JOURNAL OF ALGEBRA 52, 437–459 (1978)

La Finitude des Représentations Linéaires des Semi-groupes est Décidable

GÉRARD JACOB

Université Lille I, UER d'IEEA, Lille, France

Communicated by P. M. Cohn

Received September 7, 1976

We give here an effective decision procedure for the finiteness of a linear semigroup over a commutative field. In order to do this, we define notions of rank and image over semigroups, and develop combinatorial methods which we have used previously in a paper concerning factorization properties in matrix semigroups. In the case of a semigroup H of endomorphisms of a finite-dimensional vector space E over a skewfield, we prove that a congruence is finite over H if and only if it is finite over a class of canonically defined groups of automorphisms of subspaces of E, in other terms, over a class of subsemigroups of End(E), which for that reason we call the characteristic groups of H. This paper proves, as a direct consequence, the "Burnside theorem" for matrix semigroups over a commutative field, already proved in another way by McNaughton and Zalcstein. In addition, we prove the decidability of the finiteness. We also give an effective decision procedure for local testability of matrix semigroups over skewfields.

INTRODUCTION

La première intention de ce texte est de prolonger les méthodes que nous avons introduites dans [2] pour établir que l'on peut décider de la finitude des représentations linéaires des semi-groupes de matrices sur un corps commutatif. Ce résultat prolonge et précise le "théorème de Burnside" sur les semi-groupes de matrices, obtenu par McNaughton et Zalcstein [6].

Gardant de l'algèbre linéaire (en dimension finie) certaines propriétés élémentaires du rang et de l'image, nous définissons une notion de "représentation ordonnée à droite," dont les représentations linéaires fournissent un exemple. On verra que l'on a obtenu ainsi un outil très fécond pour l'analyse structurelle des semi-groupes munis d'une représentation ordonnée de rang borné—ou localement borné—relativement aux problèmes de finitude. Nous mettons alors en relief la notion d'*Im-noyau* d'un semi-groupe: ce sont les sous-semi-groupes de type fini sur lesquels l'image reste constante. Les Im-noyaux d'un semi-groupe H contiennent toute l'information concernant sa finitude. Mieux, une

0021-8693/78/0522-0437$02.00/0

congruence est localement finie sur H si et seulement si elle est finie sur tous ses Im-noyaux. Et la finitude d'une congruence est décidable sur H si et seulement si elle est décidable sur tous ses Im-noyaux.

Dans le cas d'une représentation linéaire sur un espace vectoriel E de dimension finie sur un corps quelconque (skewfield), les Im-noyaux sont particulièrement simples. Ils sont formés d'endomorphismes de E qui ont tous même image, et induisent sur cette image des automorphismes. En se restreignant à cette image, on peut donc attacher à tout Im-noyau un groupe d'automorphismes d'un sous-espace de E, ou encore un sous-groupe de End E, qui lui est canoniquement associé, et que nous appelons le "groupe caractéristique" de cet Im-noyau. Il est clair qu'un Im-noyau est fini si et seulement si son groupe caractéristique est fini.

Pour décider si un semi-groupe linéaire est fini, il faut donc décider de la finitude de ses groupes caractéristiques. Nous le ferons—sur un corps commutatif—en suivant pas à pas la démonstration du théorème de Burnside pour les groupes de matrices, telle qu'elle est donnée dans Kaplansky [4], en observant qu'elle peut être refaite de manière constructive.

Pour un exposé plus systématique de l'algorithme que nous obtenons, nous renvoyons le lecteur à [3]. Nous nous contenterons ici d'en exposer les grandes lignes. Nous avons en effet choisi, dans le texte qui suit, de développer davantage, d'une part les techniques combinatoires, d'autre part la présentation des propriétés algébriques structurelles mises en valeur par nos résultats.

Ceci nous amène à proposer le plan suivant:

1. Rang sur un semi-groupe.
2. Images à droite, représentations ordonnées à droite.
3. Théorèmes de finitude et de décidabilité.
4. La finitude des semi-groupes linéaires est décidable (sur un corps commutatif).
5. Relativisations de la notion de finitude.

1. Rang sur Semi-groupe

Nous précisons ici les résultats de factorisation que l'on peut obtenir en développant la technique mise en œuvre dans [2].

Soit donc X un ensemble quelconque, aussi appelé alphabet. On note X^* le monoïde libre sur X, dont les éléments sont aussi appelés mots. Un mot f de X^* est dit de longueur k (notation: $|f| = k$) si f appartient à X^k, où k est un entier positif. L'élément neutre de X^* est le mot vide de X^*, que nous notons e. La longueur du mot vide est zéro. Le sous-semi-groupe de X^* formé des mots non vides est le semi-groupe libre X^+ sur X.

Notation. Soient H un semi-groupe, et $[H]$ l'ensemble sous-jacent. Nous appelons *phrase sur* H tout mot de $[H]^*$. Une phrase w' sur H est une *sous-phrase* d'une phrase w si et seulement si le mot w' de $[H]^*$ est un facteur, ou sous-mot de w. On notera alors:

$$w' \subseteq w.$$

Si w est une phrase sur H appartenant à $[H]^k$, on dira qu'elle est de *longueur* k, et on la notera sous forme d'une suite:

$$w = (g_1, g_2, \ldots, g_k).$$

La *réalisation de* w *dans* H est le produit dans H défini par:

$$w_x = g_1 g_2 \cdots g_k .$$

Une phrase w sur un semi-groupe libre X^+ sera dite *phrase extraite d'une mot* f *de* X^+ si et seulement si sa réalisation w_x est un facteur, ou sous-mot du mot f.

DÉFINITION 1.1. On appelle *rang sur un semi-groupe* H toute application ρ de H dans $\mathbf{N}$ qui vérifie:

$$\forall f, g \in H, \qquad \rho(fg) \leqslant \inf(\rho f, \rho g).$$

Le rang ρ sur H est dit *borné* s'il existe un entier m_0 vérifiant:

$$\forall f \in H, \qquad \rho f \leqslant m_0 .$$

On dira dans ce cas que ρ est *majoré par* m_0 .

DÉFINITION 1.2. Soient ρ un rang sur un semi-groupe H et $w = (g_1, g_2, \ldots, g_k)$ une phrase sur H. Nous dirons que ρ est *constant sur la phrase* w si l'on a:

$$\forall i \in [1, k] \subset \mathbf{N}, \qquad \rho(g_i) = \rho(g_1 g_2 \cdots g_k).$$

En d'autres termes, ρ est constant sur w si et seulement si pour toute sous-phrase w' de w on a l'égalité:

$$\rho(w_x') = \rho(w_x).$$

Nous rappelons maintenant — avec des notations légèrement modifiées — l'énoncé du lemme technique établi dans un précédent article [2].

