Semigroup Forum Vol. 18 (1979) 33-49

RESEARCH ARTICLE

UNE TOPOLOGIE DU MONOÏDE LIBRE

Christophe Reutenauer

Communiqué par G. Lallement

Nous étudions dans cet article une topologie du monoïde libre X^* et en particulier les sous-monoïdes fermés pour celle-ci. Cette topologie s'obtient par restriction d'une topologie du groupe libre G_X engendré par X, à savoir la topologie des sous-groupes d'indice fini, étudiée par M. Hall [6], qui joue un rôle fondamental dans la théorie des groupes profinis. Les sous-monoïdes fermés de X^* sont étroitement liés à des sous-monoïdes déjà étudiés par M. Keenan et G. Lallement [7] et par J.F Perrot [8]. Enfin, les ensembles denses pour cette topologie caractérisent certaines propriétés arithmétiques des séries rationnelles comme l'ont montré G. Rauzy [11], J. Berstel [2] et l'auteur [12].

La topologie de X^* que nous considérons admet pour base d'ouverts les langages rationnels à groupe (les langages p-réguliers de G. Thierrin [10]) i.e. les sous-ensembles de X^* dont le monoïde syntactique est un groupe fini ; un langage est rationnel à groupe si et seulement s'il est intersection avec X^* d'une partie reconnaissable de G_X.

Nous montrons qu'il y a bijection canonique entre les sous-monoïdes rationnels à groupe de X^* et les sous-groupes d'index fini de G_X (théorème 1) : à un tel sous-monoïde est associé le sous-groupe H qu'il engendre dans G_X et l'application réciproque est $H \longmapsto H \cap X^*$. Les sous-monoïdes rationnels à groupe sont aussi caractérisés par le fait qu'ils sont à la fois ouverts et fermés (proposition 11). Nous donnons une caractérisation des sous-monoïdes fermés de X^* (proposition 8) analogue à celle des sous-groupes fermés de G_X donnée par M. Hall [6] (th. 3.4.). Par ailleurs, ces sous-monoïdes sont bipréfixes et en particulier libres. Les sous-monoïdes fermés qui sont rationnels font l'objet d'une caractérisation plus précise, en termes de leur automate

0037-1912/79/0018-0033 $03.40

minimal : celui-ci est à transitions injectives et fini (théorème 2). Lorsque cette hypothèse de finitude est levée on obtient exactement les sous-monoïdes de X^* qui sont intersection avec X^* d'un sous-groupe de G_X (proposition 5). Nous montrons encore que si M est un sous-monoïde rationnel qui est fermé, alors sa base est également fermée (proposition 10) et que le sous-groupe qu'il engendre dans G_X est fermé dans G_X (proposition 12). Curieusement, ces considérations topologiques permettent de démontrer un résultat de théorie des autómates dont la preuve directe n'est pas immédiate (proposition 9).

I. GENERALITES.

1. Rappels.

Nous évoquons brièvement les notions classiques dont nous aurons besoin. Un exposé plus complet se trouve dans le traité de S. Eilenberg [4] (chap. II,III,IV).

Soit M un monoïde et A une partie de M. Il existe un couple (M_A, φ_A) où M_A est un monoïde et φ_A un homomorphisme surjectif $M \longrightarrow M_A$ tel que $A = \varphi_A^{-1}(\varphi_A(A))$ et vérifiant : pour tout couple (M', φ) où M' est un monoïde et φ un homomorphisme surjectif $M \longrightarrow M'$ tels que $A = \varphi^{-1}(\varphi(A))$, il existe un unique homomorphisme $M' \longrightarrow M_A$ rendant commutatif le diagramme :

$$\begin{tikzcd} & M \arrow[dl, "\varphi"'] \arrow[dr, "\varphi_A"] & \\ M' \arrow[rr] & & M_A \end{tikzcd}$$

M_A est appelé le monoïde syntactique de A. A est reconnaissable si M_A est fini ou, ce qui est équivalent, s'il existe un couple (M', φ) comme ci-dessus avec M' fini.

L'ensemble des parties rationnelles de M est le plus petit ensemble de parties de M qui contient les parties finies et qui est fermé par réunion finie, produit et étoile (le produit de deux parties A et B est $\{ab \mid a \in A, b \in B\}$ et l'étoile de A est $A^* = \bigcup_{n \geqslant 0} A^n$: c'est le sous-monoïde engendré par A).

On sait (cf. [4] chap. VII prop. 5.4) que si M est un monoïde de type fini, alors toute partie reconnaissable est rationnelle.

Soit X un ensemble fini et X^* le monoïde libre engendré par X ; ses éléments sont appelés des mots, son élément neutre est noté 1 et ses sous-ensembles sont appelés des langages. Dans X^*, une partie est reconnaissable si et seulement si elle est rationnelle (théorème de Kleene).

