ n'ont « en général » aucune propriété remarquable de factorisation et motive la proposition suivante dont la vérification est le but de cette note :

PROPOSITION. — *Si le polynôme T défini par ($\bigstar$) est irréductible sur* $\mathbf{Z}[X]$, *alors A satisfait* $(\mathfrak{U}'_r)$ *ou* $(\mathfrak{U}'_l)$.

Le lecteur pourra trouver dans [4] une étude des notions utilisées ici d'un point de vue qui donne une interprétation un peu différente de cette proposition.

Résultats préliminaires. — Soit

$$K = \{k_1, k_2, \ldots, k_n\} = \{f \in X^* ; fXX^* \cap A \neq \emptyset\}$$

l'ensemble des facteurs propres gauches des mots de A, les indices étant choisis de telle sorte que k_i soit un facteur gauche de k_j seulement si $i \leqq j$, ce qui implique que k_1 soit l'élément neutre e de X^*.

(1). — *Il existe une représentation μ de X^* par des $n \times n$-matrices ayant les propriétés suivantes :*

(1.1) *Quel que soit $f \in X^*$, tous les éléments de μf appartiennent à $\{0, 1\}$ et*

$$A^* = \{f \in X^* ; (\mu f)_{1,1} = 1\}.$$

(1.2) *Posant $M = \{\mu f ; f \in X^*\}$ et $M' = \{\mu f ; f \in A^*\}$, on a*

$(\mathfrak{U}_l)$ $$M' = \{m \in M ; mM' \cap M'm \cap M' \neq \emptyset\}$$

et

$(\mathfrak{D}\mathfrak{U}_l)$ $$\emptyset = \{m \in M ; MmM \cap M' = \emptyset\}.$$

(1.3) $$1 - \sum_{a \in A} \alpha a = \det\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right), \quad \text{où la matrice} \sum_{x \in X} \alpha x . \mu x$$

appartient à l'anneau des $n \times n$ matrices ayant leurs éléments dans $\mathbf{Z}[X]$.

Preuve.

(1.1). — Nous prenons μe égale à la $n \times n$-matrice unité, et nous définissons μ par sa restriction à X en posant pour chaque $x \in X$ et $i, j \in [1, n]$:

$$(\mu x)_{i,j} = 1 \quad \text{si } j = 1 \text{ et } k_i x \in A \quad \text{ou si } j \neq 1 \text{ et } k_i x = k_j ;$$
$$= 0 \quad \text{dans tous les autres cas.}$$

Donc, pour $f \in X$, nous avons, d'une part $(\mu f)_{1,j} \neq 0$ si et seulement si $f \in A^* k_j$ et, d'autre part, $(\mu f)_{1,j} \in \{0, 1\}$. Supposant que ceci est vrai pour $f \in X^*$, nous vérifions qu'il en est encore de même pour fx $(x \in X)$.

En effet, si $(\mu fx)_{1,j} \neq 0$, on doit avoir $(\mu f)_{1,i} \neq 0$ et $(\mu x)_{i,j} \neq 0$ pour au moins un $k_i \in K$. L'hypothèse d'induction montre que $f \in A^* k_i$ et que $k_i x \in A$ ou que $k_i x = k_j$ selon que $j = 1$ ou non, et l'on a donc encore

$$fx \in A^* k_i x \subset A^* A \subset A^* \qquad \text{ou} \qquad fx \in A^* k_i x = A^* k_j.$$

Réciproquement, si $fx \in A^* A$, l'hypothèse $(\mathfrak{U}'_d)$ implique l'existence d'un et d'un seul mot $a \in A$ tel que $fx \in A^* a$, et le mot a détermine univoquement un $k_i \in K$ tel que $a = k_i x$, ce qui entraîne

$$f \in A^* k_i \qquad \text{et} \qquad (\mu fx)_{1,1} = 1;$$

si $fx \in A^* k_j$ $(j \neq 1)$, il existe un et un seul $k_i \in K$ tel que $k_j = k_i x$, et l'on a encore

$$f \in A^* k_i \qquad \text{et} \qquad (\mu fx)_{1,j} = 1.$$

On a donc montré que

$$A^* = \{ f \in X^*;\ (\mu f)_{1,1} = 1 \}$$

et que tous les éléments des premières lignes des matrices μf $(f \in X^*)$ sont 0 ou 1.

Maintenant, par construction, $(\mu k_i)_{1,i} = 1$ quel que soit $k_i \in K$; donc, pour chaque $f \in X^*$, la première ligne de la matrice $\mu k_i f$ est la somme d'un vecteur non négatif et de la $i^{\text{ième}}$ ligne de μf; puisque $(\mu k_i f)_{1,j} \in \{ 0, 1 \}$, ceci montre que $(\mu f)_{i,j} \in \{ 0, 1 \}$ identiquement, et (1.1) est vérifiée.

Il est clair que si $K' = \{ k'_1, k'_2, \ldots, k'_{n'} \}$ est l'ensemble des facteurs droits propres des mots de A, il existe aussi une représentation μ' de X^* par des $n' \times n'$-matrices ayant les mêmes propriétés que μ; on peut vérifier que, pour tout $f \in X^*$, on a $\mu f . \nu = \nu . \mu' f$, où ν est la $n \times n'$-matrice à éléments dans $\{ 0, 1 \}$ telle que $\nu_{i,i'} = 1$ si et seulement si $k_i k'_{i'} \in \{ e \} \cup A$.