LEMME 1.1. *Pour toute fonction ν de* **N** *dans* **N**, *il existe une fonction $R(\nu)$ de* **N** *dans* **N**, *vérifiant la condition suivante*:

pour tout rang ρ sur X^+ majoré par un entier m_0 et tout mot f de X^+ de longueur au moins égale à $R(\nu, m_0) = R(\nu)(m_0)$, et de rang non nul, on peut trouver:

— *un entier s non nul,*

— *une phrase w extraite de f de la forme*

$$w = (g_1, g_2, \ldots, g_{\nu(s)}) \text{ avec } 1 \leqslant |g_i| \leqslant s$$

tels que ρ soit constant sur la phrase f.

Preuve. Pour la preuve du lemme 1.1, nous renvoyons à [2], où nous avons établi ce résultat en construisant une telle fonction $R(\nu)$ comme suit, par récurrence.

$$R(\nu, 1) = \nu(1),$$
$$R(\nu, n+1) = R(\nu, n) \cdot \nu(R(\nu, n)).$$

COROLLAIRE 1.1. *Pour toute fonction μ de* **N** *dans* **N**, *il existe une fonction $S(\mu)$ de* **N** *dans* **N** *vérifiant la propriété suivante*:

pour tout alphabet de cardinal au plus égal à un entier d, et tout mot f de V^+ de longueur au moins égale à $S(\mu, d) = S(\mu)(d)$, on peut trouver

— *un entier s non nul,*

— *une phrase w extraite de f de la forme*

$$w = (v, h_1, v, h_2, v, \ldots, v, h_{\mu(s)}, v)$$

avec

$$v \in V \text{ et } 1 \leqslant |h_i v| \leqslant s$$

Preuve. Définissons une fonction ν de **N** dans **N** en posant:

$$\forall t \in \mathbf{N}, \qquad \nu(t) = 1 + \mu(2t - 1).$$

Pour tout mot f de V^+, notons $\rho(f)$ le nombre de lettres de V qui ne sont pas utilisées pour écrire f. Alors ρ est un rang sur V^+ majoré par d. Si f est de longueur au moins égale à $R(\nu, d)$, il existe d'après le lemme 1.1, un entier t et une phrase w_1 extraite de f

$$w_1 = (g_1, g_2, \ldots, g_{\nu(t)}) \text{ avec } 1 \leqslant |g_i| \leqslant t,$$

sur laquelle le rang ρ est constant.

On en déduit que chacun des mots g_i est écrit en utilisant exactement le même ensemble de lettres de V. Choisissons l'une de ces lettres et notons-la v:

on trouvera v dans chacun des g_i, et deux occurences de v ainsi repérées dans les mots g_i et g_{i+1} seront séparées par au plus $(2t-2)$ lettres. On obtient donc une phrase extraite de f de la forme:

$$w = (v, h_1, v, h_2, v, \ldots, v, h_{\nu(t)-1}, v), \qquad 1 \leqslant |h_i v| \leqslant 2t-1.$$

C'est bien la phrase cherchée, correspondant à la valeur de s:

$$s = 2t - 1.$$

THÉORÈME 1. *Soit X un alphabet fini de cardinal d.*

Pour toute fonction α de $\mathbf{N}$ dans $\mathbf{N}$, il existe une fonction $T_d(\alpha)$ de $\mathbf{N}$ dans $\mathbf{N}$ vérifiant la propriété:

pour tout rang ρ sur X^+ majoré par un entier m_0 et tout mot f de X^+ de longueur au moins égale à $T_d(\alpha, m_0) = T_d(\alpha)(m_0)$, on peut trouver:

— *un entier s non nul*

— *une phrase extraite de f de la forme:*

$$w = (u, f_1, u, f_2, u, \ldots, u, f_{\alpha(s)}, u),$$
$$1 \leqslant |f_i u| \leqslant s \text{ et } |u| \neq 0$$

tels que ρ soit constant sur w.

Preuve du théorème 1. Pour tout entier p, notons d_p le cardinal de l'ensemble des mots non vides de longueur au plus p sur l'alphabet X à d éléments. On a:

$$d_p = \frac{d - d^{p+1}}{1 - d}.$$

Pour tout entier n, soit λ_n la fonction de $\mathbf{N}$ dans $\mathbf{N}$ définie par:

$$\forall s \in \mathbf{N}, \qquad \lambda_n(s) = \alpha(n \cdot s)$$

Nous posons enfin pour tout entier n:

$$\nu_d(n) = S(\lambda_n, d_n) \qquad \text{(cf. corollaire 1.1)},$$
$$T_d(\alpha, m_0) = R(\nu_d, m_0) \qquad \text{(cf. lemme 1.1)}.$$

Si f est un mot de X^+ de longueur au moins égale à $T_d(\alpha, m_0)$, il existe d'après le lemme 1.1 un entier p, et une phrase w_1 extraite de f de la forme:

$$w_1 = (g_1, g_2, \ldots, g_{\nu(p)}) \text{ avec } 1 \leqslant |g_i| \leqslant p$$

sur laquelle ρ est constant.

Soit V l'alphabet dont les lettres sont les mots de X^+ de longueur au plus égale à p. Considérons w_1 comme un mot sur l'alphabet V, de longueur:

$$| w_1 | = v(p) = S(\lambda_p , d_p).$$

D'après le corollaire 1.1, il existe un entier t strictement positif et une phrase extraite du mot w_1 de la forme:

$$w_2 = (v, h_1 , v, h_2 , v,..., v, h_{\alpha(p\cdot t)} , v)$$

avec

$$1 \leqslant | h_i v | \leqslant t$$

où v est une lettre de V, et où la longueur $| h_i v |$ est calculée dans V^+.

Remplaçant à présent chacun des mots v et h_i par sa réalisation dans X^+, on obtient une phrase extraite de f de la forme:

$$w = (u, f_1 , u, f_2 , u,..., u, f_{\alpha(p\cdot t)} , u)$$

où l'on a posé: $u = v_x$; $f_i = (h_i)_x$, avec les conditions:

$$1 \leqslant i \leqslant \alpha(p \cdot t) \Rightarrow 1 \leqslant | f_i u | \leqslant p \cdot t.$$

La phrase w est donc la phrase cherchée, correspondant à l'entier:

$$s = p \cdot t$$

2. Images à droite — représentations ordonnées à droite

Après avoir formalisé la notion de rang, nous allons formaliser la notion d'image d'un endomorphisme d'un espace vectoriel de dimension finie. Nous définirons la notion de régularité d'un semi-groupe par rapport à l'image, généralisant la notion d'"endomorphisme pseudo-régulier" étudiée dans [3].

Définition 2.1. Nous appelons *degré sur un ensemble ordonné* Δ la donnée d'une application δ de Δ dans $\mathbf{N}$ vérifiant: δ est une application ordonnée,

$$(\delta(d) = \delta(d') \text{ et } d \leqslant d') \Rightarrow d = d'.$$

En d'autres termes, un degré sur Δ est une application strictement croissante de Δ dans $\mathbf{N}$.

