Séminaire Dubreil.
Algèbre et théorie
des nombres

Jean-François Perrot

Une famille de monoïdes inversifs 0-bisimples généralisant le monoïde bicyclique

Séminaire Dubreil. Algèbre et théorie des nombres, tome 25, n° 1 (1971-1972), exp. n° 3, p. 1-15

<http://www.numdam.org/item?id=SD_1971-1972__25_1_A3_0>

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1971-1972, tous droits réservés.

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

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

Séminaire DUBREIL
(Algèbre)
25e année, 1971/72, n° 3, 15 p.

17 janvier 1973

UNE FAMILLE DE MONOÏDES INVERSIFS 0-BISIMPLES GÉNÉRALISANT LE MONOÏDE BICYCLIQUE

par Jean-François PERROT

Dans les pages qui suivent, nous allons étudier (sans donner de démonstrations, celles-ci se trouvant dans notre thèse [11]) la situation d'une famille de monoïdes syntactiques, dont l'étude est par ailleurs de la plus grande importance pour la théorie des langages algébriques, comme l'a montré M. NIVAT. Cette recherche nous conduira à tracer les premières lignes d'une théorie des X-monoïdes qui généralise d'une manière nouvelle celle des ω-monoïdes, due à REILLY et à WARNE. Certains de nos résultats ont fait l'objet d'une Note aux Compte Rendus [10], et d'un exposé au "Second Florida symposium on automata and semigroups", à Gainesville (Florida) en avril 1971.

1. Les monoïdes polycycliques.

1.0. Rappels sur les monoïdes syntactiques et sur les langages de Dyck.

(a) Étant donnée une partie L d'un monoïde M, la congruence syntactique (L) de L est la congruence de M la plus grossière saturant L, i. e., d'après M. TEISSIER [15], on a, pour p et $q \in M$, $p \equiv q \mod (L)$ si, et seulement si, pour tout couple u, v d'éléments de M, $(upv \in L) \Longleftrightarrow (uqv \in L)$.

Le monoïde syntactique M_L de L, est, par définition, le monoïde-quotient $M/(L)$.

On prend le plus souvent pour M le monoïde libre X^*, engendré par un alphabet X : le langage L est alors doué de propriétés combinatoires qui se retrouvent, sous forme algébrique, dans la structure de M_L (cf. M. P. SCHÜTZENBERGER [14] ; le cas particulier où M_L est fini et où tous ses sous-groupes sont triviaux fait l'objet du livre de McNAUGHTON and PAPERT [5]).

D'autre part, le monoïde syntactique M_L est fidèlement représenté par transformations de l'ensemble M/R_L, où R_L est la congruence à droite principale (principal right congruence [2], t. 2), déterminée par L, i. e. pour p, $q \in M$, $p \equiv q \mod R_L$ si pour tout $u \in M$, on a $(pu \in L) \Longleftrightarrow (qu \in L)$: le monoïde M opère à droite dans M/R_L par $\overline{u}.p = \overline{up}$ (où $\overline{u}$ désigne la classe de $u \in M \mod R_L$), définissant ainsi l'automate minimal acceptant L, dont M_L est isomorphe au monoïde de transitions (cf. [11]).

(b) On trouve dans la littérature deux types de langages de Dyck, qui jouent dans la théorie des langages algébriques des rôles fondamentaux très analogues (théorèmes de Chomsky-Schützenberger et de Shamir, cf. M. NIVAT [9], et l'exposé de

L. BOASSON à ce même Séminaire [1]).

Soient X un alphabet, et $\overline{X}$ un alphabet disjoint de X, en bijection avec X : pour $x \in X$, on notera $\overline{x}$ l'élément de $\overline{X}$ qui lui est associé par cette bijection. On considère alors l'alphabet $Z = X \cup \overline{X}$ et le monoïde libre Z^*, sur lequel on définit deux congruences ρ_1 et ρ_2 engendrées respectivement par les relations

$$\{(x\overline{x}, 1) ; x \in X\} \cup \{(\overline{x}x, 1) ; x \in X\} \text{ et } \{(x\overline{x}, 1) ; x \in X\} .$$

Le langage de Dyck du premier type (resp. du second type) sur X, soit $D_1(X)$ (resp. $D_2(X)$), est la classe de 1_{Z^*} mod ρ_1 (resp. mod ρ_2).

Il est clair que le monoïde-quotient Z^*/ρ_1 est isomorphe au groupe libre $\Gamma(X)$ engendré par X, de sorte que le monoïde syntactique correspondant $M_{D_1(X)}$ est isomorphe à $\Gamma(X)$ lui-même. Par exemple, pour $|X| = 1$, on a

$$D_1(\{x\}) = \{w \in \{x , \overline{x}\}^* ; |w|_x = |w|_{\overline{x}}\} ,$$

et $M_{D_1(\{x\})}$ est isomorphe au groupe additif Z des entiers.

C'est à l'étude du monoïde syntactique $M_{D_2(X)}$ du langage de Dyck du second type, ou "langage de Dyck restreint" et à ses prolongements naturels qu'est consacrée la présente section. Nous noterons désormais $D(X)$ au lieu de $D_2(X)$, et nous dirons "langage de Dyck" pour "langage de Dyck du second type".

1.1. Le cas $|X| = 1$.

Pour $|X| = 1$, on vérifie facilement que

$$D(\{x\}) = \{w \in \{x , \overline{x}\}^* ; (|w|_x = |w|_{\overline{x}} \text{ et } w = uv) \text{ entraîne } (|u|_x \geqslant |u|_{\overline{x}})\} .$$

(a) Le quotient du monoïde libre $\{x , \overline{x}\}^*$ par la congruence engendrée par la seule relation $(x\overline{x}, 1)$ est bien connu sous le nom de monoïde bicyclique (cf. [2]), nous le désignerons par B. Il est clair que le monoïde syntactique $M_{D(\{x\})}$ est image homomorphe de B ; or on sait que B n'a d'autres quotients propres que les groupes cycliques, et que, pour toute congruence non triviale, la classe de 1_B ne se réduit pas à $\{1_B\}$, il en résulte donc le théorème suivant.

