CAHIERS MATHÉMATIQUES

MONTPELLIER

3

COMPTES RENDUS

DES JOURNÉES MATHÉMATIQUES S. M. F.

UNIVERSITÉ DES SCIENCES
ET TECHNIQUES
DU LANGUEDOC
U. E. R. DE MATHÉMATIQUES
Place Eugène Bataillon
34060 MONTPELLIER CEDEX

1974

JOURNEES MATHEMATIQUES S.M.F.

MONTPELLIER 16-20 Avril 1974

INTRODUCTION

L'idée initiale pour ces Journées était de sortir des sentiers battus, comme en porte témoignage, le choix des thèmes. On a voulu exposer un certain nombre de sujets d'actualité en mathématiques ainsi que de leurs applications [on serait tenté de parler de mathématiques pures et appliquées, mais nous nous garderons bien de le faire]. Voici le programme de ces Journées :

P R O G R A M M E

* Les conférences ont lieu en Salle 102 A (1er étage du Bâtiment de Mathématiques) de 9h. à 12h. et de 14h. à 18h. Début des conférences : Mardi à 14h.

Mardi 16 Avril

MODELES

C.F. PICARD - Un aspect paradoxal de l'information

R. THOM - L'optimisation simultanée et la théorie des jeux en topologie différentielle.

K. MOUNT - Information size of Message Spaces and the regularity of the Pareto Correspondence

M. FLIESS - Une approche nouvelle de certains systèmes dynamiques utilisés en ingéniérie.

Mercredi 17 Avril

ASPECTS ALGEBRIQUES DE LA COMBINATOIRE

D. FOATA - Réarrangements d'applications associées aux nombres de Genocchi.

G. VIENNOT - Factorisations des monoïdes libres et bases des algèbres de Lie libres.

J.P. SOUBLIN - Problèmes de Burnside.

AUTOMATES ET LANGAGES

E. SPANIER - Mathematical Properties of languages.

J. PERROT - Monoïdes syntactiques des langages rationnels.

D. PERRIN - Sur les groupes de permutations associés aux codes biprefixes.

S. TERMINI - A. RESTIVO - An algorithm for deciding whether a strictly localy testable submonoïd is free.

Jeudi 18 Avril

COMPUTATIONAL PROBLEMS IN ALGEBRA

L. GERHARDS - On the construction of the automorphism group of a finite group.

D. LAZARD - Algèbre linéaire sur les anneaux de polynômes.

A. MICALI - Nombres et séries de Betti

11h. 30 Départ pour Saint-Guilhem-Le-Désert.

Vendredi 19 Avril

ASPECTS ALGEBRIQUES DE LA COMBINATOIRE

P. HILTON - Localization of nilpotent groups ; homological and and combinatorial methods.

M. BROUE - Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et Formes Formes quadratiques entières définies positives à discriminant +1.

S. FAKIR - Monoïdes et anneaux algébriquement clos.

CALCUL ET PROGRAMMATION

L. NOLIN - Programmation et logique combinatoire.

M. NIVAT - Pour une sémantique algébrique

J. VUILLEMIN - Deux problèmes liés à l'analyse d'algorithmes.

G. WERNER - Sous-classes récursivement énumérables d'une classe de complexité.

Samedi 20 Avril

AUTOMATES ET LANGAGES

A. LENTIN - Equations dans les monoïdes libres (quelques problèmes actuels).

M. MORCRETTE - Catégories de systèmes algébriques suscitées par la théorie des équations dans le monoïde libre.

M. FONTET - π-systèmes involutifs.

AUTOMATES ET LANGAGES

M.P. SCHUTZENBERGER - Sur certaines pseudo-variétés de monoïdes finis.

G. JACOB - Séries formelles en variables non commutatives. Transductions rationnelles.

Réunion de clôture.

———— : ————

Ce fascicule contient les textes de presque toutes les conférences tenues lors de ces Journées. Nous regrettons que les textes de certaines conférences qui avaient intéressé beaucoup les participants ne nous soient pas parvenus. Nous pensons tout particulièrement aux conférences faites dans le cadre du thème CALCUL et PROGRAMMATION.