Définition 2.2. Nous appelons *image à droite sur un semi-groupe* H la

donnée d'une application Im de H dans un ensemble ordonné à degré (Δ, δ) vérifiant les propriétés:

(i) *stabilité à droite*

$$\forall f, g, h \in H, \qquad \operatorname{Im} f = \operatorname{Im} h \Rightarrow \operatorname{Im} fh = \operatorname{Im} gh,$$

(ii) *décroissance à gauche*

$$\forall f, h \in H, \qquad \operatorname{Im} fh \leqslant \operatorname{Im} h,$$

(iii) *décroissance à droite "modulo le degré"*

$$\forall f, h \in H, \qquad (\delta \circ \operatorname{Im}) fh \leqslant (\delta \circ \operatorname{Im}) f.$$

L'application $\rho = \delta \circ \operatorname{Im}$ est alors un rang sur H.

On peut restreindre Δ à l'ensemble des images par Im des éléments de H. De plus, si H est un monoïde, l'ensemble $\operatorname{Im}(H)$ posséde un plus grand élément $\operatorname{Im}(1_H)$. La donnée d'une fonction image à droite sur un monoïde équivaut alors à celle d'une "représentation ordonnée à droite":

DÉFINITION 2.3. Nous appelons *représentation ordonnée à droite d'un semi-groupe* H sur un ensemble ordonné à degré (Δ, δ) muni d'un plus grand élément noté E, la donnée

(i) *d'une action* $*$ *de* H *à droite sur* Δ, *vérifiant*:

(ii) *décroissance à gauche*

$$\forall f, h \in H, \qquad E * fh \leqslant E * h,$$

(iii) *décroissance à droite "modulo le degré"*

$$\forall f, h \in H, \qquad \delta(E * fh) \leqslant \delta(E * f).$$

En effet, si Im est une fonction image à valeur dans (Δ, δ) et si Im est surjective, on définit une représentation à droite de H en posant:

$$\forall f, h \in H, \qquad (\operatorname{Im} f) * h = \operatorname{Im} fh,$$
$$E = \operatorname{Im} 1_H .$$

Inversement, étant donnée une représentation ordonné à droite de H sur (Δ, δ), on définit sur H une fonction image à droite en posant:

$$\forall f \in H, \qquad \operatorname{Im} f = E * f.$$

En particulier, si E est un espace vectoriel de dimension finie sur un corps quelconque (skewfield), soit Δ le treillis des sous-espaces vectoriels de E, et soit δ l'application qui associe à chacun des sous-espaces de E sa dimension. Le couple (Δ, δ) est un ensemble ordonné à degré. On définit canoniquement une image à droite sur le semi-groupe End(E): elle associe à chaque endomorphisme son image, au sens algébrique du terme. On notera que nous avons choisi de faire opérer les endomorphismes à droite sur E.

DÉFINITION 2.4. Soit Im une image à droite sur un semi-groupe H à valeur dans un ensemble ordonné à degré (Δ, δ). Une phrase sur H de la forme:

$$w = (g_1, g_2, g_3, \ldots, g_k)$$

est dite Im-régulière si et seulement si pour tout entier p et toute application θ de l'intervalle $[1, p]$ de $\mathbf{N}$ dans $[1, k]$, on a l'égalité:

$$\mathrm{Im}(g_{\theta(1)} g_{\theta(2)} \cdots g_{\theta(p)}) = \mathrm{Im}(g_1 g_2 \cdots g_k).$$

En d'autres termes, la phrase $w = (g_1, g_2, \ldots, g_k)$ est Im-régulière si et seulement si le semi-groupe engendré par les g_i est tout entier contenu *dans une même fibre de H au dessus de* Δ pour l'application Im.

LEMME 2.1. *Soit* $\rho = \delta \circ \mathrm{Im}$ *le rang sur un semi-groupe H, défini par une fonction image à droite* Im. *Si* ρ *est constant sur une phrase v de la forme*:

$$v = (u, f_1, u, f_2, u, \ldots, u, f_k, u)$$

alors la phrase w suivante:

$$w = (f_1 u, f_2 u, \ldots, f_k u)$$

est Im-*régulière et son image vaut* Im u.

Preuve. On a clairement les inégalités:

$$\mathrm{Im}\ uf_j u \leqslant \mathrm{Im}\ f_j u \leqslant \mathrm{Im}\ u,$$
$$\mathrm{Im}\ uf_i u \leqslant \mathrm{Im}\ f_i u \leqslant \mathrm{Im}\ u.$$

De plus, ces inégalités sont en fait des égalités à cause de la propriété de rang constant. Par stabilité à droite, on obtient:

$$\mathrm{Im}\ f_i\ uf_j u = \mathrm{Im}\ uf_j u = \mathrm{Im}\ f_j u = \mathrm{Im}\ u,$$
$$\mathrm{Im}\ f_j\ uf_i u = \mathrm{Im}\ uf_i u = \mathrm{Im}\ f_i u = \mathrm{Im}\ u.$$

Par la même méthode et l'usage d'une induction sur k, on obtient aisément le résultat.

THÉORÈME 2. *Soit X un alphabet fini de cardinal d. Pour toute fonction α de* **N** *dans* **N**, *il existe une fonction $T_d(\alpha)$ de* **N** *dans* **N** *vérifiant*:

pour toute image à droite Im *de X^+ dans un ensemble ordonné à degré (Δ, δ) majorée par un entier m_0 et pour tout mot f de X^+ de longueur au moins égale à $T_d(\alpha, m_0)$, on peut trouver*

— *un entier s non nul,*

— *une phrase w extraite de f de la forme*:

$$w = (g_1, g_2, \ldots, g_{\alpha(s)})$$

avec

$$1 \leqslant |g_i| \leqslant s$$

tels que w soit Im-*régulière.*

Preuve. La fonction $T_d(\alpha)$ a été définie dans le théorème 1. Le résultat suit du théorème 1, à condition d'y poser:

$$f_i u = g_i .$$

Le lemme 2.1 permet de conclure.

THÉORÈME 3. *Soit X un alphabet fini de cardinal d. Pour toute fonction β de* **N** *dans* **N**, *il existe une fonction $L_d(\beta)$ de* **N** *dans* **N** *vérifiant*:

pour toute image à droite Im *sur X^+ majorée par un entier m_0, et pour tout mot f de X^+ de longueur au moins égale à $L_d(\beta, m_0)$, on peut trouver*:

— *un entier s non nul,*

— *une phrase w extraite de f de la forme*:

$$w = (g_1, g_2, \ldots, g_{\beta(s)}),$$
$$\mathrm{Card}\{g_i \mid 1 \leqslant i \leqslant \beta(s)\} \leqslant s.$$

Preuve. Définissons une fonction α de **N** dans **N** en posant:

$$\forall s \in \mathbf{N}, \qquad \alpha(s) = \beta(d_s) = \beta\left(\frac{d - d^{s+1}}{1 - d}\right).$$

Nous posons alors:

$$L_d(\beta, m_0) = T_d(\alpha, m_0).$$

On conclut alors par le lemme 2.2, en remarquant que d_s est le nombre de mots de X^+ de longueur inférieure ou égale à s.