THÉORÈME. - Le monoïde syntactique du langage de Dyck sur une lettre est isomorphe au monoïde bicyclique.

(b) En tant que monoïde syntactique, B admet une représentation fidèle comme monoïde de transitions de l'automate minimal reconnaissant le langage $D = D(\{x\})$. Or, il ressort de la description de D ci-dessus que, pour $w \in Z^*$, il existe $u \in Z^*$ tel que $wu \in D$ si, et seulement si, pour tout facteur gauche w' de w, on a $|w'|_x \geqslant |w'|_{\overline{x}}$. Les mots de Z^* ne satisfaisant pas cette condition correspondent à un état nul de l'automate, désigné par ω, pour lequel les transitions sont $\omega.x = \omega.\overline{x} = \omega$. Pour tout autre mot w, soit $k = |w|_x - |w|_{\overline{x}}$; on a $wu \in D$ si, et seulement si, u vérifie $|u|_{\overline{x}} - |u|_x = k$, et pour tout facteur gauche u'

de u , $|u'|_{\overline{x}} - |u'|_x \leqslant k$; w est donc équivalent à x^k , et l'état correspondant de l'automate peut être identifié à x^k , avec pour transitions

$$x^k.x = x^{k+1}$$

$$x^k.\overline{x} = x^{k-1} \quad \text{si} \quad k \geqslant 1$$

$$x^0.\overline{x} = \omega \ .$$

Ces transitions peuvent être interprétées comme des $N \times N$ matrices à éléments 0 ou 1 , le fait qu'une transition envoie x^k sur ω apparaissant comme une colonne de rang k identiquement nulle. On retrouve alors exactement la représentation de Schützenberger de B à droite relative à la H-classe de son élément neutre.

(c) Nous allons montrer dans la suite (1.4, théorème B) que, pour $|X| \geqslant 2$, le monoïde syntactique $M_{D(X)}$ est isomorphe au monoïde polycyclique $X^{\&}$ que nous définissons maintenant. A cette fin, nous donnerons, en 1.3, quelques précisions sur le calcul dans $X^{\&}$ et sur sa structure, qui généralise celle de B .

1.2. Définitions du monoïde polycyclique $X^{\&}$ et de l'arbre de base X .

Le monoïde bicyclique B peut également être défini comme l'enveloppe inversive du monoïde additif N des entiers positifs ou nuls [2]. Il fournit le prototype de toute une famille de monoïdes inversifs bisimples. N étant isomorphe au monoïde libre engendré par un seul élément, il est naturel d'introduire la définition ci-après.

(a) Définition. - Soit X un ensemble ayant au moins deux éléments : nous appelons monoïde polycyclique engendré par X , noté $X^{\&}$, l'enveloppe inversive du du monoïde libre X^* engendré par X .

Nous allons voir qu'à de nombreux points de vue la famille des monoïdes polycycliques fournit une généralisation exacte du monoïde bicyclique.

On sait que la structure ordonnée des idempotents de B est celle d'une chaîne infinie discrète ayant un plus grand élément, qui reproduit N ordonné dans l'ordre inverse de l'ordre naturel. La généralisation correspondant à notre propos peut être ainsi définie comme suit.

(b) Définition. - Nous appelons arbre un ensemble ordonné E tel que, pour tout $e \in E$, on ait :

(i) L'idéal engendré par e , c'est-à-dire le sous-ensemble $\{f \in E \ ; \ f \leqslant e\}$, est isomorphe à E . E est donc uniforme au sens de REES [12], il possède un plus grand élément que nous noterons 1_E ;

(ii) Il existe une seule chaîne maximale reliant 1_E à e , laquelle est finie ; on a d'une manière unique $1_E = e_1 > e_2 > \ldots > e_{k-1} > e_k = e$, avec pour $i = 1 , 2 , \ldots , k - 1$, e_{i+1} maximal sous e_i , i. e. $(e_i \geqslant f \geqslant e_{i+1})$ entraîne $(f = e_i \text{ ou } f = e_{i+1})$.

Désignons par $A(X)$ l'ensemble des idéaux à gauche principaux du monoïde libre X^* ordonné par inclusion ; $A(X)$ est isomorphe à l'ensemble des mots de X^* muni de la relation d'ordre $f \leqslant g$ si, et seulement si, il existe $h \in X^*$ tel que $f = hg$. Il est clair que $A(X)$ forme un arbre ; pour $|X| = 1$, on retrouve la chaîne inverse des entiers naturels. Réciproquement, on a le lemme suivant.

(c) LEMME. - Soient E un arbre, X_E l'ensemble des éléments maximaux de E, i. e. $X_E = \{x \in E ; (1_E \geqslant f \geqslant x)$ entraîne $(f = x$ ou $f = 1_E$ pour tout $f \in E)\}$, de tels éléments existent d'après l'hypothèse (ii) : E est isomorphe à $A(X_E)$.

L'ensemble X_E des éléments maximaux de l'arbre E sera ici appelé base de E : nous parlerons d'arbres de base X , en supposant, sauf mention contraire, $|X| \geqslant 2$.

(d) Enfin, on transforme un arbre E en demi-treillis en lui adjoignant un élément nul 0 et en posant, pour e , $f \in E$, si $e \leqslant f$, $e.f = f.e = e$, et si e et f sont incomparables, $e.f = f.e = 0.e = f.0 = 0.0 = 0$. Ce demi-treillis est 0-uniforme au sens de MUNN [8], et nous verrons qu'il fournit le modèle du demi-treillis des idempotents du monoïde polycyclique $X_E^{\&}$.