D'autre part, les papiers de N. ROBY et D. ALLOUCH n'ont pas été exposés, faute de temps.

Malgré la difficulté de classer tous ces articles sous les cinq thèmes des Journées, ce fascicule a la composition suivante :

MODELES

J.L. CHABERT : Systèmes dynamiques linéaires et extensions de Fatou.

M. FLIESS : Une approche nouvelle de certains systèmes dynamiques utilisés en ingéniérie.

K. MOUNT : Information size of Message Spaces and the regularity of the Pareto Correspondence.

C.F. PICARD : Un aspect paradoxal de l'information.

R. THOM : L'optimisation simultanée et la théorie des jeux en topologie différentielle.

ASPECTS ALGEBRIQUES DE LA COMBINATOIRE

M. BROUE : Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et Formes quadratiques entières définies positives à discriminant +1.

S. FAKIR : Monoïdes et nneaux algébriquement clos.

D. FOATA : Réarrangements d'applications associées aux nombres de Genocchi.

P. HILTON : Localization of Nilpotent Groups ; homological and combinatorial methods.

N. ROBY : Méthodes probabilistes et problèmes de densité en théorie des nombres.

J.P. SOUBLIN : Problèmes de Burnside.

G. VIENNOT : Factorisations des monoïdes libres et bases des algèbres de Lie libres.

AUTOMATES ET LANGAGES

D. ALLOUCH : R-ensemble maximal de fractions.

G. JACOB : Séries formelles en variables non commutatives. Transductions rationnelles.

A. LENTIN : Equations dans les monoïdes libres.

M. FONTET : π-systèmes involutifs.

M. MORCRETTE : Catégories de systèmes algébriques suscitées par la théorie des équations dans le monoïde libre.

D. PERRIN : Sur les groupes de permutations associés aux codes biprefixes.

J.F. PERROT : Monoïdes syntactiques des langages rationnels.

A. RESTIVO et S. TERMINI : An algorithm for deciding whether a strictly localy testable submonoïd is free.

COMPUTATIONAL PROBLEMS IN ALGEBRA

CALCUL et PROGRAMMATION

Nous sommes tenus à donner quelques explications complémentaires au lecteur. Les textes de A. LENTIN, M. FONTET et M. MORCRETTE sont disposés dans l'ordre où ils doivent être lus.

Par ailleurs, notre conditionnement scientifique est tel qu'il nous est impossible d'échapper au franglais ou directement, à l'anglais en tant que langue scientifique. Il nous a semblé qu'il n'y avait pas de titre français pouvant rendre compte de la situation en aussi peu de mots, raison pour laquelle nous avons conservé directement le titre anglais : COMPUTATIONAL PROBLEMS IN ALGEBRA.

Finalement, nous tenons à rendre publique la liste des organismes qui nous ont aidé financièrement dans la réalisation de ces Journées :

SOCIETE MATHEMATIQUE DE FRANCE-CNRS

UER de Mathématiques Appliquées aux Sciences Humaines, Université Paul Valéry (Université de Montpellier III)

Conseil Scientifique de l'USTL (Université de Montpellier II).

MIAGE (Maîtrise Informatique Appliquée à la Gestion des Entreprises) de l'USTL.

IUT (Institut Universitaire de Technologie) de Montpellier.

UER de Mathématiques de l'USTL.

Ce fascicule n'a pu voir le jour que grâce aux moyens matériels de notre UER de Mathématiques et aux actions heroïques de Madame C. MORI qui a assuré la frappe et de Monsieur Meyran, pour la pagination. Qu'il leur soit rendu grâce ainsi qu'à tous ceux qui nous ont aidé et dont les noms nous échappent en ce moment.

———— : ————

Nous implorons finalement la clémence des Dieux pour avoir dépensé tant de papier et par conséquent, avoir contribué à abattre tant d'arbres....