Le lemme suivant a pour but d'interpréter la notion de phrase Im-régulière dans le cas des semi-groupes linéaires.

LEMME 2.2. *Soit E un espace vectoriel sur un corps K quelconque, et soit ψ une suite finie d'endomorphismes de E de rang fini*:

$$\psi = (\phi_1 , \phi_2 ,..., \phi_k).$$

Il y a équivalence entre les énoncés suivants:

(i) *ψ est une phrase* Im-*régulière*,

(ii) *les ϕ_j ont tous même image E_1 , et chacun d'eux induit sur E_1 un automorphisme*,

(iii) *il existe un idempotente e_1 de End(E) qui opère par produit à droite sur les ϕ_j comme l'identité, et tel que les endomorphismes $e_1 . \phi_j$ engendrent un semi-groupe régulier*,

(iv) *les ϕ_j sont tous nuls, ou alors il existe une base de E dans laquelle chaque ϕ_j puisse s'écrire, pour une décomposition par blocs commune aux ϕ_j , sous la forme*:

$$\begin{pmatrix} A_j & 0 \\ B_j & 0 \end{pmatrix}$$

où les matrices A_j sont des matrices carrées inversibles.

Preuve. (i) $\Rightarrow$ (ii) Soit E_1 le sous-espace de E, image commune attachée à la phrase Im-régulière ψ. On a alors:

$$\text{Im } \phi_i = E_1 = \text{Im } \phi_i\phi_j = \phi_j(\text{Im } \phi_i).$$

On en déduit que les ϕ_j induisent sur E_1 des automorphismes.

(ii) $\Rightarrow$ (iii) Soit e_1 un endomorphisme de projection de E sur E_1 . Il est défini par une décomposition directe $E = E_1 + E_0$. Pour tout i, l'endomorphisme $e_1\phi_i$ est nul sur E_0 , et induit sur E_1 le même automorphisme que ϕ_i . Le semi-groupe engendré par les $e_1\phi_i$ est alors régulier, puisqu'il est isomorphe à un semi-groupe d'automorphismes de E_1 .

(iii) $\Rightarrow$ (iv) On choisit une base de E qui soit réunion d'une base de E_1 et d'une base de E_0 . L'énoncé (iv) ne fait que traduire (iii) en écriture matricielle.

(iv) $\Rightarrow$ (i) C'est une conséquence immédiate des calculs de produits:

$$\begin{pmatrix} A_i & 0 \\ B_i & 0 \end{pmatrix}\begin{pmatrix} A_j & 0 \\ B_j & 0 \end{pmatrix} = \begin{pmatrix} A_iA_j & 0 \\ B_iA_j & 0 \end{pmatrix}.$$

3. Théorèmes de finitude et de décidabilité

Nous avons pour but de mettre ici en évidence la notion d'*Im-noyau*. Il s'agit là d'une notion essentielle lorsque l'on veut étudier les problèmes de finitude. De plus elle apparaît dès que l'on étudie la structure induite sur un semi-groupe par une représentation ordonnée à droite; elle permet alors de réinterpréter le théorème 3 en termes de structure. Dans le cas des semi-groupes linéaires, à chaque Im-noyau sera canoniquement associé un *groupe caractéristique*. Les groupes caractéristiques d'un semi-groupe linéaire joueront exactement le même rôle, en ce qui concerne la finitude des congruences, et la décidabilité de cette finitude, que celui joué (théorèmes 4 à 8) par les Im-noyaux dans le cas général.

Dans toute cette partie, nous raisonnons sur une présentation d'un semi-groupe H, c'est-à-dire sur la donnée d'un ensemble S de générateurs de H. Le *type* de la présentation (H, S) est le cardinal de S. Le semi-groupe H est *de type fini* s'il admet une présentation de type fini; il est *de type k* (entier) s'il admet une présentation de type k, mais n'admet pas de présentation de type k' strictement inférieur à k.

Définition 3.1. Nous appelons *largeur de H pour la présentation* (H, S) le plus petit entier j, s'il existe, vérifiant:

$$S^j \subset S \cup S^2 \cup \cdots \cup S^{j-1}.$$

La largeur de H pour la présentation (H, S) est infinie si un tel entier n'existe pas.

La *largeur de H* (sens absolu) est la borne supérieure des largeurs de H pour toute présentation de H.

Si H est de type fini et de largeur finie, il est fini. Noter qu'un semi-groupe peut être localement fini sans être de largeur finie.

Avant de démontrer les théorèmes fondamentaux, il nous faut préciser quel est l'outil de description structurelle que nous fournissent les théorèmes 2 et 3, relativement à la finitude et à sa décidabilité.

Définition 3.2. Soit Im une fonction image à droite sur un semi-groupe H, à valeur dans un ensemble ordonné à degré. Nous appellerons *Im-noyau* l'objet défini par l'un des énoncés équivalents suivants:

(i) tout semi-groupe engendré par les "mots" de H utilisés pour écrire une phrase Im-régulière sur H.

(ii) tout sous-semi-groupe de H de type fini et Im-régulier.

(iii) tout sous-semi-groupe de type fini de H contenu dans une seule fibre de H au dessus de Δ.

Soit à présent H un semi-groupe linéaire, muni canoniquement d'une applica-

tion image à droite à valeur dans le treillis Δ des sous-espaces d'un espace vectoriel de dimension finie E sur un corps quelconque (skewfield).

A tout élément d de Δ, on peut attacher un idempotent e de End(E) qui opère par produit à droite comme l'identité sur d, et donc aussi sur $\mathrm{Im}^{-1}(d)$, et dont l'image dans Δ est d. Nous l'appellerons idempotent caractéristique de d. Avec les notations du lemme 2.2, d est l'espace vectoriel E_1, image commune à toute une phrase Im-régulière. Le choix de l'idempotent e correspond biunivoquement au choix d'un sous-espace supplémentaire de E_1 dans E.

DÉFINITION 3.3. Soit $\mathcal{N}$ un Im-noyau du semi-groupe linéaire H, et soit d l'élément de $\mathcal{N}$ dont la fibre contient $\mathcal{N}$. Nous appellerons *groupe caractéristique de H attaché à $\mathcal{N}$*, le groupe $G(\mathcal{N})$ engendré par le semi-groupe régumier $e = e\mathcal{N}e$, où e désigne un idempotent caractéristique de d.

Le groupe caractéristique $G(\mathcal{N})$ est donc défini à similitude près.