(1.2). — Si les éléments (1,1) des matrices μf et $\mu f'$ sont positifs, il en est de même pour la matrice $\mu ff'$; donc M' est un sous-monoïde de M et

$$M' \subset \{ m \in M;\ mM' \cap M'm \cap M' \neq \emptyset \}.$$

Réciproquement, si les éléments (1,1) de μa, $\mu a'$, μfa et $\mu a' f$ sont positifs, il doit exister deux indices i et i' tels que $(\mu f)_{1,i}$, $(\mu a)_{i,1}$, $(\mu f)_{i',1}$ et $(\mu a')_{1,i'}$ soient positifs et l'on ne peut avoir $(\mu a' fa)_{1,1} \leq 1$ que si $i = i' = 1$, c'est-à-dire que si $f \in A^*$; donc, *a fortiori*,

$$\{ m \in M;\ mM' \cap M'm \cap M' \neq \emptyset \} \subset M',$$

et $(\mathfrak{U}_d)$ est établie.

Pour vérifier $(\mathfrak{R}_d)$, on peut toujours supposer que X contient au moins deux lettres distinctes x et x' car, sinon, $A = \{ x^n \}$, et $(\mathfrak{R}_d)$ est trivialement vraie. Supposons qu'il existe un mot $f \in X^q x'$ qui soit tel

que $M.\mu f.M \cap M' = \emptyset$, et montrons qu'en posant $b = x^g f$, l'ensemble $A' = \{b\} \cup A$ engendre librement un sous-monoïde A'^*, en contradiction avec $(\mathcal{U}'_d)$. Pour cela, soit g le mot le plus court dont il n'a pas encore été établi que la factorisation comme produit de mots de A' est unique; puisque, d'une part A engendre librement A^* et que, d'autre part, $X^* b X^* \cap A^* = \emptyset$, le seul cas qui requiert une discussion est celui de deux factorisations de g contenant chacune, au moins une fois, le mot b, et l'on peut supposer que $g = a_1 b a'_1 = a_2 b a'_2$, où $a_1, a_2 \in A^*$; $a'_1, a'_2 \in A'^*$ et où $a_2 b$ est un facteur gauche de $a_1 b$. En raison de $X^* b X^* \cap A^* = \emptyset$, $a_2 b$ n'est pas un facteur gauche de a_1; comme la définition $b = x^g f$ $(f \in X^g x', x \neq x')$ entraîne que e est le seul mot qui soit en même temps un facteur gauche et un facteur droit de b, on a donc $a_2 b = a_1 b$, et l'unicité de la factorisation de g résulte de l'hypothèse d'induction.

Ceci termine la vérification de (1.2) qui dépend donc seulement du fait que tous les éléments des matrices μf sont dans $\{0, 1\}$; si cette condition est satisfaite par une représentation ρ de X^*, on peut montrer que $F = \{f \in X^*; (\rho f)_{1,1} = 1\}$ est un sous-monoïde librement engendré par $F \cap XX^* \setminus (F \cap XX^*)^2$ et que, quand ρ est de dimension finie, $(\mathcal{U}_d)$ est équivalente à $(\mathcal{U}'_d)$ (*cf.* [4]).

(1.3). — Considérons la matrice

$$\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right)^{-1} = \mu e + \sum_{m>0} \left(\sum_{x \in X} \alpha x . \mu x\right)^m$$

dont les éléments appartiennent à l'algèbre large du monoïde commutatif libre engendré par les $\alpha x (x \in X)$. D'après (1.1) et $(\mathfrak{U}'_d)$, l'élément (1,1) de cette matrice est égal à

$$1 + \sum \{\alpha f; f \in AA^*\} = 1 + \sum_{m>0} \left(\sum_{a \in A} \alpha a\right)^m = \left(1 - \sum_{a \in A} \alpha a\right)^{-1}$$

D'autre part, ce même élément est égal au produit de $\left(\mathbf{det}\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right)\right)^{-1}$ par l'élément (1,1), soit u, de la matrice adjointe de $\mu e - \sum_{x \in X} \alpha x . \mu x$; par construction, u est égal à 1, car tous les éléments non nuls de $\sum_{x \in X} \alpha x . \mu x$ sont dans la première colonne ou au-dessus de la diagonale principale. On a donc

$$\left(\mathbf{det}\left(\mu e - \sum_{x \in X} \alpha x . \mu x\right)\right)^{-1} = \left(1 - \sum_{a \in A} \alpha a\right)^{-1}$$

et la vérification de la remarque (1) est achevée.

Le monoïde M ayant au plus 2^{n^2} éléments, nous pourrons utiliser le théorème suivant qui est dû à SUSCHKÉWITSCH, et que nous formulons dans des notations inspirées de REES [6].