Montpellier le 23 Janvier 1975

Yves CESARI

Artibano MICALI

SUR CERTAINES PSEUDO-VARIETES DE MONOIDES FINIS

par

M.P. SCHUTZENBERGER

I. Selon la théorie de S. Eilenberg, une pseudo-vairété de semi-groupes (ou monoïdes, ou groupes) est une famille de telles structures contenant toute image homomorphe du produit sous direct de deux de ses membres. En particulier, étant donnée une pseudo-variété de groupes $\mathcal{V}$ on peut définir la pseudo-variété $\bar{\mathcal{V}}$ de monoïdes finis par la condition que $M \in \bar{\mathcal{V}}$ ssi chaque groupe dans M appartient à $\mathcal{V}$ et pour chaque alphabet Σ la famille $\bar{\mathcal{V}}$-Rec des parties P de monoïde libre Σ^* telles que leur monoïde syntactique appartienne à $\bar{\mathcal{V}}$.

On sait d'autre part que la pseudo-variété (de groupes) $\mathcal{V}$ associe à chaque groupe G un plus petit sous-groupe normal V_G (= le $\mathcal{V}$-noyau de G) tel que $G/V_G \in \mathcal{V}$. L'hypothèse que $\mathcal{V}$ est une pseudo-variété, équivaut à la condition que pour tout morphisme $\phi : G \to H$, on ait $V_{G\phi} \subset V_H$ si ϕ est injectif et $V_H \subset V_{G\phi}$ si ϕ est surjectif.

Le résultat principal de ce travail est la

Propriété I.1.

Soit $A \in \bar{\mathcal{V}}$-Rec. On a $A^* \in \bar{\mathcal{V}}$-Rec ssi l'image $B = A^*\rho_{A^*}$ de A^* dans son monoïde syntactique $S = \Sigma^*\rho_{A^*}$ satisfait la condition :

($\mathcal{V}$). B contient le $\mathcal{V}$-noyau de chacun des groupes qu'elle rencontre.

Il est trivial que cette condition est nécessaire : en effet, comme B est un sous semi groupe du monoïde fini : son intersection avec chaque groupe G dans S contient l'idempotent e de ce dernier qui est lui-même précisément le $\mathcal{V}$-noyau de G ssi $G \in \mathcal{V}$.

Nous ne nous occuperons donc plus désormais que de l'implication inverse. Dans la section III nous utilisons la propriété précédente pour retrouver divers résultats connus.

Nous terminons cette introduction en rappelant quelques propriétés du monoïde syntactique, elles aussi connues depuis les travaux de R. Croisot (Equivalences Principales Bilatères définies dans un demi-groupe. J. de Math. Pures et Appl. 36 (1957). pp. 373-417).

Proposition I.2

Soit $M' = M\rho_E$ le monoïde syntactique de la partie E de M. Le morphisme syntactique ρ_E, de la partie $E' = E\rho_E$ de M' est l'identité.

Preuve : Par définition M' est le plus petit quotient de M pour lequel le morphisme correspondant ϕ de M satisfasse $E = E\phi\phi^{-1}$. L'énoncé en découle en vérifiant que cette dernière relation est satisfaite par $\phi = \rho_E\rho_{E'}$.

Q.E.D.

Pour chaque $m_1 \in M$ nous posons

$E:: m_1 = \{(m,m') \in MxM : mm_1m' \in E\}$.

Proposition I.3

Pour tout $m_1, m_2 \in M$ on a $m_1\rho_E = m_2\rho_E$ ssi $E : m_1 = E : : m_2$.

Preuve : Il est clair que la relation $E :: m_1 = E : : m_2$ définit une équivalence $\equiv$ sur M. Comme $E ::(m_1m_3) = \{(m,m') \in E ::m_1 : m' \in m_3M\} = (E ::m_1) \cap (M,m_3M)$ pour tout $m_1, m_3 \in M$ puisque M contient un élément neutre 1, et comme une relation semblable vaut pour m_3m_1, on voit que de fait, $\equiv$ est une congruence. Puisque $(1,1)$ appartient à $E::m_1$ ssi $m_1 \in E$,

elle sature E et elle contient toutes les congruences ayant cette propriété puisque $m_1 \neq m_2$ implique l'existence d'une paire $(m_1 m')$ pour laquelle un seul des éléments mm_1m' et mm_2m' appartient à E.