En d'autres termes, si $\mathcal{N}$ est engendré par une suite finie de matrices simultanément réduites (cf. lemme 2.2) sous la forme:

$$\begin{pmatrix} A_i & 0 \\ B_i & 0 \end{pmatrix}$$

où les A_i sont des matrices carrées inversibles, alors $G(\mathcal{N})$ est le groupe engendré par les matrices A_i.

LEMME 3.1. *Soit H un semi-groupe linéaire. Un Im-noyau $\mathcal{N}$ de H est fini si et seulement si le groupe caractéristique $G(\mathcal{N})$ est fini.*

Preuve. Soit N un système (fini) de générateurs de $\mathcal{N}$. D'après la forme de la représentation matricielle, on voit que tout élément de $\mathcal{N}$ s'écrit comme produit d'un élément de N par un élément du monoïde $\{e\} \cup e\mathcal{N}e$, où e est l'idempotent caractéristique associé à $\mathcal{N}$. Donc $\mathcal{N}$ est fini si et seulement si $e\mathcal{N}e$ est fini.

On conclut soit directement, soit par le lemme suivant.

LEMME 3.2. *Soit H un semi-groupe linéaire. Tout Im-noyau fini $\mathcal{N}$ de H contient un sous-groupe isomorphe au groupe caractéristique $G(\mathcal{N})$. En particulier, tout semi-groupe de matrices périodiques contient au moins un sous-groupe isomorphe à chaque groupe caractéristique.*

Preuve. Tout Im-noyau fini $\mathcal{N}$ contient une matrice périodique, dont une puissance est un idempotent e. Il est clair que e opère par produit à droite comme l'identité sur l'image de e, et donc sur tout l'Im-noyau $\mathcal{N}$. Le semi-groupe $e\mathcal{N}e$ est donc un semi-groupe régulier fini: c'est donc un groupe; or il engendre le groupe caractéristique de $\mathcal{N}$ (à similitude près), il est donc lui-même ce groupe caractéristique.

PROPOSITION 3.1. *Soit β une fonction de* **N** *dans* **N**. *Soit H un semi-groupe linéaire engendré par un ensemble S de cardinal fini d d'endomorphismes de K^m.*

Pour tout mot f du semi-groupe libre S^+ de longueur au moins égale à $L_d(\beta, m)$, on peut trouver:

— *un entier s non nul,*

— *une phrase extraite de f de la forme:*

$$w = (g_1, g_2, \ldots, g_{\beta(s)}),$$
$$\mathrm{Card}\{g_i \mid 1 \leqslant i \leqslant \beta(s)\} \leqslant s$$

tels qu'en notant ϕ l'homomorphisme canonique de S^+ sur H,

(i) *les endomorphismes $\phi(g_i)$ engendrent un Im-noyau $\mathcal{N}$ de H,*

(ii) *le produit d'endomorphismes $\phi(f)$ ne change pas si l'on remplace chacun des $\phi(g_i)$ par son image dans le groupe caractéristique de $\mathcal{N}$.*

Preuve. Cette proposition reprend le théorème 3, le précisant un peu dans le cas des semi-groupes linéaires. Ces précisions sont obtenues en observant la façon dont on passe du théorème 1 au théorème 3.

On obtient la phrase w en posant, pour tout entier i de l'intervalle $[1, k]$ de **N**,

$$g_i = f_i u$$

dans une phrase extraite de f de la forme:

$$(u, f_1, u, f_2, u, \ldots, u, f_k, u)$$

obtenue par le théorème 1. On a de plus pour tout i:

$$\mathrm{Im}\ \phi(f_i u) = \mathrm{Im}\ \phi(u).$$

Or le groupe caractéristique $G(\mathcal{N})$ décrit exactement les endomorphismes induits par les $\phi(g_i)$ sur l'espace vectoriel $\mathrm{Im}\ \phi(u)$.

Il est clair que les mêmes observations permettraient de réécrire et de préciser, sous le même mode, le théorème 2 dans le cas des semi-groupes linéaires.

Nous énonçons à présent les principaux résultats que nous avons obtenus sur la finitude des semi-groupes, et sur la décidabilité de la finitude.

THÉORÈME 4. *Soit H un semi-groupe, admettant un système S de générateurs de cardinal fini d. Soit Im une image à droite sur H majorée par un entier m_0.*

Si β est une fonction de **N** *dans* **N** *telle que pour tout entier k, $\beta(k)$ soit un majorant de la largeur de tout Im-noyau de type au plus k, alors l'entier $L_d(\beta, m_0)$ majore la largeur de H.*

Preuve. Ce théorème est prouvé par le théorème 3. Nous verrons qu'il n'en épuise pas la portée.

Plus généralement, soit $\mathscr{R}$ une congruence sur H. Nous appellerons *$\mathscr{R}$-largeur* de H, ou d'un semi-groupe M de H, la largeur du semi-groupe quotient $H/\mathscr{R}$, ou de l'image de M dans ce quotient.

LEMME 3.3. *Un semi-groupe H, muni d'une image à droite bornée, est de largeur finie si et seulement si ses groupes caractéristiques sont de largeur bornée.*

Preuve. Théorème 4.

THÉORÈME 5. *Soit H un semi-groupe vérifiant les conditions du théorème* 4. *Soit $\mathscr{R}$ une congruence de semi-groupe sur H.*

Si pour tout entier k, l'entier $\beta(k)$ majore la $\mathscr{R}$-largeur de tout Im-noyau de H de type au plus k, alors l'entier $L_d(\beta, m_0)$ majore la $\mathscr{R}$-largeur de H.

Preuve. Théorème 3.

THÉORÈME 6. *Soit H un semi-groupe muni d'une image à droite bornée. Supposons H de type fini.*

Une congruence est finie sur H si et seulement si sa restriction à tout Im-noyau est finie.

COROLLAIRE 3.1. Soit H un semi-groupe muni d'une image à droite localement bornée. Une congruence est localement finie sur H si et seulement si sa restriction à tout Im-noyau est une congruence finie.

COROLLAIRE 3.2 (théorème de Burnside) (cf. [6]). Tout semi-groupe de matrices périodiques à coefficients dans un corps commutatif est localement fini.

Preuve. Tout groupe de matrices périodiques à coefficients dans un corps commutatif est fini, d'après le théorème de Burnside pour les groupes de matrices (Schur [8]).

On en déduit que tout groupe caractéristique d'un semi-groupe de matrices périodiques est fini. Tout Im-noyau de ce semi-groupe est donc fini, d'où l'on conclut par le théorème 6.

Ce dernier résultat a déjà été établi par McNaughton et Zalcstein par d'autres voies [6]. La démonstration proposée ici donne des raisons structurelles au résultat. On verra qu'elle permet, en outre, d'établir la décidabilité de la finitude.