Suivant les notations d'Eilenberg [4], un automate $\mathcal{A}$ sur X^* est un quadruplet $\mathcal{A} = (Q, q_o, Q_f, \lambda)$ où Q est un ensemble (appelé ensemble des états), $q_o \in Q$(l'état initial), Q_f une partie de Q (l'ensemble des états finaux) et où $\lambda : Q \times X^* \to Q$ est une application partielle vérifiant :

. $\forall q \in Q, \forall w,w' \in X^* : \lambda(q,ww') \neq \emptyset$ est équivalent à $\lambda(q,w) = q' \neq \emptyset$ et $\lambda(q',w') \neq \emptyset$. Et dans ce cas : $\lambda(q,w\,w') = \lambda(\lambda(q,w),w')$.

. $\forall q \in Q,\ \lambda(q,1) = q$.

Autrement dit, X^* opère à droite sur Q, ou encore : l'application $w \longmapsto \lambda(\ ,w)$ de X^* dans le monoïde des applications partielles $Q \longrightarrow Q$ est un homomorphisme. L'image de cette application est appelée le monoïde des transitions de l'automate $\mathcal{A}$. Comme X^* est librement engendré par X, la donnée de λ équivaut à la donnée de sa restriction à $Q \times X$. Le langage reconnu par $\mathcal{A}$, noté $L(\mathcal{A})$, est $\{w \in X^* \mid \lambda(q_o,w) \in Q_f\}$. On montre aisément que le monoïde des transitions de $\mathcal{A}$ reconnaît $L(\mathcal{A})$. Réciproquement, si M est un monoïde, φ un homomorphisme $X^* \longrightarrow M$ et P une partie de M, on leur associe l'automate $\mathcal{A}' = (M, \varphi(1), P, \lambda)$ où λ est défini par l'opération à droite de X^* sur M déterminée par φ ; on a clairement : $L(\mathcal{A}) = \varphi^{-1}(P)$.

Un automate $\mathcal{A}$ est dit émondé cf. [13] si : $\forall q \in Q$
(1) $\exists\, w,w' \in X^*$ tels que $\lambda(q_o,w) = q$, $\lambda(q,w') \in Q_f$. Si $\mathcal{A}$ n'est pas émondé, l'automate $\mathcal{A}'$ obtenu en supprimant dans $\mathcal{A}$ les états q ne vérifiant pas (1) est émondé et l'on a $L(\mathcal{A}) = L(\mathcal{A}')$. On dit que $\mathcal{A}'$ s'obtient en émondant $\mathcal{A}$.

Toute partie de X^* possède un automate qui lui est canoniquement associé et qui la reconnaît, son automate minimal. Un automate $\mathcal{A}$ est minimal pour $L(\mathcal{A})$ si et seulement si $\mathcal{A}$ est émondé et si
(2) $\forall q,q' \in Q$: si $\forall w \in X^*$, $(q,w) \in Q_f$ équivaut à $(q',w) \in Q_f$, alors $q = q'$.

On montre que le monoïde syntactique d'un langage est canoniquement isomorphe au monoïde des transitions de son automate minimal. Par suite un langage est reconnaissable (rationnel) si et seulement si son automate minimal est fini (i.e. Q est fini).

$\mathcal{A}$ est dit pointé si $Q_f = \{q_o\}$.
Un code préfixe est une partie C de X^* qui vérifie : $\forall u,v \in X^*$: $u,uv \in C \Rightarrow v = 1$. C est alors la base d'un sous-monoïde libre de X^*. Une partie de X^* est un sous-monoïde libre admettant pour base un code préfixe si et seulement si son automate minimal est pointé [4] (chap. IV prop. 3.1.). Un tel sous-monoïde est dit unitaire.

Un code bipréfixe est un code préfixe C dont l'image miroir C est également un code préfixe. Un sous-monoïde M de X^* est libre et admet pour base un code bipréfixe si et seulement si : $\forall u,v \in X^*$
(3) $u,uv \in M \Rightarrow v \in M$ et : $vu,u \in M \Rightarrow v \in M$.
Nous dirons dans ce cas que M est un sous-monoïde biunitaire.

Soit G_X le groupe libre engendré par X. Observons que si H est un sous-groupe de G_X, le sous-monoïde $H \cap X^*$ de X^* vérifie (3), donc est biunitaire.

2. Automates à groupe, à transitions injectives.

DEFINITION 1. Soit $\mathcal{A} = (Q,q_o,Q_f,\lambda)$ un automate sur X^*. $\mathcal{A}$ est un automate à groupe si pour tout $w \in X^*$ l'application (a priori partielle) $Q \rightarrow Q$, $q \longmapsto (q,w)$ est une bijection de Q.