Q.E.D.

Nous appliquons ceci au groupe G dans $S = \Sigma^*\rho$ en désignant désormais par ρ le morphisme syntactique ρ_{A^*}. Comme ci-dessus, e et V sont l'idempotent et le $\mathcal{V}$-noyau de G.

Lemme I.4. Soit $b \in e\,\rho^{-1}$. Supposons que pour tout $f, f' \in \Sigma^*$ tels que $fbb^*f' \subset A^*$ et chaque $v \in V$ il existe un $c \in v\,\rho^{-1}$ pour lequel on ait

(X) $\qquad fb^*cb^*f' \cap A^* \neq \emptyset$

Alors $\qquad V = \{e\}$.

Preuve Comme $b\rho = e = e^2$ on a $bb^*\,\rho = e$, et par conséquent $fbb^*f' \subset A^*$ implique $(f\rho)e(f'\rho) \in A^*\rho$. De même, comme $v = ev = ve = eve$ puisque $v \in V \subset G$, la relation (X) implique $(f\rho)v(f'\rho) \in A^*$.

Maintenant d'après I.2 et I.3 ci-dessus avec $M = S$ et $E = A^*$ on a $e = v$ ssi $A^*\rho::e = A^*\rho::v$.

L'hypothèse du lemme équivaut à l'assertion que chaque $(s,s') \in A^*\rho::e$ appartient à tous les $A^*\rho::v$ $(v \in V)$. En effet la première relation implique $(s\rho^{-1})(e\rho^{-1})(s'\rho^{-1}) \subset A^*\rho\rho^{-1} = A^*$ donc $fbb^*f' \subset A^*$ pour tout $f \in s\rho^{-1}$, $f' \in s\,\rho^{-1}$ et la relation (X). Ceci suffit pour entrainer l'égalité de $A^*\rho::e$ et de chacun des $A^*\rho::v$ car si (s,s') est dans ce dernier ensemble on a $(s,s'') \in A^*\rho::e$ pour $s'' = vs'$ donc $(s,s'') \in A^*\rho::v^{-1}$, ce qui équivaut à $(s,s') \in A^*\rho::e$ puisque $sv^{-1}s'' = sv^{-1}v's' = ses'$.

Q.E.D.

II. Vérification de la proposition I.1.

Nous gardons les mêmes notations que dans le lemme I.4. Dans le premier énoncé ci-dessous, nous choisissons un mot $b \in ep^{-1}$. Dans les suivants nous véridions que (X) est vraie dans tous les cas. Dans les deux derniers, seul intervient le fait que Σ^* est un monoïde libre et plus exactement que chaque mot $s \in \Sigma^*$ a une longueur $|s| \in N$, (avec $|s| > 0$ ssi $s \neq 1$). Dans les trois premiers on exploite l'hypothèse $T \in \bar{\mathcal{V}}$ où pour abréger $\tau : \Sigma^* \to T$ désigne le morphisme syntactique de A.

II.1. Sous l'hypothèse $T \in \bar{\mathcal{V}}$, il existe un sous-ensemble fini C de Σ^* tel que $C\rho = G$ et $C\tau = u$ où u est un idempotent de T.