PROPOSITION 3.2. *Soit H un semi-groupe admettant un ensemble fini de générateurs de cardinal d. Soit Im une image à droite sur H majorée par un entier m_0.*

Si β est une fonction de **N** *dans* **N** *telle que, pour tout entier k l'entier $\beta(k)$ soit*

un majorant de la largeur de tous les Im-noyaux finis de type au plus k, alors l'entier $L_d(\beta, m_0)$ *majore la largeur de H, à supposer qu'elle soit finie.*

Preuve. Théorème 3. Cette formulation légèrement différente de celle donnée par le théorème 5 nous permet d'aborder le problème de la décidabilité de la finitude.

THÉORÈME 7. *Soit H un semi-groupe vérifiant les conditions de la proposition* 3.2.

Si pour tout entier k on peut calculer un entier $\beta(k)$ *qui majore la largeur de tout Im-noyau fini de type au plus égal à k, alors on peut décider si H est fini.*

Preuve. Conséquence directe de la proposition 3.2. En effet, pour calculer l'entier $L_d(\beta, m_0)$, on n'utilise qu'un nombre fini de valeurs de la fonction β. On calculera donc les valeurs de β nécessaires au calcul successif des entiers

$$L_d(\beta, 1), L_d(\beta, 2), \ldots, L_d(\beta, m_0).$$

Ce calcul est fondé sur les parties techniques 1 et 2. Pour plus de précision sur cet "algorithme", voir [3].

On verra dans la quatrième partie de cet article, que les conditions du théorème 7 sont vérifiées pour les semi-groupes linéaires sur un corps commutatif.

THÉORÈME 8. *Soit H un semi-groupe vérifiant les conditions de la proposition* 3.2.

Supposons que l'on puisse, pour chaque Im-noyau $\mathcal{N}$ *de H, présenté par un système fini de générateurs, donner un algorithme, s'arrêtant toujours, qui détermine si* $\mathcal{N}$ *est fini et en calcule, dans ce cas, la largeur. Alors il existe un algorithme décidant si H est fini.*

Preuve. La fonction β utilisée dans le théorème 3 ne nous est dans le cas présent d'aucune utilité. Nous utiliserons plutôt le théorème 2. Nous chercherons donc à calculer une fonction α remplissant les conditions de ce théorème, si cela est possible.

L'algorithme que nous proposons travaille donc ainsi. Pour les valeurs successives de l'entier k, il détermine s'il existe un Im-noyau, engendré par des éléments de $S \cup S^2 \cup \cdots \cup S^k$, qui soit infini. Si la réponse est positive, H est infini. Si elle est négative, il calcule la plus grande largeur, $\alpha(k)$, obtenue pour ces Im-noyaux.

Il calcule ainsi jusqu'à pouvoir calculer l'entier $T_d(\alpha, 1)$. Il détermine alors les valeurs de $\alpha(k)$ nécessaires au calcul de $T_d(\alpha, 2)$ et cherche à les calculer si c'est possible, de la même façon.

S'il a pu calculer $T_d(\alpha, m_0)$, il lui reste à vérifier si la largeur de H est inférieure ou égale à $T_d(\alpha, m_0)$. Dans le cas positif, H est fini. Dans le cas négatif, H est infini.

PROPOSITION 3.3. *Soit H un semi-groupe linéaire sur un corps quelconque (skewfield) muni de son image à droite canonique.*

Tous les résultats de cette partie (théorèmes 4 à 8) restent inchangés si l'on y remplace "Im-noyau" par "groupe caractéristique".

Preuve. Proposition 3.1.

COROLLAIRE 3.3. Un semi-groupe linéaire sur un corps quelconque (skewfield) est localement fini si et seulement si tous ses groupes caractéristiques sont finis.

Ce résultat généralise un résultat de McNaughton et Zalcstein [6]. De même, nous pouvons prolonger certains résultats du même article et d'un article de Zalcstein [11] sur les semi-groupes linéaires localement testables.

Notation (semi-groupes localement testables). Soit k un entier non nul. Notons $\mathscr{L}_k$ la congruence sur H définie comme suit: si w et w' sont deux phrases sur H admettant même sous-phrase initiale (resp. terminale) de longueur $k-1$, et admettant même ensemble de sous-phrases de longueur k. Alors les mots w et w' sont congrus modulo $\mathscr{L}_k$. La congruence $\mathscr{L}_k$ est la plus petite congruence vérifiant ces relations.

DÉFINITION 3.4. Le *semi-groupe h* est dit *k-testable* si et seulement si la congruence $\mathscr{L}_k$ est l'égalité sur H.

H est dit *testable* si, pour un entier k, il est k-testable.

H est dit *localement testable* si tout sous-semi-groupe de type fini de H est testable.

On voit que nos terminologies diffèrent un peu de celles de Zalcstein [11] si H n'est pas de type fini.

LEMME 3.4. *Soit H un semi-groupe linéaire sur un corps quelconque. Si H est localement testable, ses groupes caractéristiques sont triviaux. Il est donc localement fini.*

Preuve. Si H est k-testable, on a pour tout élément de H, et donc aussi d'un groupe caractéristique:

$$g^{k+1} = g^k$$

ce qui établit que tout groupe caractéristique est réduit à son élément neutre. En raisonnant localement, ceci établit la première affirmation.

Les groupes caractéristiques étant finis, H est localement fini.

PROPOSITION 3.4. *Soit H un semi-groupe linéaire. On a les équivalences suivantes*:

(i) *H est localement testable*

(ii) *Tout Im-noyau de H contient un idempotent, et pour tout idempotent e de H le semi-groupe eHe est un semi-groupe commutatif formé d'idempotents.*

Preuve.

(i) $\Rightarrow$ (ii) Si tout groupe caractéristique est trivial, il s'en suit que tout Im-noyau est composé d'idempotent. Le reste de l'énoncé est alors établi par Zalcstein [11], puisque H est localement fini.

(ii) $\Rightarrow$ (i) établi par Mc Naughton [5].

COROLLAIRE 3.4. Soit H un semi-groupe linéaire de type fini sur un corps quelconque (skewfield). Il existe un algorithme décidant si H est localement testable.

Preuve. Si le corps de base était commutatif, nous pourrions dans un premier temps décider de la finitude de H, grâce à la technique développée en 4ème partie. L'énoncé (ii) de la proposition 3.4 permet alors de décider si H est localement testable.

Ce premier procédé est très coûteux en complexité de calcul. Nous disposons en effet d'un algorithme plus rapide, qui de plus reste valable sur un corps non commutatif.