THÉORÈME (SUSCHKÉWITSCH [5]). — *Soient M un monoïde fini et M' un sous-monoïde de M satisfaisant $(\mathfrak{D}_d)$. M possède un idéal bilatère unique $D = MDM$ qui est à la fois l'union des idéaux à droite minimaux $R_i = R_i M$ $(i \in I)$ et des idéaux à gauche minimaux $L_j = ML_j$ $(j \in J)$ de M. Il existe un groupe fini G, une famille d'éléments $\{g_{j,i}\}$ de G indexés par les paires $(j, i) \in J \times I$, deux sous-ensembles non vides d'indices $I' \subset I$ et $J' \subset J$, un sous-groupe G' de G et une bijection $\gamma : I \times G \times J \to D$ qui ont les propriétés suivantes :*

(S. 1) *Quels que soient (i, g, j) et $(i', g', j') \in I \times G \times J$, on a*

$$\gamma(i, g, j).\gamma(i', g', j') = \gamma(i, g.g_{j,i'}.g', j') \in R_i \cap L_{j'};$$

(S. 2) *Pour chaque $(j, i) \in J' \times I'$, l'élément $g_{j,i}$ appartient à G' et*

$$M' \cap D = \{\gamma(i, g, j) ; (i, g, j) \in I' \times G' \times J'\}.$$

Nous aurons aussi besoin de la conséquence très simple suivante du théorème de Suschkéwitsch :

(S. 3) *Il existe une représentation de M par des applications (notées multiplicativement) de I (resp. de J) dans lui-même telle que, pour chaque $m \in M$ et $i \in I$ (resp. $j \in J$), la restriction à R_i (resp. à L_j) de la translation $m' \to mm'$ (resp. $m' \to m'm$) soit une bijection de R_i (resp. de L_j) sur $R_{m.i}$ (resp. sur $L_{j.m}$).*

En effet, ceci résulte immédiatement de (S. 1) si $m \in D$. Soit $m \in M$ quelconque et pour chaque $i \in I$ prenons un $j \in J$ arbitraire. Posant

$$u = \gamma(i, (g_{j,i})^{-1}, j),$$

(S. 1) montre que $ur = r$ pour tout $r \in R_i$; d'autre part, puisque u appartient à l'idéal à gauche minimal $L_j = ML_j$, on peut écrire $mu = v = \gamma(i', g', j)$ pour une certaine paire $i' \in I$, $g' \in G$; quel que soit $r \in R_i$, on a donc $mr = mur = vr \in R_{i'}$ et l'indice i' ne dépend par conséquent que de m et de i; nous le désignerons par $m.i$. Le fait que la translation $r \to mr$ est une bijection résulte de ce qu'il en est de même pour la translation $r \to vr$, et un raisonnement symétrique s'applique aux idéaux à gauche minimaux.

Ceci étant rappelé, nous établissons les remarques suivantes :

(2). — *L'ensemble P' des $f \in X^*$ tels que $ff'X^* \cap A^* \neq \emptyset$ pour tout $f' \in X^*$ est identique à l'ensemble P des $f \in X^*$ tels que, pour tout $f' \in X^*$, on ait $A^*ff' \cap A^* \neq \emptyset$ si et seulement si $ff' \in A^*$.*

Preuve. — Puisque $A^* = \mu^{-1}M' (= \{ f \in X^* ; \mu f \in M' \})$, il suffit d'établir l'énoncé correspondant pour les sous-ensembles $\mu P' (= \{ \mu f ; f \in P' \})$ et μP de M.

Soient $p \in \mu P$ et $m \in M$ arbitraires, et prenons un élément m' de $M' \cap D$ quelconque; le produit $m'pm$ appartient au même idéal à droite minimal que m' et, d'après (S. 1) et (S. 2), nous pouvons trouver un $m'' \in M$ tel que $m'pmm'' \in M'$; comme $p \in \mu P$, cette dernière relation implique $pmm'' \in M'$, et nous avons montré que $pmM \cap M' \neq \emptyset$ quel que soit m, pour chaque $p \in \mu P$, c'est-à-dire que $\mu P \subset \mu P'$.

Soit maintenant $p \in \mu P'$. Nous allons montrer que si $m' \in M'$ et $m \in M$ satisfont $m'pm \in M'$, on a nécessairement $pm \in M'$, ce qui établira que $p \in \mu P$ et $\mu P' = \mu P$. Prenons $r \in M' \cap D$ quelconque; l'hypothèse $p \in \mu P'$ implique qu'on puisse trouver un $m'' \in M$ satisfaisant $pmrm'' \in M'$; de fait, puisque $r \in D$, le produit pmr appartient à un idéal à droite minimal, $R_{i''}$, contenant aussi $pmrm''$ et, comme ce dernier produit est dans M', l'indice i'' appartient à I'. Utilisant (S. 1), on voit que, sans perte de généralité, on peut prendre $m'' = \gamma(i'', g'', j'')$, où $(i'', j'') \in I' \times J'$. Vérifions qu'on doit avoir $g'' \in G'$; en effet, puisque $m'pm$ et r appartiennent à M', on peut écrire :

$$m'pmr = \gamma(i', g', j'),$$

où $(i', g', j') \in I' \times G' \times J'$ en vertu de (S. 2), donc, d'après (S. 1),

$$m'pmrm'' = \gamma(i', g' . g_{j', i''} . g'', j'');$$

maintenant, comme m' et $pmrm''$ appartiennent à M', on a $g' . g_{j', i''} . g'' \in G'$, où $g' \in G'$ en raison de $m' \in M'$ et $g_{j', i''} \in G'$ en raison de $(j', i'') \in J' \times I'$ et $g'' \in G'$ est établi. Nous avons donc $m'' \in M'$. Le produit pm satisfait la double égalité

$$(pmrm''m')pm = pm(rm''m'pm) = (pmrm'')(m'pm),$$

où tous les termes entre parenthèses appartiennent à M' par hypothèse ou par construction ainsi qu'on vient de le voir. Faisant appel à $(\mathfrak{U}_d)$ on en conclut que $pm \in M'$, et la vérification de $P' = P$ est achevée.