Preuve : Comme $G\rho^{-1}$ est un semi groupe et T un ensemble fini, l'ensemble $G\rho^{-1}\tau$ est un semi groupe fini. D'après un théorème classique de Clifford (Am. J. of Math. 70 (1948) pp. 521-526) il contient un groupe H tel que $H = H(G\rho^{-1}\tau)H$. Cette relation entraine que $P\rho = G$ et $P_\tau = H$ où P désigne l'intersection de $G\rho^{-1}$ et $H\tau^{-1}$. Suit e l'idempotent de G. Posons $g\lambda = (g\rho^{-1} \cap P)\tau$ pour chaque $g \in G$. On a identiquement

(2.1.) $(g_1\lambda)(g_2\lambda) \subset (g_1g_2)\lambda$

puisqu'une relation semblable vaut pour ρ^{-1}. Prenant en particulier $g_1 = g_2 = e$, on en déduit en utilisant la finitude de H que $e\lambda$ est un sous groupe K de H. Prenant successivement $g_1 = e$ et $g_1 = g_2^{-1}$, la même relation (2.1.) montre que K est un sous groupe normal et que λ induit un morphisme de G sur H/K. De façon symétrique, on trouve que le noyeau L de λ est l'ensemble $C'\rho$ où $C' = P \cap u\,\tau^{-1}$ $(u = u^2 \in H)$. Faisons intervenir l'hypothèse $T \in \bar{\mathcal{V}}$. Comme $\mathcal{V}$ est une pseudo variété de groupes elle entraine que H et H/K appartiennent à $\mathcal{V}$ et nous

en concluons que L contient le $\mathcal{V}$-noyau V de G en raison de l'isomorphie de G/L et H/K et du caractère minimal de V. L'énoncé en résulte en prenant pour G une partie convenable de $C' \cap V\rho^{-1}$.

Q.E.D.

Corollaire II.2.

Soient b, c $\in$ C. On a xbcx'$\in$ A pour tout x, x'$\in \Sigma^*$ tels que xbx'$\in$ A.

Preuve : Ceci résulte immédiatement de $C\tau = u = u^2$ et de la définition de τ comme morphisme syntactique de A.

Q.E.D.

Dorénavant b sera un mot fixe de $C \cap e\rho^{-1}$ et f, f' une paire de mots telle que $fbb^*f' \subset A^*$.

II.3. Supposons $fb^nf' \in (A \setminus 1)^k$ pour une paire d'entiers n,k telle que $n \geq k+1$. Pour chaque c $\in$ C on a la relation

(X) $fb^*cb^*f' \cap A \neq \phi$

Preuve : Soit $fb^nf' = a_1a_2\ldots a_k$ où chaque $a_i \in A$.

On associe à chaque $m \leq n$ le plus grand entier $i = i_m$ pour lequel $a_1\ldots a_i$ est un facteur gauche de fb^m. Comme $n \geq k+1$ il existe un m pour lequel $i_m = i_{m+1}$. Ceci permet de trouver des mots a',a"$\in A^*$; a $\in$ A, x, x' $\in \Sigma^*$ satisfaisant les relations $fb^m = a'x$; $xbx' = a$; $b^{m'}f = x'a"$. Celles ci entrainent que pour tout mot d le mot $w = fb^mdb^{m'}f'$ soit égal à a'd'a" où d' = xbdx'. D'après le corollaire II.2. et xbx'$\in$ A, on a donc w $\in A^*$ quand d = c $\in$ C.

Q.E.D.

Nous n'utiliserons plus désormais l'hypothèse $T \in \bar{\mathfrak{V}}$ mais nous supposerons toujours que la condition $(\mathfrak{V})$ est satisfaite.

II.4. Soient $t,t' \in S$ tels que $tt' = e$ et $t'et \in A^*\rho$. La condition $(\mathfrak{V})$ entraîne que V soit contenu dans $t(A^*\rho)t'$.

Preuve : Soit $g\theta = t'gt$ pour chaque $g \in G$. On a $t(g\theta)t' = tt'gt't' = ege = g$ et $(g\theta)(g'\theta) = tgt'tg't' = tgeg't = tgg't' = (gg')\theta$ pour tout $g' \in G$. Par conséquent θ est un morphisme sur un groupe G' et $V = tV_{G'}t'$. Maintenant nous avons $e\theta = t'et \in A^*\rho$ par hypothèse, donc $V_{G'} \subset A^*\rho$ d'après $(\mathfrak{V})$.