Soit donc S un système de générateurs de H de cardinal fini d. Soit m_0 la dimension des endomorphismes de H. Nous pouvons calculer l'entier $L_d(1, m_0)$ défini au théorème 3, dans le cas où la fonction β de $\mathbf{N}$ dans $\mathbf{N}$ est la fonction constante égale à 1 sur tout $\mathbf{N}$. Nous disons que $L_d(1, m_0)$ majore la largeur de H, à supposer que H soit localement testable. En effet, si c'est le cas, les groupes caractéristiques de H sont triviaux, et donc de largeur égale à 1 (en admettant, dans la définition de la largeur d'un groupe, que l'on a posé $S^0 = \{1\}$, on voit qu'un groupe est de largeur 1 si et seulement si il est trivial). On vérifiera donc dans une première étape si la largeur de H est majorée par $L_d(1, m_0)$. Dans le cas négatif, H est peut-être fini, mais n'est certainement pas localement testable. Dans le cas positif, il nous reste à décider de la testabilité locale pour un semi-groupe fini, ce que l'on fait à nouveau par l'énoncé (ii) de la proposition 3.4.

4. LA FINITUDE DES SEMI-GROUPES LINÉAIRES EST DÉCIDABLE (SUR UN CORPS COMMUTATIF)

On trouvera des précisions sur les calculs de cette partie dans [3]; nous y développons l'algorithme dont nous prouvons ici l'existence, en présentant

synthétiquement sous forme d'organigramme la succession des calculs à effectuer pour emporter la décision.

Dans toute la suite, on supposera donné un corps K commutatif.

Au vu des résultats du théorème 7 et du lemme 3.1, il s'agira ici essentiellement d'établir la décidabilité du "critère de Burnside" simultanément pour tous les groupes caractéristiques de H. Nous le ferons en reprenant la preuve du théorème de Burnside pour les groupes de matrices, telle qu'elle est donnée dans Kaplansky [4], en montrant que cette preuve peut se faire de manière "constructive".

THÉORÈME 9. *On peut décider si un semi-groupe linéaire sur un corps commutatif est fini. Plus précisément, connaissant H, on peut calculer un entier qui en majore la largeur. (H est supposé donné par un ensemble fini de générateurs).*

Preuve. Pour établir ce théorème, utilisant le théorème 7 et le lemme 3.1, il nous suffira de prouver le résultat suivant:

THÉORÈME 10. *Soit H un semi-groupe de type fini de matrices à coefficients dans K. Pour tout entier k strictement positif, il existe un entier $\beta(k)$ qui majore la largeur de tout groupe caractéristique de H de type au plus k.*

L'entier $\beta(k)$ dépend de la dimension m des matrices de H, du cardinal d d'un ensemble fini S de générateurs de H, et de l'ensemble $\mathscr{S}$ des coefficients des matrices de S.

Preuve du théorème 10. Nous décrivons les étapes de la preuve du théorème 10 sous forme de trois lemmes.

LEMME 4.1. *Les racines de l'unité qui sont racines caractéristiques d'une matrice de H sont d'ordre majoré par un entier calculable $N = N(m, \mathscr{S})$ ne dépendant que de la dimension m et de l'ensemble $\mathscr{S}$ des coefficients des matrices de S.*

Preuve. Les coefficients des matrices de S engendrent, sur le sous-corps premier Π de K une extension $\Pi(\mathscr{S})$ qui est, puisque de type fini, extension algébrique, dont nous noterons τ le degré, d'une extension Π' purement transcendante de Π. On en déduit aisément que $\Pi(\mathscr{S})$ est isomorphe à un corps de matrices carrées de dimension τ sur Π', et par suite il est clair que H est isomorphe à un semi-groupe H' de matrices de dimension $\tau \times m$ sur Π'.

En *caractéristique* $p \neq 0$, on en déduit, puisque tout polynôme à coefficients dans et irréductible sur Π reste irréductible sur Π', que toute racine de l'unité qui soit racine caractéristique d'une matrice de H est d'ordre majoré par:

$$N = N(m, \mathscr{S}) = p^{\tau \times m} - 1$$

En *caractéristique nulle*, soit, pour tout entier i, $\lambda(i)$ un entier tel que tout polynôme cyclotomique d'une racine de l'unité d'ordre supérieur à $\lambda(i)$ soit

un polynôme de degré supérieur à i (Pour le calcul d'une telle fonction λ, qui réalise en quelque sorte une inversion de la caractéristique d'Euler, voir [3]). Il suffira de poser:

$$N = N(m, \mathscr{S}) = \lambda(\tau \times m)$$

LEMME 4.2. *Soit Λ un ensemble fini de racines de l'unité, et soit G un groupe de matrices de dimension m sur K, dont toutes les racines caractéristiques appartiennent à Λ. Si G est irréductible sur la clôture algébrique de K, alors il est fini, et de cardinal majoré par*:

$$(\text{Card } \Lambda)^{m^3}.$$

Preuve. La condition supposée implique que la fonction trace prend sur G au plus $(\text{Card } \Lambda)^m$ valeurs. Le résultat s'en déduit aussitôt.

LEMME 4.3. *Soit G un groupe admettant, en tant que groupe, un système fini de q générateurs. Soit G/R un quotient fini de G, de cardinal r. Il existe un système fini D de cardinal $(2q + r)$ d'éléments de G, et un sous-monoïde T de R engendré par $(2q + r)$ éléments, vérifiant*:

$$G = T \cdot D.$$

Preuve. On prend pour former D les q générateurs de G ainsi que leurs inverses, et l'on complète ce système pour que soient représentées toutes les classes de G modulo R. Si alors a_i et a_j sont dans D, il existe un $a_{j'}$ dans D et un t_{ij} dans R, vérifiant:

$$a_i a_j = t_{ij} a_{j'} .$$

Les t_{ij} engendrent alors dans R le sous-monoïde cherché.

LEMME 4.4. *Soit Λ un ensemble fini de racines de l'unité. Pour tout couple (m, s) d'entiers strictements positifs, il existe un entier $\beta_m(s)$ qui majore le cardinal de tout groupe fini G de matrices de dimension m sur K engendré par s matrices dont toutes les racines caractéristiques appartiennent à Λ.*

Preuve. Nous raisonnons par récurrence sur m.

(a) Supposons $m = 1$.

Si G n'est pas réduit à 0, il est clair que G est un sous-groupe de Λ. On peut donc poser:

$$\forall s \in \mathbf{N}, \qquad \beta_1(s) = \text{Card } \Lambda.$$

(b) Supposons $\beta_{m'}(s)$ connu en dimension m' strictement inférieure à m, calculons $\beta_m(s)$.

Si G est irréductible sur la clôture algébrique de K, il est fini, de cardinal majoré par:

$$(\text{Card } \Lambda)^{m^3}.$$

Si G n'est pas irréductible, on peut, par similitude, réduire simultanément toutes les matrices de G sous la forme:

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

où toutes les matrices A engendrent un groupe irréductible de matrices de cardinal au plus égal à:

$$(\text{Card } \Lambda)^{(m-1)^3}$$

et où les matrices C engendrent, par hypothèse de récurrence, un groupe fini de cardinal majoré par $\beta_{m-1}(s)$. Le groupe G admet pour quotient le groupe G/R des matrices de la forme:

$$\begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}.$$

Ce groupe G/R est de cardinal majoré par:

$$\beta_{m-1}(s) \times (\text{Card } \Lambda)^{(m-1)^3}.$$

Le noyau R de ce quotient est, à similitude près, formé des matrices de G de la forme:

$$\begin{pmatrix} I_1 & 0 \\ 0 & I_2 \end{pmatrix}$$

où I_1 et I_2 sont les matrices identité de dimension convenable.