1.3. Les monoïdes polycycliques comme monoïdes inversifs 0-bisimples.

Nous allons voir que tout monoïde polycyclique $X^{\&}$, par définition inversif, est de plus 0-bisimple.

(a) Une variante de la théorie de CLIFFORD. - Qualifions de "propre", tout monoïde M possédant un zéro tel que $M \setminus \{0\}$ ne soit pas fermé par multiplication, i. e. un monoïde qui ne peut être obtenu par adjonction formelle d'un zéro à un autre monoïde.

Les résultats classiques de CLIFFORD relatifs aux monoïdes inversifs bisimples [2] conduisent à envisager la propriété suivante d'un monoïde P .

(*) P est simplifiable à droite, et pour deux éléments quelconques a et b de P , soit il existe $c \in P$ avec $Pa \cap Pb = Pc$, soit on a $Pa \cap Pb = \emptyset$; de plus, il existe effectivement a et $b \in P$ pour lesquels $Pa \cap Pb = \emptyset$.

On obtient alors les résultats suivants, exactement parallèles à ceux de CLIFFORD.

THÉORÈME.

(i) Soient P vérifiant (*), et M l'enveloppe inversive de P : M est 0-bisimple propre, et le demi-treillis E_M des idempotents de M est isomorphe au demi-treillis obtenu en adjoignant $\emptyset$ à l'ensemble des idéaux principaux à gauche de P . De plus, la R-classe de 1_M coïncide avec la représentation régulière à droite $\overline{P}$ de P , et tout élément non nul de M est de la forme $\overline{q}^{-1}\,\overline{p}$, avec $\overline{p}$, $\overline{q} \in \overline{P}$.

(ii) Soient M un monoïde 0-bisimple propre, P la R-classe de 1_M ; P vérifie (*), et M est isomorphe à l'enveloppe inversive de P .

COROLLAIRE. - Soit P un monoïde vérifiant (*) et n'ayant pas d'autre élément inversible que 1_P : l'enveloppe inversive M de P est isomorphe au monoïde obtenu en munissant l'ensemble $P \times P \cup \{0\}$ de la multiplication suivante : pour $p , q , r , s \in P$, on pose :

$$(p , q)0 = 0(p , q) = 00 = 0 ,$$

$$(p , q)(r , s) = (ap , bs) \text{ si } Pp \cap Pq = Pt \text{ avec } t = aq = br ,$$

$$= 0 \text{ dans tous les autres cas.}$$

De plus, sur M , la relation de Green H se réduit à l'égalité.

(b) La structure des monoïdes polycycliques. - En raison de l'isomorphisme entre P et sa représentation régulière à droite $\overline{P}$, nous les confondrons dans la suite, et nous écrirons p^{-1} , avec $p \in P$, en supposant P plongé dans un monoïde M isomorphe à son enveloppe inversive.

Le théorème et son corollaire sont tous deux applicables si on prend pour monoïde P le monoïde libre X^* engendré par un ensemble X contenant au moins deux éléments. Nous pouvons donc énoncer un théorème.

THÉORÈME. - Le monoïde polycyclique $X^{\&}$ est 0-bisimple ; ses idempotents forment un arbre de base X ; la relation de Green H se réduit à l'égalité sur $X^{\&}$; enfin, $X^{\&}$ est isomorphe au monoïde obtenu en munissant l'ensemble $X^* \times X^* \cup \{0\}$ du produit suivant :

Pour $f , g , f' , g' \in X^*$, on pose :

$$(f , g).0 = 0.(f , g) = 0.0 = 0 ,$$

$$(f , g).(f' , g') = (f , hg') \text{ si } g = hf' ,$$

$$= (kf , g') \text{ si } f' = kg ,$$

$$= 0 \text{ dans tous les autres cas.}$$

N.B. - L'opération ci-dessus a été introduite par M. NIVAT [9] sous le nom de "produit sélectif".

(c) Représentation. - Le monoïde polycyclique $X^{\&}$ est défini en tant qu'enveloppe inversive de X^* comme un monoïde de bijections partielles de X^* dans lui-même. D'autre part, puisque, dans $X^{\&}$, H se réduit à l'égalité, $X^{\&}$ est fondamental au sens de MUNN [7] ; comme tel, on peut le représenter fidèlement par des bijections partielles du demi-treillis de ses idempotents dans lui-même [7] ; or ce dernier est de façon naturelle en bijection avec X^* , chaque idempotent de $X^{\&}$ s'écrivant $u^{-1} u$ avec $u \in X^*$ unique, de sorte que cette représentation est équivalente à celle de la définition.

Ces bijections partielles peuvent aussi être interprétées comme des matrices infinies, de format $X^* \times X^*$, à éléments 0 ou 1 : la matrice correspondant à

$f^{-1}g$, $g \in X^*$, est définie par $(f^{-1}g)_{p,q} = 1$ si, et seulement si, il existe $r \in X^*$ tel que $p = rf$ et $q = rg$. On obtient ainsi une représentation matricielle de $X^\&$ identique à sa représentation de Schützenberger à droite, relative à la H-classe de 1 . Nous verrons plus loin une autre interprétation de cette représentation.

(d) Un exemple de calcul. - L'étroite ressemblance entre le produit sélectif et la représentation du monoïde bicyclique B , donnée en [2] (1.12, exercice 2), permet de transposer pour le monoïde polycyclique un certain nombre de calculs valables dans B : par exemple, sachant que ce dernier est équidivisible [4], on vérifie mécaniquement la proposition suivante.