Q.E.D.

II.5 Supposons que l'hypothèse de II.3 ne soit pas satisfaite par b,f,f'. Pour chaque $v \in V$, on peut trouver un $c \in v\rho^{-1}$ pour lequel (X) est vérifiée.

Preuve : Soit $w = fb^n f'$ où $n = |f| + |f'| + 2|b|^2$. Par l'hypothèse, w est un produit $a_1a_2\ldots a_k$ de mots de $A\setminus 1$ où $k \geq n$. Soit d le plus petit indice pour lequel $p_0 = a_1\ldots a_d$ ait f comme facteur gauche et soit d' le plus grand indice pour lequel $p_{|b|+1} = a_{d'+1}\ldots a_k$ ait f' comme facteur droit. Comme tous les a_i ont une longueur positive, le on a $d \leq |f|$ et $k-d' \leq |f'|$ et par conséquent $w = p_0 p p_{|b|+1}$ ou p est le produit d'au moins $2|b|^2$ mots de $A\setminus 1$. On peut donc écrire $p = \bar{p}_1\bar{p}_2\ldots\bar{p}_{|b|}$ où chaque $p_i \in A^*$ à une longueur au moins égale à $2|b|$. Ceci définit pour chaque $j = 0,1,\ldots,|b|$ un facteur gauche $b_j \neq b$ de b tel que $\bar{p}_0\bar{p}_1\ldots\bar{p}_j \in fb^*b_j$.

Comme b a évidemment $|b|$ facteurs gauches propres, on a $b_{j'} = b_j$ pour au moins une paire $0 \leq j' < j \leq |b|$. Définissant b' par

$b = b_j$, $b' = b_j b'$.

$\bar{a}_1 = \bar{p}_0 \cdots \bar{p}_{j'} = f b^m b_{j'}$

$\bar{a}_2 = \bar{p}_{j'+1} \cdots \bar{p}_j = b' b^q b_j$

$\bar{a}_3 = \bar{p}_{j+1} \cdots \bar{p}_{|b|+1} = b' b^{m'} f'$.

où $q \geq 1$ en raison de $|\bar{p}_{j'+1}| \geq 2|b|$.

Les hypothèses de II.4 sont satisfaites par $t = b_j \rho = b_{j'} \rho$ et $t' = b' \rho$ et nous pouvons donc trouver pour chaque $v \in V$ un mot $a \in A^*$ tel que $c = b_j a b' \in v\rho^{-1}$. Considérons maintenant le mot $w' = \bar{a}_1 \bar{a}_1 a \bar{a}_3 \in A^*$. Il est égal au mot $f b^{m+1} b j a b' b^{m'} f'$ qui appartient à $fb^* c b^* f'$.

Q.E.D.

Ceci achève de montrer que les hypothèses du lemme I.4. sont satisfaites dans tous les cas et conclut la preuve de la proposition I.1.

III. Exemples.

Dans ce qui suit, nous utiliserons le théorème suivant qui ne rassemble que des faits connus.

Théorème III.1. Soit s un élément d'un monoïde S ayant au plus $m < \infty$ éléments et soit $p \geq 1$ le plus petit commun multiple des entiers $\leq m$.

(i) Soit $q \geq 0$ le plus petit entier tel que $s^q \in Ss^{q+1}S$. L'ensemble $s^q s^*$ est un groupe cyclique C_s dont l'ordre $\pi(s)$ divise p.

(ii) Pour chaque multiple $p' \geq q$ de $\pi(s)$, $s^{p'}$ est l'idempotent de C_s;

(iii) $s^{p-1} \in C_s$.