En *caractéristique nulle*, on voit qu'un tel groupe est nécessairement trivial. On posera donc:

$$\beta_m(s) = \sup((\text{Card } \Lambda)^{m^3}, \beta_{m-1}(s) \times (\text{Card } \Lambda)^{(m-1)^3})$$

et plus explicitement, comme on le vérifie aisément:

$$\beta_1(s) = \text{Card } \Lambda,$$

$$\beta_2(s) = (\text{Card } \Lambda)^8,$$

si $m \geqslant 3$:

$$\beta_m(s) = (\text{Card } \Lambda)^{m^3}$$

On notera qu'en caractéristique 0, les entiers $\beta_m(s)$ ne dépendent pas de la valeur de l'entier s.

En *caractéristique p non nulle*, après avoir noté que R est un groupe commutatif, on constate que, si G est fini, les matrices de R ont nécessairement pour ordre un diviseur de p. On en déduit que le sous-monoïde T de R décrit au lemme 4.3 est de cardinal majoré par l'entier:

$$p^{(2s+r)^2}$$

On peut donc construire les entiers $\beta_m(s)$ par récurrence, par les formules suivantes:

$$r_m = \beta_{m-1}(s) \cdot (\text{Card } \Lambda)^{(m-1)^3},$$

$$\beta_m(s) = \sup((\text{Card } \Lambda)^{m^3}, p^{(2s+r_m)^2} \cdot (2s + r_m)),$$

$$\beta_1(s) = \text{Card } \Lambda.$$

Preuve du théorème 10 (*fin*). Soit Λ l'ensemble des racines de l'unité qui sont racines caractéristiques des matrices de H. D'après le lemme 4.1, on a:

$$\text{Card } \Lambda \leqslant \frac{N(N-1)}{2}$$

avec, en *caractéristique p non nulle*:

$$N = p^{\tau \times m} - 1$$

et en *caractéristique* 0:

$$N = \lambda(\tau \times m).$$

Le lemme 4.4 nous permet de construire une fonction β de $\mathbf{N}$ dans $\mathbf{N}$ en posant pour tout entier positif s:

$$\beta(s) = \beta_m(s)$$

Cette fonction β est la fonction cherchée. Il est clair en effet que tout entier qui majore le cardinal d'un groupe fini, en majore aussi la largeur.

5. Relativisations de la notion de finitude

Nous présentons à présent quelques possibilités d'extension des résultats précédents, naturellement suggérées par la nature des techniques combinatoires mises en œuvre, et qui ne semblent pas dénuées d'intérêt.

Soit donc H un semi-groupe muni d'une fonction image à droite Im, à valeur dans un ensemble ordonné à degré (Δ, δ).

Définition 5.1. Un sous-ensemble F de H est dit *Δ-fini* si son image dans Δ est un ensemble fini. Une propriété est dite *vraie Δ-localement* si elle est vraie pour tout sous-semi-groupe de H engendré par un système de générateurs Δ-fini.

Les deux théorèmes qui suivent sont des généralisations immédiates des théorèmes 6 et 8.

Théorème 11. *Soit H un semi-groupe muni d'une image à droite Δ-localement bornée. Une congruence est Δ-localement Δ-finie sur H si et seulement si elle est Δ-finie sur tous les Im-noyaux de H.*

Théorème 12. *La Δ-finitude d'une congruence sur H est décidable si et seulement si elle est décidable sur tous ses Im-noyaux.*

D'autres relativisations de la notion de finitude sont possible, menant à des théorèmes généralisant les résultats ici présentés. C'est le cas, par exemple, avec les définitions suivantes:

Définition 5.2. Soit k un entier. Un semi-groupe à image à droite H sera dit de *(k, Δ)-type fini* si et seulement H^k admet un système de générateurs Δ-fini.

Une propriété sera dite vraie *(k, Δ)-localement* si et seulement si elle est vraie pour tous les sous-semi-groupes de H qui sont de (k, Δ)-type fini.

Nous laissons au lecteur le soin d'énoncer les résultats obtenus dans le cadre de ces définitions.

Conclusion

On peut constater que les résultats que nous avons obtenus, concernant les factorisations de produits dans un semi-groupe à image à droite, peuvent apporter des informations qui dépassent nettement le cadre de l'étude des questions de finitude. En effet, on peut dire — en parlant informellement — que les Im-noyaux sont les objets dans lesquels on pourra caractériser toutes les propriétés "persistantes" du semi-groupe étudié. Cela laisse en particulier indiquer la possibilité d'applications à l'étude des chaines de Markov.

BIBLIOGRAPHIE

1. J. A. BRZOZOWSKI AND I. SIMON, Characterizations of locally testable events, *Discrete Math.* **4** (1973), 243–271.
2. G. JACOB, Un théorème de factorisation des produits d'endomorphismes de K^N, *J. Algebra*, à paraître.
3. G. JACOB, On peut décider si un semi-groupe de matrices est fini, *Theoretical Computer Sci.* **5** (1977), 183–204.
4. I. KAPLANSKY, "Fields and Rings," Chicago Lecture Notes in Mathematics, Univ. of Chicago Press, Chicago, 1969.
5. R. MCNAUGHTON, Algebraic decision procedures for local testability, *Math. Systems Theory* **8** (1974), 60–76.
6. R. MCNAUGHTON AND Y. ZALCSTEIN, The Burnside theorem for semi-groups, *J. Algebra* **34** (1975), 292–299.
7. C. PROCESI, The Burnside problem, *J. Algebra* **4** (1966), 421–425.
8. I. SCHUR, Über Gruppen periodischer Substitutionen, *Sitzungsber. Preuss. Akad. Wiss.* (1911), 619–627.
9. M. P. SCHUTZENBERGER, On finite monoids having only trivial subgroups, *Inform. Contr.* **8** (1965), 190–194.
10. D. SUPRUNENKO, "Soluble and Nilpotent Linear Groups," 1958; Translations of Mathematical Monographs, *Amer. Math. Soc.*, Providence, R. I., 1963.
11. Y. ZALCSTEIN, Locally testable semigroups, *Semigroup Forum* **5** (1973), 216–227.
12. Y. ZALCSTEIN, Finiteness conditions for matrix semigroups, *Proc. Amer. Math. Soc.* **38** (1973), 247–249.
13. Y. ZALCSTEIN, Syntactic semigroups of some classes of star-free languages, *in* "Automata, Languages and Programming" (M. Nivat, Ed.), North–Holland, Amsterdam, 1973.