PROPOSITION. - Le monoïde polycyclique $X^\&$ est 0-équidivisible, i. e. pour $p , q , r , s \in X^\&$, avec $pq \neq 0$, l'égalité $pq = rs$ entraîne l'existence de $m \in X^\&$ vérifiant l'une au moins des deux conditions :

$pm = r$ et $q = ms$,

$q = rm$ et $qm = s$.

1.4. Les monoïdes polycycliques comme monoïdes syntactiques des langages de Dyck.

(a) Une des définitions du monoïde bicyclique B le représente comme le quotient du monoïde libre à deux générateurs x et $\bar{x}$ par l'unique relation $x\bar{x} = 1$. Nous obtiendrons ici une présentation analogue pour le monoïde polycyclique $X^\&$, dont nous déduirons que $X^\&$ est isomorphe à $M_{D(X)}$.

Il est clair que $X^\&$ est engendré en tant que monoïde par l'ensemble des générateurs de X^* et de leurs inverses : soit donc $\bar{X} = \{\bar{x} ; x \in X\}$ un ensemble disjoint de X , en bijection avec X , et $Z = X \cup \bar{X}$; notons ρ la congruence du monoïde libre Z^* engendrée par les relations $\{x\bar{x} = 1 ; x \in X\}$: il est clair que $X^\&$ est une image homomorphe de Z^*/ρ . Plus précisément, on a le théorème A.

THÉORÈME A. - $X^\&$ est isomorphe au quotient de Rees de Z^*/ρ par son idéal bilatère maximal.

Or, le langage de Dyck D(X) étant la classe de 1_{Z^*} mod ρ , son monoïde syntactique M est image homomorphe de Z^*/ρ , et deux éléments de l'idéal bilatère maximal de Z^*/ρ ont même image dans M : M est donc l'image homomorphe de $X^\&$. Nous verrons dans la section suivante (une preuve directe a été donnée en [10]) que $X^\&$ n'admet point de quotient propre non trivial, d'où le théorème B.

THÉORÈME B. - Pour $|X| \geqslant 2$, le monoïde syntactique du langage de Dyck sur X est isomorphe au monoïde polycyclique $X^\&$.

Mentionnons pour mémoire que le théorème A implique également, pour $|X|$ fini, que $X^\&$ admet une présentation finie.

COROLLAIRE. - Le monoïde polycyclique admet la présentation suivante :

ensemble générateur $Z = \{x\ ;\ x \in X\} \cup \{\overline{x}\ ;\ x \in X\}$,

relations de définition $\{x\overline{x}=1\ ;\ x \in X\} \cup \{\overline{x}yz=zx\overline{y}=\overline{xy}\ ;\ x,y \in X\ ,\ x \neq y\ ,\ z \in Z\}$.

(b) $X^{\&}$ comme monoïde de transitions : Nous avons vu que la représentation du monoïde bicyclique comme monoïde de transitions était en fait identique à sa représentation de Schützenberger : nous allons à présent faire la même observation pour le monoïde polycyclique $X^{\&}$, monoïde syntactique du langage de Dyck $D = D(X)$.

Un mot $w \in Z^*$ tel qu'il existe $u \in Z^*$ avec $wu \in D$ a une image dans $X^{\&}$ qui est nécessairement dans la $\mathcal{R}$-classe de l'élément neutre, et deux mots de Z^* sont équivalents si, et seulement si, ils ont même image. L'automate se compose donc de l'état nul, et d'un ensemble d'états qu'on peut identifier avec X^* , les transitions étant, pour $u \in X^*$ et $x \in x$,

$$u.x = ux$$

$$u\overline{x} = u' \quad \text{si} \quad u = u'x$$

$$u\overline{x} = \omega \quad \text{sinon.}$$

En convenant de dénoter qu'une transition envoie l'état w , $w \in X^*$, sur ω , par une colonne de rang w identiquement nulle, on peut représenter $X^{\&}$ par des $X^* \times X^*$ matrices à éléments 0 et 1 , qui sont exactement celles de la représentation de Schützenberger à droite relative à la $\mathcal{H}$-classe de l'élément neutre.

2. Les X-monoïdes.

REILLY [13], sous le nom de " ω semigroupes", et WARNE [16], avec une autre terminologie, ont étudié les monoïdes inversifs bisimples dont les idempotents forment une chaîne discrète, et ont montré que, dans cette théorie, le monoïde bicyclique jouait un rôle distingué. Nous sommes donc conduits à chercher si, dans la théorie des monoïdes inversifs 0-bisimples dont les idempotents forment un arbre de base X , le monoïde polycyclique $X^{\&}$ joue un rôle comparable : nous allons voir que la situation est sensiblement plus compliquée que dans le cas des ω-semigroupes.

Étant donné un ensemble $X \neq \emptyset$, nous appelons X-monoïde tout monoïde inversif 0-bisimple (ou bisimple si $|X| = 1$) dont les idempotents forment un arbre de base X . Pour $|X| = 1$, on obtient les ω-semigroupes.

Nous étudierons d'abord les congruences des X-monoïdes pour $|X| \geqslant 2$, nous donnerons ensuite l'amorce d'une classification pour $|X|$ quelconque.

2.1. Des congruences d'un X-monoïde ($|X| \geqslant 2$) .

(a) THÉORÈME. - Pour $|X| \geqslant 2$, toute congruence d'un X-monoïde autre que la congruence universelle est plus fine que l'équivalence de Green H .

On montre que, si θ est une congruence d'un X-monoïde M, l'existence de p et $q \in M$, $p \equiv q \mod \theta$, $p \not\equiv q \mod \mathcal{K}$, entraîne l'existence d'un élément non nul de M, congru à $0 \mod \theta$, ce qui entraîne le résultat puisque M est 0-simple et que la classe de $0 \mod \theta$ est un idéal bilatère.