Nous examinons maintenant le cas particulier d'une pseudo-variété de groupes $\mathcal{V}(H)$ définie par un ensemble non vide Π d'entiers positifs

et la condition que l'ordre $\pi(g)$ de tout élément g d'un groupe de $\mathcal{V}$ soit dans Π. Comme $\mathcal{V}$ contient tous les sous groupes de ses membres, Π doit contenir les diviseurs de ses éléments et comme $\mathcal{V}$ est fermée par produit direct, Π doit l'être par rapport au p.p.c.m. Réciproquement, il est clair que tout Π satisfaisant ces deux conditions définit une pseudo-variété. Le cas où Π est formé de toutes les puissances d'un nombre premier donné a été étudié par Bret Tilson ("On the p-Length of p-solvable semi groups" in "Semi groups", K.W. Folley Ed. 1969). Le cas où Π se réduit à $\{1\}$ donne la pseudo-variété des monoïdes finis dont tous les groupes sont triviaux qui sert dans la théorie des "Counter Free Automata" de R.Mc Naughton et S. Pappert (MII Press 1971).
Nous considérons maintenant une pseudo-variété $\mathcal{V} = \mathcal{V}(\Pi)$ fixe.

Exemple III.2. Soit $A \in \mathcal{V}(\Pi)$-Rec ; A^* appartient à la même famille ssi pour chaque mot $h \in \Sigma^*$ et tout $n \in N$ assez grand on a l'implication : $h^n \in A^* \Rightarrow h^{n+m} \in A^*$ où
$m = n \wedge \Pi$ désigne le plus grand diviseur de n qui appartienne à Π.

Preuve : Supposons $h^n \in A^*$ pour un $n \geq 1$. D'après le Théorème III.1, il existe un entier $q \in N$ tel $(h^q h^*)\rho$ soit un groupe cyclique C et comme A^* est un monoïde, $(h^q h^* \cap A^*)\rho$ est un sous groupe C' de C. Posant $r = \mathrm{Card}(C)$, $r' = \mathrm{Card}(C')$ on a que le $\mathcal{V}$-noyau V de C est formé des éléments de la forme $C\rho$ $(c \in C)$ où $p = r \wedge \Pi$ et que pour chaque $n \geq q$ on a $h^n \in A^*$ ssi $n \in r'N$. Par conséquent, la condition énoncée équivaut à $V \subset C'$ et le résultat découle de la Prop. III.1.

Q.E.D.

Une formulation plus élégante due aussi à S.Eilenberg est la suivante : Pour chaque $h \in \Sigma^*$, et $n \in N$ tels que $(h^n)^* \setminus A^*$ est fini on a $(h^m)^* \setminus A^*$ fini, où $m = n \wedge \Pi$.

Nous laissons au lecteur d'en vérifier l'équivalence avec la précédente.

On notera que comme $\mathrm{Card}(A^*\rho)$ peut être borné à priori en fonction de $k = \mathrm{Card}(A\rho)$, il suffit de vérifier l'implication pour tous les mots h de longueur inférieure à une certaine fonction de k et tous les n appartenant à un interval fini qui est aussi fonction de k.

Nous revenons maintenant à des pseudo-variétés plus générales. Elles requièrent une construction assez pesante pour obtenir des ensembles d'éléments contenus dans un groupe.

Nous commençons par introduire un résultat technique en utilisant les théorèmes classiques de Miller et Clifford (Regular D-classes in Semi groups ; Trans Am. Math. Soc. 82 1956. 270-280).

Dans tous ce qui suit Ω_m désigne le segment initial $\{\omega_1, .. \omega_m\}$ de l'alphabet infini $\Omega = \{\omega_j : j \geq 1\}$.

Définition : Soit α_m l'endomorphisme de Ω^* défini par :

$$\omega_j \alpha_m = \omega_1^p \omega_2^p \ldots \omega_{j-1}^p \omega_j^{p+1} \omega_{j+1}^p \ldots \omega_m^p$$

(où $p \geq 1$ est le p.p.c.m des entiers $\geq m$) pour $1 \leq j \leq m$;

$\omega_j \alpha_m = 1$ pour $j \geq m + 1$.

Nous considérons maintenant les endomorphismes α_m^k $(k \in N)$ obtenus en itérant α_m et pour abréger nous écrivons α au lieu de α_m.