(2 *bis*). — *Une condition nécessaire et suffisante pour que A satisfasse* $(\mathfrak{U}'_r)$ *est qu'il satisfasse :*

$(\mathfrak{R}_r)$ *Tout mot de* X^* *est facteur gauche d'au moins un mot de* A^*.

Preuve. — La condition $(\mathfrak{R}_r)$ équivaut à $P' = X^*$ (c'est-à-dire, dans la théorie de Dubreil [1], à l'hypothèse que A^* est « net à droite ») donc, à $P = X^*$, donc, enfin à l'hypothèse que $A^*f \cap A^* = \emptyset$ pour tout $f \notin A^*$ (ce qui, selon [2], signifie que A^* est « unitaire à gauche »). Si cette dernière condition est satisfaite, il est clair qu'aucun mot de A n'est facteur gauche d'un autre mot de A et que, par conséquent, tout mot de X^*

a au plus un facteur gauche dans A; réciproquement, si A satisfait $(\mathfrak{U}'_r)$, et si a, $a' \in A^*$ et $f \in X^*$ sont tels que $af = a'$, on voit par induction sur le nombre des facteurs de a appartenant à A que f doit être un mot de A^* et que, par conséquent, $(\mathfrak{U}'_r)$ entraîne $P = X^*$.

Afin de pouvoir recourir à des résultats connus, nous faisons maintenant appel à des considérations un peu différentes. Soient désormais x_0 un élément distingué de X et π une bijection de $X \setminus \{x_0\}$ sur un nouvel ensemble Y; π peut être prolongé en un homomorphisme de X^* dans la structure multiplicative de $Z[Y]$ en posant

$$\pi x_0 = 1 - \sum_{x \in X \setminus \{x_0\}} \pi x,$$

et il n'y aura pas d'inconvénient à désigner aussi par π l'homomorphisme naturel de l'algèbre large $\hat{Z}[X]$ du monoïde commutatif libre engendré par les αx $(x \in X)$ dans l'algèbre large $\hat{Z}[Y]$ du monoïde commutatif libre engendré par les $y \in Y$. De plus, nous définirons Λ comme l'ensemble des homomorphismes λ de X^* dans $]0, 1]$ qui ont la forme $\lambda = \lambda'\pi$, où λ' est un homomorphisme de $Z[Y]$ dans les réels. Finalement, pour tout sous-ensemble F de X^*, nous poserons

$$\lambda_n F = n^{-1} \sum \{ \lambda f; f \in F \setminus X^n X^* \} \qquad \text{et} \qquad \lambda_\infty F = \limsup_{n \to \infty} \lambda_n F.$$

Il résulte immédiatement des définitions que $0 < \lambda f \leq 1$ pour tout $f \in X^*$, que $\lambda_n X^* = 1$ pour tout entier n et que $\lambda_\infty f X^* = \lambda f$ pour tout $f \in X^*$.

(3). — *L'application* $\lambda_\infty \mu^{-1}$ *(notée* $\bar{\lambda}$, *pour abréger) de* M *dans les réels définit une mesure de probabilité idempotente sur* M *qui a les propriétés suivantes :*

(3.1). *Quel que soit le sous-ensemble* M'' *de* M,

$$\bar{\lambda} M'' = \bar{\lambda}(M'' \cap D).$$

(3.2). *Quels que soient* $(i, j) \in I \times J$ et $m \in R_i \cap L_j$,

$$\bar{\lambda} m = (\mathrm{Card}(G))^{-1} . \bar{\lambda} R_i . \bar{\lambda} L_j > 0,$$

où

$$\sum_{i \in I} \bar{\lambda} R_i = \sum_{j \in J} \bar{\lambda} L_j = \bar{\lambda} D = 1.$$

Preuve. — Prenons M lui-même comme ensemble d'indices, et définissons, pour chaque $m \in M$, une $M \times M$ matrice ρm par la condition que, pour tout m', $m'' \in M$, l'élément (m', m'') de ρm soit égal à 1 ou

à o selon que $m'm = m''$ ou non; ρ est la représentation régulière droite de M et l'on a identiquement

$$\rho m_1 . \rho m_2 = \rho(m_1 m_2) \qquad \text{pour tout} \quad m_1, m_2 \in M.$$

Par construction, chacune des matrices ρm est une matrice stochastique; comme l'hypothèse $\lambda \in \Lambda$ implique $\sum_{x \in X} \lambda x = 1$, il en résulte que $\sum_{x \in X} \lambda x . \rho \mu x$ est une $M \times M$ matrice stochastique que nous désignerons par $\mathbf{X}$. Donc, d'après le théorème de Perron-Frobenius, la limite de $n^{-1} \sum_{0 \leq n' < n} \mathbf{X}^{n'}$, pour n tendant vers l'infini est une matrice stochastique idempotente que nous désignerons par $\overline{\mathbf{X}}$.