(b) On sait (HOWIE [3]) que, dans un monoïde inversif M, les congruences plus fines que $\mathcal{K}$ sont exactement celles qui séparent les idempotents de M, et que M possède une congruence maximale de ce type unique, notée $\mu(M)$, et définie ainsi : Pour $p, q \in M$, on a $p \equiv q \mod \mu(M)$ si, et seulement si, tout idempotent $e \in M$ vérifie $p^{-1}ep = q^{-1}eq$. MUNN [7] appelle <u>fondamental</u> un monoïde M pour lequel $\mu(M)$ est réduite à l'égalité, et montre que $M/\mu(M)$ est toujours fondamental.

COROLLAIRE.

(i) <u>Dans un X-monoïde M, $\mu(M)$ est l'unique congruence maximale de M</u> ;

(ii) <u>Un X-monoïde M possède un seul quotient fondamental non trivial, à savoir</u> $M/\mu(M)$;

(iii) <u>Un X-monoïde n'admet pas d'autre congruence que l'égalité et la congruence universelle si, et seulement si, il est fondamental : c'est en particulier le cas du monoïde polycyclique $X^{\&}$</u>.

(c) Par ailleurs, MUNN [6] a montré que l'idéal $\mathcal{C}$ du treillis des congruences d'un monoïde inversif 0-bisimple M, formé des congruences plus fines que $\mathcal{K}$, était isomorphe au sous-treillis du treillis des sous-groupes distingués du groupe G des éléments inversibles de M, formé des sous-groupes D, vérifiant $pD \subset Dp$, pour tout p dans la $\mathcal{R}$-classe P de 1_M, à $\theta \in \mathcal{C}$ correspondant la classe de $1_M \mod \theta$. On a donc en particulier le théorème suivant.

COROLLAIRE. - <u>Le treillis des congruences d'un X-monoïde est modulaire</u>.

(d) Soit K le sous-groupe de G correspondant à μ dans la bijection précédente : d'après Munn, K est le sous-groupe maximum de G vérifiant $pK \subset Kp$ pour tout $p \in P$. On peut également le caractériser par la :

PROPOSITION. - <u>On a</u> $K = \{k \in G \mid Ppk = Pp$ <u>pour tout</u> $p \in P\}$.

Notons que les sous-groupes distingués de G contenus dans K ne possèdent pas tous la propriété requise, si bien que le sous-treillis obtenu, dont K est le plus grand élément, ne coïncide pas avec l'idéal engendré par K du treillis des sous-groupes distingués de G : des exemples seront donnés en 2. d).

De la proposition suit le :

(e) COROLLAIRE. - <u>Soit M un X-monoïde, P la $\mathcal{R}$-classe de 1_M</u> :

(i) <u>la congruence maximale μ de M est définie par $a, b \in M$, on a</u> $a \equiv b$

mod μ si $a = u^{-1} v$, $b = r^{-1} s$, avec $u = gr$ et $v = hs$, $u , v , r , s \in P$, et g , h inversibles dans M vérifiant, pour tout $p \in P$, $Ppg = Pph$.

(ii) M est fondamental si, et seulement si, pour tout élément inversible g de M , $g \neq 1_M$, il existe $p \in P$ tel que l'on ait $Ppg \neq Pp$.

(f) Exemple de X-monoïde fondamental :

Soit P le produit semi-direct à gauche d'un monoïde libre X^* par son groupe d'automorphismes G (qui est isomorphe au groupe symétrique sur X), obtenu en munissant l'ensemble GxX^* de l'opération $(g , u)(h , v) = (gh , h(u)v)$. Il est clair que $P.(g , u) = \{(h , wu) ; h \in G , w \in X^*\}$ de sorte que P vérifie (*) et que ses idéaux à gauche principaux forment un arbre de base X ; l'enveloppe inversive M de P est un X-monoïde fondamental d'après le corollaire précédent, car aucun élément de G ne laisse fixes tous les mots de X^* .

2.2. Une généralisation du théorème de Reilly ($|X| \geq 2$) .

(a) L'exemple 1.f ci-dessus montre qu'il existe des X-monoïdes fondamentaux pour lesquels H ne se réduit pas à l'égalité, donc pour lesquels H n'est pas une congruence. De ce point de vue, le monoïde polycyclique peut être ainsi caractérisé parmi les X-monoïdes :

THÉORÈME. - Un X-monoïde M est isomorphe au monoïde polycyclique $X^{\&}$ si, et seulement si, H se réduit à l'égalité sur M .

Ce résultat découle immédiatement de la proposition suivante.

(b) PROPOSITION. - Tout X-monoïde M contient un sous-monoïde isomorphe à $X^{\&}$, qui possède exactement un élément par $\mathcal{R}$-classe de M .

Soit P la $\mathcal{R}$-classe de 1_M : d'après le théorème 1 , P vérifie (*), et ses idéaux à gauche principaux forment un arbre de base X . Nous montrerons, en adaptant un raisonnement de REES [12], que P contient un sous-monoïde isomorphe à $X^{\&}$, qui a exactement un élément par $\mathcal{L}$-classe de P . M étant isomorphe à l'enveloppe inversive de P , il est clair que ses éléments de la forme $u^{-1} v$, $u , v \in X^*$, constituent le sous-monoïde cherché. La proposition se déduit donc du lemme ci-après.

LEMME. - Soit P un monoïde simplifiable à droite dont les idéaux principaux à gauche forment un arbre de base X ; P contient un sous-monoïde isomorphe au monoïde libre X^* , qui possède exactement un élément dans chaque $\mathcal{L}$-classe de P .

(c) COROLLAIRE. - Un X-monoïde M admet $X^{\&}$ comme (unique) quotient fondamental si, et seulement si, H est une congruence de M .