III.3. Soit ϕ un morphisme de Ω_m^* dans un monoïde S ayant au plus m éléments.

(i) $\alpha^k\phi = \alpha^{k'}\phi$ pour tout $k' \geq k$ quand $S_k = \Omega_m \alpha^k\phi$ est contenu dans un groupe ;

(ii) Cette dernière condition est satisfaite par au moins un $k \leq m$.

Preuve : Nous posons $s_{j,k} = \omega_j \alpha^k\phi$ et $e_{j,k} = (s_{j,k})p = \omega_j^{p\,k}\alpha^{\phi}$. Donc

$$s_{j,0} = \omega_j\phi \quad \text{et} \quad s_{j,k+1} = e_{1,k}e_{2,k}\cdots e_{j,k}s_{j,k}e_{j+1,k}\cdots e_{m,k},$$

identiquement.

D'après le théorème III.1. et notre choix de p, tous les $e_{j,k}$ sont des idempotents. Donc quand $S_k = \Omega_m \alpha^k\phi = \{s_{j,k} : 1 \leq j \leq m\}$ est contenu dans un groupe, tous ces éléments sont égaux à l'idempotent e de ce dernier et l'on a identiquement $s_{j,k+1} = es_{j,k}e = s_{j,k}$ ce qui établit(i). Soit maintenant pour chaque $k \geq 0$, J_k l'union des idéaux $Se_{j,k}S(1\leq j\leq m)$. Il est clair que chacun de ces derniers contient tous les $s_{i,k+1}$ $(1\leq i\leq m)$ et que par conséquent $J_k \supset J_{k+1}$. Si ℓ est la longueur maximum d'une chaine décroissante d'idéaux (non vides) de S, il existe donc un plus petit $k \leq \ell$ pour lequel $J_k = J_{k+1}$. Or, comme on vient de le dire, J_{k+1} est contenu dans l'intersection des idéqux $Se_{j,k}S(1\leq j\leq m)$ et l'on a la relation $J_{k+1} = J_k = J_{j,k}(1\leq j\leq m)$ qui montre que J_k est un idéal principal. Soit $D = \{s \in S : S\,s\,S = J_k\}$. La relation précédente équivaut à l'assertion que D contient tous les $e_{j,k}(1\leq j\leq m)$ et au poins un $e_{i,k+1}$.

Posons $P = G_1G_2\ldots G_m$, où chaque G_j est la $\mathcal{H}$-classe de $e_{j,k}$. Tous les $s_{j,k+1}(1\leq j\leq m)$ sont contenus dans P. Par conséquent, l'existence d'au moins un $e_{i,k+1} \in D$ montre que $P \cap D \neq \phi$. Comme P est par construction un produit de $\mathcal{H}$-classes contenues dans la $\mathcal{H}$-classe D, les résultats de Clifford et Miller impliquent P soit elle une $\mathcal{H}$-classe contenue dans D et enfin que P soit un groupe ssi $PP^+ \cap D \neq \phi$.

Or cette dernière relation résulte immédiatement de l'existence de $e_{i,k+1} \in D$ et nous avons donc établi que S_{k+1} est contenu dans un groupe.

Pour justifier que $k \leq m$, il suffit enfin d'observer que $\ell = m$ ssi $S = \{1, s, s^2, \ldots, s^m = s^{+1}\}$ où $s^j \neq s^m$ pour $j < m$ et que dans ce cas particulier, l'on a soit $S_0 = S_1 = \ldots = \{1\}$, soit $S_1 = \{s^m\}$.

Q.E.D.

On notera que si l'on suppose $S_k = S_{k+1}$ au lieu de $J_k = J_{k+1}$, la première partie de l'argument montre que chaque $S_{j,k}$ est contenu dans le <u>groupe</u> G_j et que $S_{k+1} \subset p =$ une $\mathcal{H}$-classe dans D. On en conclut de même que P est un groupe d'après $G_j \subset P$ $(1 \leq j \leq m)$.

Université Paris VII
et IRIA
domaine de Voluceau
78150 Rocquencourt