Maintenant, pour chaque n fini, on a

$$n^{-1} \sum_{0 \leq n' < n} \mathbf{X}^{n'} = n^{-1} \sum \{ \lambda f . \rho \mu f ; f \in X^* \setminus X^n X^* \} = \sum_{m \in M} \lambda_n \mu^{-1} m . \rho m.$$

Comme, par définition, l'élément $(\mu e, m')$ de ρm est égal à 1 ou à o selon que $m' = m$ ou non, on en conclut que $\bar{\lambda} m$ est égal à l'élément $(\mu e, m)$ de $\overline{\mathbf{X}}$. Ceci suffit pour établir $\bar{\lambda} m > 0$ et $\sum_{m \in M} \bar{\lambda} m = 1$, et le fait que $\bar{\lambda}$ est une mesure idempotente résulte immédiatement de l'idempotence de la matrice $\overline{\mathbf{X}}$. Une fois ces propriétés établies, (3.1) et (3.2) sont, aux notations près, les théorèmes 2.3.2 (*a*) et 2.3.2 (*b*) de [3].

(4). — *Il existe deux polynômes* πH, $\pi H' \in Z[Y]$ *tels qu'en désignant par* q *l'indice du sous-groupe* G' *de* G, *et en posant*

$$\pi A^* = \sum_{a \in A^*} \pi a,$$

on ait $q . \pi H . \pi H' . \pi A^* = 1$ *et que* A *satisfasse* $(\mathfrak{U}'_r)$ [*resp.* $(\mathfrak{U}'_l)$] *si et seulement si* $\pi H = 1$ (*resp.* $\pi H' = 1$).

Preuve. — Prenons un mot $a \in A^*$ fixe, tel que $\mu a \in M' \cap D$, et posons $F = \{ f \in X^* ; af \in A^* \}$. Les énoncés (S. 1) et (S. 2) montrent que pour chaque paire $(i, j) \in I \times J$, l'intersection de μF (resp. de M') avec $R_i \cap L_j$ contient exactement $\mathbf{Card}(G')$ ou zéro élément selon que $(i, j) \in I \times J'$ (resp. $\in I' \times J'$) ou non. Donc, utilisant (3.1) et (3.2), on a

$$\lambda_\infty F = \bar{\lambda}(D \cap \mu F) = q^{-1} . \bar{\lambda} L' \tag{4.1}$$

et

$$\lambda_\infty A^* = \bar{\lambda}(D \cap M') = q^{-1} . \bar{\lambda} L' . \bar{\lambda} R', \tag{4.2}$$

où

$$L' = \bigcup_{j \in J'} L_j \qquad \text{et} \qquad R' = \bigcup_{i \in I'} R_i.$$

Soit maintenant H l'ensemble des $f \in F$ qui n'admettent aucune factorisation de la forme $f = f'a'$, avec $f' \in F$ et $a' \in A$. Par définition, H est formé de facteurs droits de mots de A; donc H est fini, et $\pi H = \sum_{h \in H} \pi h$ est un polynôme de $Z[Y]$. De plus, tout $f \in F$ a au moins une factorisation de la forme $f = ha'$, où $h \in H$ et $a' \in A^*$; cette factorisation est unique car, sinon, le produit af aurait deux factorisations distinctes comme produit de mots de A en contradiction avec $(\mathfrak{U}'_d)$. On a donc

$$\lambda_n F = \sum_{h \in H} \left(\lambda h . n^{-1} \sum \{ \lambda a' ;\ a' \in A^* ;\ ha' \in X^* \setminus X^n X^* \} \right).$$

Comme H est fini, chacune des sommes

$$n^{-1} \sum \{ \lambda a' ;\ a' \in A^* ;\ ha' \in X^* \setminus X_n X^* \}$$

tend uniformément vers $\lambda_\infty A^*$ quand n tend vers l'infini, et l'on a donc

$$\lambda_\infty F = \lambda' \pi H . \lambda_\infty A^*,$$

c'est-à-dire, d'après (4.1) et (4.2),

$$\bar{\lambda} R' . \lambda' \pi H = 1 ;$$

il est clair qu'il existe aussi un polynôme $\pi H' \in Z[Y]$ tel que $\bar{\lambda} L' . \lambda' \pi H' = 1$, et la formule désirée résulte de (4.2) et du fait que toutes les égalités écrites sont identiquement vraies pour tous les $\lambda = \lambda' \pi \in \Lambda$.

Maintenant, comme $R' \subset D$, on a

$$(\lambda' \pi H)^{-1} = \bar{\lambda} R' \leqq \bar{\lambda} D = 1$$

avec égalité si et seulement si $R' = D$, c'est-à-dire $I' = I$, c'est-à-dire enfin, $P' = X^*$ et, d'après (2 *bis*), on a donc $\pi H = 1$ si et seulement si A satisfait $(\mathfrak{U}'_r)$; un raisonnement symétrique s'applique à $\pi H'$ et (4) est établie.

Fin de la vérification. — Soit maintenant $\mathbf{Q}(M)$ l'anneau engendré par les $n \times n$ matrices $m \in M$ sur le corps des nombres rationnels; pour chaque matrice $m \in \mathbf{Q}(M)$ nous désignons par $\overleftarrow{m}$ (resp. $\overrightarrow{m}$) le n-vecteur égal à la première colonne (resp. ligne) de m.

PROPOSITION. — *Il existe trois polynômes* T_1, T'_3 *et* $T_4 \in Z[X]$ *tels que*

$$1 - \sum_{a \in A} \alpha a = \left(1 - \sum_{x \in X} \alpha x\right) . T_1 . T_4 . \left(q + \left(1 - \sum_{x \in X} \alpha x\right) . T'_3\right)$$

et qu'en outre, T_1 *(resp.* T_4*) ne se réduise à* 1 *que si A satisfait* $(\mathfrak{U}'_r)$ *[resp.* $(\mathfrak{U}'_l)$*]*.