D'après la proposition, les seuls X-monoïdes admettant $X^{\&}$ pour quotient fonda-

mental sont donc les produits semi-directs (split extensions) de $X^{\&}$ par des groupes : on peut les décrire en traduisant les formules générales données par MUNN [8] dans une notation inspirée par la forme du théorème de Reilly :

Soient G un groupe, et φ un homomorphisme de X^* dans le monoïde $End(G)$ des endomorphismes de G (considérés comme opérant à gauche dans G) ; on désigne par $M(X , G , \varphi)$ le monoïde obtenu en munissant l'ensemble $(X^* \times G \times X^*) \cup \{0\}$ de la multiplication suivante :

$$(u , g , v).0 = 0.(u , g , v) = 0.0 = 0$$

$$(u , g , v).(u' , g' , v') = (u , g\varphi(h)g' , hv') \quad \text{si} \quad v = hu'$$

$$= (ku , \varphi(k)gg' , v') \quad \text{si} \quad u' = kv$$

$$= 0 \quad \text{dans tous les autres cas.}$$

Nous pouvons donc énoncer le théorème suivant.

THÉORÈME. - Un monoïde M est un X-monoïde pour lequel H est une congruence si, et seulement si, il existe un homomorphisme φ de X^* dans $End(G)$, G étant le groupe des éléments inversibles de M , tel que M soit isomorphe au monoïde $M(X , G , \varphi)$.

(d) Remarque. - Ce résultat généralise évidemment la structure des ω-semigroupes bisimples. $M(X , G , \varphi)$ est d'autre part l'enveloppe inversive de $P = G \times X^*$ avec pour multiplication, pour $g , h \in G$ et $u , v \in X^*$,

$$(g , u)(h , v) = (g\varphi(u)h , uv)$$

qui généralise la construction de REES [12].

On peut ainsi construire des monoïdes M pour lesquels le treillis de congruences est strictement contenu dans l'idéal du treillis des sous-groupes distingués de G , engendré par K (cf. 1 (d)) : on a ici $K = G$, il suffit donc de prendre G abélien, et φ tel que pour un élément g et un mot $w \in X^*$ au moins $\varphi(w)g$ ne soit pas une puissance de g : le sous-groupe cyclique $\langle g \rangle$ engendré par g ne vérifiera pas $w\langle g \rangle \subset \langle g \rangle w$, il ne lui correspondra donc pas de congruence de M .

2.3. Structure des X-monoïdes : le théorème fondamental.

(a) Nous venons de voir que les X-monoïdes permettaient effectivement de généraliser le théorème de Reilly, mais que ce résultat n'épuisait pas leur structure : nous nous proposons, dans la section suivante, d'indiquer les grandes lignes d'une classification de ce type de monoïdes.

D'après le théorème 1.3 (a), un X-monoïde M est déterminé à un isomorphisme près par la donnée de la $\mathcal{R}$-classe P de 1_M , M étant isomorphe à l'enveloppe inversive de P : ce sont donc les monoïdes P , simplifiables à droite et dont les idéaux principaux à gauche forment un arbre de base X , que nous allons prendre comme base de notre étude, et dans la suite, P désignera un tel monoïde, G le

groupe de ses éléments inversibles, et X la base de l'arbre des idéaux à gauche principaux, identifiée avec un système de représentants des $\mathcal{L}$-classes engendrant les idéaux à gauche principaux maximaux.

(b) Structure de P .

PROPOSITION. - P est en bijection avec l'ensemble $G \times X^*$.

Il reste à munir l'ensemble $G \times X^*$ d'une multiplication qui transforme cette bijection en un isomorphisme. Notons d'abord que, dans P , on a

$$(gw)(g' w') = g(wg')w'$$

de sorte que le problème se ramène à trouver la décomposition de wg' sous la forme $wg' = hu$, avec $h \in G$ et $u \in X^*$: il est clair que h peut être cherché sous la forme " g' transformé par l'action de w " et u sous la forme " w transformé par l'action de g' ". Considérons donc une application φ de X^* dans l'ensemble de toutes les applications de G dans lui-même, qui à $w \in X^*$ associe l'application $g \longmapsto \varphi_w(g)$, et une application ψ de G dans l'ensemble de toutes les applications de X^* dans lui-même qui à $g \in G$ associe l'application $w \longmapsto w\psi_g$: nous sommes amenés à écrire ainsi la multiplication cherchée :

$$(g , w).(g' , w') = (g\varphi_w(g') , w\psi_{g'} , w') .$$

Cette multiplication doit faire de $G \times X^*$ un monoïde possédant les propriétés requises, ce qui ne manquera pas d'imposer quelques restrictions au choix des applications φ et ψ .

Désignons par $P(X , G , \varphi , \psi)$ le monoïde obtenu par le procédé que nous venons d'esquisser. Tous calculs faits, on obtient le résultat suivant :

THÉORÈME. - Soient G un groupe, X un ensemble, $\hat{\psi}$ un homomorphisme de G dans le groupe S_X des permutations de X , opérant à droite dans X , $\hat{\varphi}$ une application de X dans le monoïde de toutes les applications de G dans lui-même qui laissent 1_G fixe, opérant à gauche dans G , $\hat{\varphi}$ et $\hat{\psi}$ étant liées par la relation :

$$\hat{\varphi}_x(gg') = \hat{\varphi}_x(g)\, \hat{\varphi}_{x\hat{\psi}_g}(g') .$$

On considère l'homomorphisme φ du monoïde libre X^* engendré par X qui prolonge $\hat{\varphi}$, et pour $w \in W^*$ et $g \in G$, on définit par récurrence sur $|w|$ le mot $w\psi_g$ comme suit :

$$1_{X^*}\psi_g = 1_{X^*} ;$$

pour $w = ux$, $u \in X^*$, $x \in X$,

$$w\psi_g = u\psi_{\hat{\varphi}_x(g)}\, x\hat{\psi}_g .$$

Alors :

(a) ψ est un homomorphisme de G dans le groupe de toutes les bijections de

X^* sur lui-même qui conservent la longueur des mots ;

(b) l'ensemble $G \times X^*$ est muni par la multiplication

$$(g , w)(g' , w') = (g\varphi_w(g') , w\psi_{g'} , w') ,$$

avec $(1_{G'} , 1_{X^*})$ comme unité, d'une structure de monoïde $P(X , G , \varphi , \psi)$ simplifiable à droite, dont les idéaux à gauche principaux forment un arbre de base X.