Preuve. — Soit V l'espace vectoriel sous-tendu par tous les vecteurs $\overleftarrow{m}$ $[m \in \mathbf{Q}(M)]$, $\mathbf{Q}(M)$ opérant par multiplication à gauche sur V; pour chaque $i \in I$, nous posons $\overleftarrow{r}_i = \sum_{r \in R_i} \overleftarrow{r}$, et nous définissons les sous-espaces suivants de V :

V_1 : le sous-espace sous-tendu par toutes les différences

$$\overleftarrow{r}_i - \overleftarrow{r}_{i'} \qquad (i, i' \in I);$$

V_2 : le sous-espace sous-tendu par tous les

$$\overleftarrow{r}_i \quad (i \in I);$$

V_3 : le sous-espace formé de tous les $v \in V$ tels que

$$0 = \left(\sum_{m \in L_j} \overrightarrow{m} - \sum_{m \in L_{j'}} \overrightarrow{m}\right) . v \text{ pour toutes les paires } j, j' \in J.$$

Comme la restriction de la translation $r \to mr$ $(m \in M)$ à chaque R_i est une bijection de cet ensemble sur $R_{m.i}$, ainsi qu'on l'a vu plus haut, les sous-espaces V_1 et V_2 sont invariants. D'après (S. 1), on a

$$\left(\sum_{m \in L_j} m\right)\left(\sum_{m \in R_i} m\right) = \mathbf{Card}(G) . \left(\sum_{m \in D} m\right)$$

quels que soient $(i, j) \in I \times J$. Par conséquent,

$$\left(\sum_{m \in L_j} m - \sum_{m \in L_{j'}} m\right) . r_i = 0 \quad \text{identiquement}$$

et $V_2 \subset V_3$; de plus, V_3 est invariant puisqu'il en est de même, par rapport à la multiplication à droite par les éléments de $\mathbf{Q}(M)$, de l'espace W sous-tendu par tous les vecteurs $\sum_{m \in L_j} \overrightarrow{m} - \sum_{m \in L_{j'}} \overrightarrow{m}$ $(j, j' \in J)$. Convenant que $V = V_4$, nous pouvons donc, pour $k = 1, 2, 3, 4$, définir μ_k comme la représentation de X^* induite par μ sur l'espace quotient V_k / V_{k-1} $(V_0 = \{ 0 \})$, et poser

$$T_k = 1 \text{ ou } = \mathbf{det}\left(\mu_k e - \sum_{x \in X} \alpha x . \mu_k x\right)$$

selon que V_k/V_{k-1} a pour dimension zéro ou non. D'après (1.3), nous avons

$$1-\sum_{a\in A}\alpha a=\mathbf{det}\left(\mu e-\sum_{x\in X}\alpha x.\mu x\right)=T_1T_2T_3T_4,$$

et il suffit de considérer l'homomorphisme de $\mathbf{Z}[X]$ dans $\mathbf{Z}$ qui envoie tous les $\alpha x(x\in X)$ sur zéro pour vérifier que chacun des polynômes T_k a un terme constant égal à 1; en vertu du lemme de Gauss, et du fait que le produit des T_k est dans $\mathbf{Z}[X]$, il en résulte que tous ces polynômes appartiennent à $\mathbf{Z}[X]$; nous discuterons successivement T_2, T_1, T_4 et T_3.

(T_2) *Le polynôme T_2 est égal à* $1-\sum_{x\in X}\alpha x$.

En effet, d'après (S. 3), on a

$$m.\overleftarrow{r_i}=\overleftarrow{r_{m.i}}=\overleftarrow{r_i}-\left(\overleftarrow{r_i}-\overleftarrow{r_{m.i}}\right)$$

quels que soient $m\in M$ et $i\in I$; donc V_2/V_1 a pour dimension 1, et $\mu_2 f=1$ pour tout $f\in X^*$, ce qui entraîne trivialement le résultat cherché.

(T_1) *Le polynôme T_1 est égal à 1 si et seulement si A satisfait* ($\mathfrak{U}'_r$)

D'après (S. 2), la première coordonnée de chaque vecteur $\overleftarrow{r_i}$ ($i\in I$) est égale à $\mathbf{Card}(G').\mathbf{Card}(J')$ ou a zéro selon que $i\in I'$ ou non. Donc, si μ'_2 est la représentation de X^* induite par μ sur V_2 et si i_1 est un indice fixe de I', il existe une matrice fixe $\mathbf{t}_1$ ayant ses éléments dans $\mathbf{Q}$ et satisfaisant la condition que, pour chaque $f\in X^*$, la trace $\mathbf{Tr}(\mathbf{t}_1.\mu'_2 f)$ soit égale à 1 ou à 0 selon que $f\in F_1=\{f'\in X^*;\ \mu f'.i_1\in I'\}$ ou non.