Réciproquement, la $\mathcal{R}$-classe P de l'élément neutre d'un X-monoïde M est isomorphe à un monoïde $P(X , G , \varphi , \psi)$, où G est le groupe des éléments inversibles de M, pour un choix convenable de $\hat{\varphi}$ et de $\hat{\psi}$.

2.4. Construction de quelques familles de X-monoïdes.

Nous allons à présent montrer comment le théorème de structure précédent permet de classer les X-monoïdes que nous avons rencontrés jusqu'ici et d'en construire quelques autres. Nous noterons $\mathcal{M}(X , G , \varphi , \psi)$ l'enveloppe inversive de $P(X , G , \varphi , \psi)$.

(a) Construction "avec endomorphismes" et "avec automorphismes". - Par la facilité de manipulation qu'il autorise, un cas particulier de la construction générale précédemment décrite retient l'attention : celui où φ envoie X^* dans le monoïde $\mathrm{End}(G)$ des endomorphismes de G.

Ceci a lieu si, et seulement si, l'image de X par $\hat{\varphi}$ est entièrement contenue dans $\mathrm{End}(G)$, donc, après calculs, si, et seulement si, $\hat{\varphi}$ et $\hat{\psi}$ vérifient, pour tout $g \in G$ et $x \in X$,

$$(+) \qquad \hat{\varphi}_{x\hat{\psi}_g} = \hat{\varphi}_x .$$

Une condition suffisante, qui est aussi nécessaire si l'image de G par $\hat{\psi}$ est un groupe transitif sur X, pour que (+) soit satisfaite est que l'on ait $\hat{\varphi}_x = \hat{\psi}_y$ pour tout couple (x , y) d'éléments de X : l'image de X par $\hat{\varphi}$ se réduit alors à une seule application α de G dans lui-même, nécessairement un endomorphisme de G, et l'homomorphisme φ se factorise à travers l'homomorphisme canonique de X^* sur N qui à chaque mot associe sa longueur ; on en tire comme prévu $\varphi_{w\psi_g} = \varphi_w$ pour tout $w \in X^*$ et tout $g \in G$ puisque ψ_g conserve la longueur. L'agrément de ce procédé vient de ce que le choix de l'endomorphisme est indépendant de la donnée de $\hat{\psi}$, la nature de α n'intervenant que pour étendre $\hat{\psi}$ en ψ, alors que dans les autres cas on est conduit à des vérifications fastidieuses.

Symétriquement, on peut examiner le cas où ψ envoie G dans le groupe des automorphismes de X^*, et montrer que ce cas se réalise si, et seulement si, $\hat{\varphi}$ et $\hat{\psi}$ vérifient

$$(++) \qquad \hat{\psi}_{\hat{\varphi}_x(g)} = \hat{\psi}_g \quad \text{pour tout } x \in X \text{ et tout } g \in G .$$

(b) X-monoïdes pour lesquels H est une congruence. - Si $|X| = 1$, X^* est isomorphe à N, nous utiliserons donc la notation correspondante ; le groupe S_X

étant trivial, la relation (+) est vérifiée et $\varphi_1 = \alpha$ est un endomorphisme de G, on a $\varphi_n = \alpha^n$, et la multiplication de P se réduit à

$$(g , n)(g' , n') = (g\alpha^n(g') , n + n') .$$

On retrouve la structure étudiée par REES [12] sur laquelle se fonde le théorème de REILLY [13].

Plus généralement, lorsque l'image de G par ψ est triviale (l'image de G par $\hat{\psi}$ est triviale en même temps), (+) est vérifiée, et φ est un homomorphisme de X^* dans $\mathrm{End}(G)$; la multiplication de P s'écrit

$$(g , w)(g' , w') = (g\varphi_w(g') , ww') ,$$

l'enveloppe inversive de P est alors un X-monoïde $M(X , G , \varphi)$ dans lequel H est une congruence et auquel s'applique le théorème 2 (d).

Nous voyons donc que les théorèmes "à la Reilly" sont obtenus lorsque l'image de G par ψ est triviale. Il résulte en effet de la caractérisation 2.1 (e) de la congruence maximale d'un X-monoïde que le noyau de ψ dans G est exactement de la classe de $1_M \bmod \mu$.

(c) X-monoïdes fondamentaux. - On tire immédiatement de la remarque précédente un théorème.

THÉORÈME. - Le X-monoïde $M(X , G , \varphi , \psi)$ est fondamental si, et seulement si, ψ est un monomorphisme.

Une première manière d'obtenir des X-monoïdes fondamentaux est de choisir pour $\hat{\psi}$ un monomorphisme de G dans S_X, i. e. de prendre pour G un sous-groupe du groupe symétrique S_X, et pour $\hat{\varphi}$ une application convenable, en se servant éventuellement du procédé exposé en (a) : en effet, dans ce cas, ψ est nécessairement aussi un monomorphisme, comme on le vérifie facilement. Si G est trivial, on obtient le monoïde polycyclique ; si on prend $G = S_X$ tout entier, $\hat{\psi}$ étant l'application identique de G sur lui-même, l'action de G pourra être étendue par ψ pour donner $\mathrm{Aut}(X^*)$, d'après (++), si, et seulement si, φ envoie X tout entier sur l'automorphisme identique de G : on retrouve ainsi l'exemple de X-monoïde fondamental donné en 1 (f).