Posant

$$\mathbf{X}'_2=\sum_{x\in X}\alpha x.\mu'_2 x\qquad\text{et}\qquad T'_1=\mathbf{Tr}(\mathbf{t}_1.\mathbf{Adj}(\mu'_2 e-\mathbf{X}'_2))\in\mathbf{Q}[X],$$

on a donc

$$\alpha F_1\left(=\sum_{f\in F_1}\alpha f\right)=\mathbf{Tr}(\mathbf{t}_1.(\mu'_2 e-\mathbf{X}'_2)^{-1})$$

$$=T'_1.\mathbf{det}(\mu'_2 e-\mathbf{X}'_2)^{-1}=T'_1.\left(1-\sum_{x\in X}\alpha x\right)^{-1}.(T_1)^{-1},$$

c'est-à-dire

$$T_1.\alpha F_1=T'_1.\left(1-\sum_{x\in X}\alpha x\right)^{-1}.$$

Comme $T_1 \in \mathbf{Z}[X]$ et comme tous les coefficients des séries infinies αF_1 et $\left(1 - \sum_{x \in X} \alpha x\right)^{-1}$ sont entiers, ceci montre que T'_1 appartient aussi à $\mathbf{Z}[X]$.

De plus, pour tout homomorphisme $\lambda = \lambda' \pi \in \Lambda$, on a

$$\lambda' \pi T_1 . \lambda_\infty F_1 = \lambda' \pi T'_1 .$$

Observons maintenant que $D \cap \mu F_1 = R'$; utilisant (3.1), et la vérification de (4), on trouve

$$\lambda_\infty F_1 = \bar{\lambda} R' = (\lambda' \pi H)^{-1},$$

d'où

$$\lambda' \pi T_1 = \lambda' \pi H . \lambda' \pi T'_1$$

et enfin

$$\pi T_1 = \pi H . \pi T'_1 .$$

Donc, si $T_1 = 1$, on a $\pi T_1 = 1$, et par conséquent, $\pi H = 1$ puisque tous ces polynômes ont des coefficients entiers. Ceci prouve que $T_1 = 1$ seulement si A satisfait $(\mathfrak{U}'_r)$.

Réciproquement, si cette dernière condition est satisfaite, chacune des matrices $\mu f (f \in X^*)$ possède un et un seul élément non nul par ligne; donc tous les vecteurs $\overleftarrow{r}_i$ $(i \in I)$ sont égaux à un même multiple du n-vecteur unité, donc enfin $V_1 = \{ 0 \}$ et $T_1 = 1$ par définition.

(T_4) *$T_4 = 1$ si, et seulement si A satisfait $(\mathfrak{U}'_l)$.*

Il suffit de répéter de façon symétrique la discussion précédente puisque par construction la représentation μ_4 est isomorphe à la représentation de X^* induite par μ (opérant à droite) sur l'espace W.

(T_3) *Il existe un polynôme $T'_3 \in \mathbf{Z}[X]$ tel que*

$$T_3 = q + \left(1 - \sum_{x \in X} \alpha x\right) . T'_3 .$$

D'après la formule (4.2), on a

$$\lambda_\infty A^* . \pi H . q . \pi H' = 1$$

et, d'après les résultats qui viennent d'être obtenus,

$$\lambda_\infty A^* . \pi T_1 . \pi T'_3 . \pi T_4 = 1$$

avec, en outre, $\pi T_1 = \pi H . \pi T'_1$ et $\pi T_4 = \pi H' . \pi T'_4$, où toutes les expressions de la forme πS sont des polynômes de $\mathbf{Z}[Y]$. Il en résulte immé-

diatement que $\pi T'_1 = \pi T'_4 = 1$ et que $\pi T_3 = q$, c'est-à-dire, puisque $T_3 \in Z[X]$, que

$$T_3 = q + \left(1 - \sum_{x \in X} \alpha x\right) T'_3, \qquad \text{avec} \quad T'_3 \in \mathbf{Z}[X].$$

La vérification est achevée. On peut noter que la condition $q = 1$ équivaut à la condition

$$\emptyset = \{ f \in X^* ;\ A^* f A^* \cap A^* = \emptyset \}$$

puisque, d'une part si $q = 1$, c'est-à-dire si $G' = G$, on a $m' m m' \in M'$ pour tout $m \in M$ et $m' \in M' \cap D$ et que, d'autre part, si $G' \neq G$, les énoncés (S. 1) et (S. 2) montrent que $M' m M' \cap M' = \emptyset$ pour tout $m \in (R_i \cap L_j) \setminus M'$ quand $(i, j) \in I' \times J'$. Par conséquent, $T = T_1 T_3 T_4$ a au moins *trois* facteurs $\neq 1$ dans $\mathbf{Z}[X]$ quand A ne satisfait ni $(\mathfrak{U}'_r)$, ni $(\mathfrak{U}'_l)$ ni la condition qui vient d'être écrite.

Observation. — Par définition, l'ensemble $P = P'$ de (2) est un idéal à droite de X^*; de fait, P est le plus grand idéal à droite de X^* tel que $R' = D \cap \mu P$. Soit $B = P \setminus PXX^*$ l'ensemble engendrant P en tant qu'idéal à droite. Par construction, $P = BX^*$, et chaque mot de X^* a au plus un facteur gauche dans B; donc,

$$\lambda_\infty P = \sum_{b \in B} \lambda' \pi b \quad (= \lambda' \pi B)$$

et, d'après (3.1) et les résultats de (4), on a

$$\lambda' \pi B = \bar{\lambda}(D \cap \mu P) = \bar{\lambda} R' = (\lambda' \pi H)^{-1},$$

d'où $1 = \pi B . \pi H$ et enfin la conclusion que B est un ensemble fini (c'est-à-dire $\pi B \in Z[Y]$) si et seulement si $H = 1$, c'est-à-dire si A satisfait $(\mathfrak{U}'_r)$. Il nous semble intéressant, en raison de la signification donnée dans [4] à la condition $\mathbf{Card}(B) < \infty$, de fournir une vérification strictement combinatoire de ce résultat. Nous supposons désormais que $B \neq \{ e \}$, [c'est-à-dire que $P = X^*$ et, d'après (2 *bis*), que A ne satisfait pas $(\mathfrak{U}'_r)$] et nous employons les notations introduites dans la discussion de (4). Nous avons d'abord :

Tout mot de X^* est facteur gauche d'au moins un mot de HBX^* et possède au plus un facteur gauche dans HB.

En effet, soit $f \in X^*$; comme par hypothèse $a \in \mu^{-1}(D \cap M') \subset P'$, il existe au moins un $f' \in X^*$ tel que $aff' \in A^*$, et l'on peut écrire $ff' = ha'$, avec $h \in H$ et $a' \in A^*$; considérons $ff'a$; comme $a \in \mu^{-1}(D \cap M')$ et

$a' \in A^*$, le mot $a'a$ appartient à P, et a donc un et un seul facteur gauche $b \in B$; nous avons donc $ff'a = hbf_1$ pour un certain $f_1 \in X^*$, et nous avons montré que tout mot de X^* est facteur gauche d'au moins un mot de HB. Gardons les mêmes notations et supposons que $ff'a = hbf_1$ est égal à $h'b'f_2$, où $h' \in H$, $b' \in B$, $f_2 \in X^*$ et où, par exemple, h' est un facteur gauche de h; nous avons $ahbf_1 = ah'b'f_2 \in A^*$; comme d'après $(\mathfrak{U}'_d)$, tout mot de X^* a au plus une factorisation comme produit de mots de A et comme $b'f_2 \in A^*$ en raison de $h' \in H$ qui entraîne $ah' \in A^*$ et de $b' \in B \subset P$, ceci n'est possible que si $h = h'a''$ pour un certain $a'' \in A^*$; en vertu de la définition de H, cette dernière relation entraîne $a'' = e$, c'est-à-dire $h = h'$, d'où $b = b'$ et la vérification de ce résultat intermédiaire est achevée.

Nous montrons maintenant que B est un ensemble infini en vérifiant que la longueur de ses mots n'est pas bornée. Comme H est un ensemble fini, nous pouvons prendre un mot $h \in H$ fixe qui ait la propriété de n'être facteur gauche d'aucun autre mot de H. Soit b un mot quelconque de $B \cap XX^*$; on a $b = fx$, où $f \in X^*$ et $x \in X$. Il existe au moins un mot $f' \in X^*$ tel que $ff'X^* \cap BX^* = \emptyset$ car, sinon, on aurait $ff'X^* \cap A^* = \emptyset$ pour tout $f'' \in X^*$, c'est-à-dire $f \in P'$ en contradiction avec la définition même de f.

On vient de voir que le mot hff' est facteur gauche d'au moins un mot de HBX^*; en prenant f' assez long, on peut faire en sorte qu'il existe $h' \in H$ et $b' \in B$ tels que $h'b'$ soit un facteur gauche de hff' et qu'on ait toujours $ff'X^* \cap BX^* = \emptyset$; on sait aussi que h' et b' sont déterminés de façon univoque par hff'. Maintenant, on ne peut pas avoir $h = h'$, car ceci entraînerait que b' soit un facteur gauche de ff' en contradiction avec $ff'X^* \cap BX^* = \emptyset$; donc h' est un facteur gauche propre de h. De plus, $h'b'$ ne peut pas être un facteur gauche de hf, car ceci entraînerait que $hfx = hb$ a deux facteurs gauches distincts dans HB; donc hf est un facteur gauche propre de $h'b'$, et nous avons obtenu la conclusion désirée que la longueur de b' est strictement plus grande que celle de b. Ceci termine la vérification du fait que si A ne satisfait pas $(\mathfrak{U}'_r)$ l'ensemble B, et par conséquent l'ensemble C, de ses facteurs gauches propres sont deux ensembles infinis.

BIBLIOGRAPHIE

[1] DUBREIL (Paul). — *Contributions à la théorie des demi-groupes*, I. — Paris, Gauthier-Villars, 1941 (Mémoires de l'Académie des Sciences de l'Institut de France, série 2, t. 63, 51 pages).

[2] DUBREIL (Paul). — Contribution à la théorie des demi-groupes, II, *Rendiconti di Matematica*, Roma, série 5, t. 10, 1951, p. 183-200.

[3] GRENANDER (Ulf). — *Probabilities on algebraic structures.* — New York, J. Wiley and Sons, 1963.

[4] NIVAT (Maurice). — Éléments de la théorie générale des codes, *Cours de l'École d'été de Ravello*, 1964.

[5] REES (D.). — On semi-groups, *Proc. Cambridge phil. Soc.*, t. 36, 1940, p. 387-400.

[6] SUSCHKÉWITSCH, A. — Ueber die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit, *Math. Annalen*, t. 99, 1928, p. 30-50.

(Manuscrit reçu le 24 janvier 1965.)

Marcel Paul SCHÜTZENBERGER,
Institut Blaise Pascal,
23, rue du Maroc, Paris, 19e.