Toutefois cette méthode est loin d'épuiser toutes les possibilités : en effet, la condition " $\hat{\psi}$ injectif" suffit à entraîner " ψ injectif", mais elle n'est nullement nécessaire. Les noyaux des deux homomorphismes ψ et $\hat{\psi}$ sont reliés par l'égalité suivante,

$$\mathrm{Ker}\ \psi = \{g \in G ;\ \text{pour tout } w \in X^* ,\ \varphi_w(g) \in \mathrm{Ker}\ \hat{\psi}\} .$$

A condition que $\mathrm{Ker}\ \hat{\psi}$ ne soit pas G tout entier, l'action de φ peut donc transformer un homomorphisme $\hat{\psi}$ non injectif en un monomorphisme ψ : il est clair que pour obtenir ce résultat le choix de $\hat{\varphi}$ n'est pas indifférent.

Par exemple, on peut prendre pour G le produit direct de k exemplaires d'un sous-groupe non trivial H de S_X (k entier positif quelconque), $\hat{\psi}$ étant le

produit de la projection de G sur sa j-ième composante (j fixé, $1 \leqslant j \leqslant k$) par un monomorphisme de H dans S_X (pour lequel on peut choisir l'injection canonique de H dans S_X), et pour $\hat{\varphi}$, suivant le procédé (a), l'application qui envoie X sur un endomorphisme α de G tel que, pour tout $g \in G$, $g \neq 1_G$, dont la j-ième composante g_j est 1_H, il existe un entier n vérifiant

$$(\alpha^n(g))_j \neq 1_H ,$$

i. e. α tel que, pour tout $g \in \operatorname{Ker} \hat{\psi} \setminus 1_G$, il existe n avec $\alpha^n(g) \notin \operatorname{Ker} \hat{\psi}$: de tels endomorphismes existent, on peut prendre notamment pour α l'automorphisme de G d'ordre k qui permute circulairement les composantes de $G = H^k$.

Ce procédé établit l'existence de X-monoïdes fondamentaux, avec X fixé, $|X| \geqslant 2$ et $|G|$ arbitrairement grand.

D'autres constructions sont certainement possibles : la recherche des méthodes utilisant les procédés précédents relève de la théorie des groupes ; si on sort de ce cadre, la détermination de $\hat{\varphi}$ est souvent délicate : voici par exemple un résultat relatif au cas $|X| = 2$ (ou $X = \{x , y\}$) :

THÉORÈME. - Soit $M(x , y , G , \varphi , \psi)$ un $\{x , y\}$-monoïde fondamental tel que $\varphi_x \neq \varphi_y$; alors nécessairement G est un 2-groupe non commutatif.

On vérifie que la construction n'est pas possible si G est le groupe des quaternions, mais qu'elle l'est effectivement pour G le groupe diédral d'ordre 8.

BIBLIOGRAPHIE

[1] BOASSON (L.). - Cônes rationnels et familles agréables de langages, Séminaire Dubreil : Algèbre, 25e année, 1971/72, n° 15, 5 p.

[2] CLIFFORD (A. H.) and PRESTON (G. B.). - The algebraic theory of semigroups, Vol. 1 and 2. - Providence, American mathematical Society, 1961 and 1967 (Mathematical Surveys, 7).

[3] HOWIE (J. M.). - The maximum idempotent-separating congruence on an inverse semigroup, Proc. Edinburgh math. Soc., Series 2, t. 14, 1964, p. 71-79.

[4] McKNIGHT (J. D. Jr) and STOREY (A. J.). - Equidivisible semigroups, J. of Algebra, t. 12, 1968, p. 24-48.

[5] McNAUGHTON (R.) and PAPERT (S.). - Counter-free automata. - MIT Press, 1971.

[6] MUNN (W. D.). - The idempotent-separating congruences on a regular 0-bisimple semigroup, Proc. Edinburgh math. Soc., t. 15, 1967, p. 233-240.

[7] MUNN (W. D.). - Fundamental inverse semigroups, Quart. J. Math., Oxford, Series 2, t. 21, 1970, p. 157-170.

[8] MUNN (W. D.). - 0-bisimple inverse semigroups, J. of Algebra, t. 15, 1970, p. 570-588.

[9] NIVAT (M.). - Transductions des langages de Chomsky, Ann. Inst. Fourier, Grenoble, t. 18, 1968, p. 339-456.

[10] NIVAT (M.) et PERROT (J.-F.). - Une généralisation du monoïde bicyclique, C. R. Acad. Sc. Paris, t. 271, 1970, Série A, p. 824-827.

[11] PERROT (J.-F.). - Contribution à l'étude des monoïdes syntactiques et de certains groupes associés aux automates finis, Thèse Sc. math. Paris, 1972.

[12] REES (D.). - On the ideal structure of a semigroup satisfying a cancellation law, Quart. J. Math., Oxford, Series 2, t. 19, 1948, p. 101-108.

[13] REILLY (N.). - Bisimple ω-semigroups, Proc. Glasgow math. Assoc., t. 7, 1966, p. 160-167.

[14] SCHÜTZENBERGER (M. P.). - Langages formels et monoïdes finis, Séminaire Dubreil-Pisot : Algèbre et théorie des nombres, 23e année, 1969/70, Fasc. 2 : Demi-groupes [1970. Nice], n° 3, 3 p.

[15] TEISSIER (M.). - Sur les équivalences régulières dans les demi-groupes, C. R. Acad. Sc. Paris, t. 232, 1951, p. 1987-1989.

[16] WARNE (R. J.). - A class of bisimple semigroups, Pacific. J. of Math., t. 18, 1966, p. 563-577.

Jean-François PERROT
8 rue Faubourg Poissonnière
75010 PARIS