Remarques.
1. Si Q est fini, on retrouve une définition de G. Thierrin [9].
2. $\mathcal{A}$ est un automate à groupe si et seulement si l'opération de X^* sur Q définie par λ se prolonge en une opération de G_X sur Q.
3. Si $w \neq 1$, l'application $q \longmapsto \lambda(q,w)$ est composée d'applications $q \longmapsto \lambda(q,x)$, $x \in X$; par suite, pour que $\mathcal{A}$ soit un automate à groupe il faut et suffit que pour tout $x \in X$ l'application $q \mapsto \lambda(q,x)$ soit une bijection de Q.

Proche de la notion d'automate à groupe est la notion suivante.

DEFINITION 2. (cf. Thierrin [9]). Un langage est rationnel à groupe (ou reconnaissable à groupe) si son monoïde syntactique est un groupe fini.

Le lien entre ces deux définitions est donné par la

PROPOSITION 1. (Thierrin [9]) Soit L une partie de X^*. Les conditions suivantes sont équivalentes :
(i) L est rationnel à groupe.

(ii) L <u>est reconnaissable par un groupe fini</u>.

(iii) <u>L'automate minimal de</u> L <u>est fini à groupe</u>.

Les rationnels à groupe jouissent des propriétés suivantes.

<u>PROPOSITION 2</u> (Thierrin [9]) <u>La réunion et l'intersection de deux rationnels à groupe est un rationnel à groupe. Le complémentaire d'un rationnel à groupe est rationnel à groupe.</u>

Nous généralisons la notion d'automate à groupe de la manière suivante.

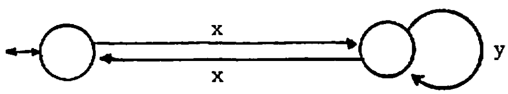
<u>DEFINITION 3</u> Soit $\mathcal{A} = (Q, q_0, Q_f, \lambda)$ un automate sur X^*. $\mathcal{A}$ est un automate à transitions injectives si pour tout $w \in X^*$ l'application partielle $Q \to Q$, $q \longmapsto \lambda(q,w)$ est injective, i.e. : $\forall\, q,q' \in Q$: $\lambda(q,w) = \lambda(q',w) \neq \emptyset$ implique $q = q'$.

<u>Remarques</u>

1. Le produit de deux applications partielles injectives est encore injectif. Par suite, pour que $\mathcal{A}$ soit à transitions injectives, il faut et suffit que pour tout $x \in X$, l'application partielle $q \longmapsto \lambda(q,x)$ soit injective.
2. Soit $\tilde{\mathcal{A}}$ l'automate miroir de $\mathcal{A}$ (cf. [4] p. 18). Alors $\mathcal{A}$ est à transitions injectives si et seulement $\tilde{\mathcal{A}}$ est déterministe.

<u>Exemples.</u>

1. Un automate à groupe est à transitions injectives.
2. L'automate suivant est à transitions injectives (sans être à groupe) : $X = \{x,y\}$



<u>LEMME 1</u> <u>Soit</u> $\mathcal{A} = (Q, q_0, q_0, \lambda)$ <u>un automate à transitions injectives pointé. Si</u> $\mathcal{A}$ <u>est émondé,</u> $\mathcal{A}$ <u>est minimal.</u>

<u>Preuve.</u> Il suffit de montrer que $\mathcal{A}$ vérifie la condition (2) du § 1. Soient $q,q' \in Q$ tels que : $\forall w \in X^*$, $\lambda(q,w) = q_0$ équivaut à $\lambda(q',w) = q_0$. Comme $\mathcal{A}$ est émondé, il existe effectivement un w tel que $\lambda(q,w) = q_0 = \lambda(q',w)$ et comme $\mathcal{A}$ est à transitions injectives $q = q'$.

<u>Remarques.</u>

1. Un automate à transitions injectives pointé reconnaît un sous-monoïde bipréfixe. En effet, on vérifie aisément que $L(\mathcal{A})$ est un

sous-monoïde vérifiant la relation (3) du § 1.

2. Si le monoïde syntactique d'un sous-monoïde bipréfixe est inversif, alors son automate minimal est à transitions injectives. D'où le lien entre le présent travail et les articles [7] de Keenan et Lallement et [8] de Perrot.

L'étude des automates à transitions injectives et des langages qu'ils reconnaissent nécessite la notion de prolongation d'automate : c'est l'objet du § suivant.

3. Prolongation d'automate.

Soient $E \subset F$ deux ensembles et $f : E \longrightarrow E$, $g : F \longrightarrow F$ des applications partielles. Rappelons que g prolonge f, ce que nous notons $f \subset g$ si : $\forall\, x \in E : f(x) \neq \emptyset \implies f(x) = g(x)$.

DEFINITION 4. *Soit* $\mathcal{A} = (Q, q_o, Q_f, \lambda)$ *et* $\mathcal{A}' = (Q', q'_o, Q'_f, \lambda')$. $\mathcal{A}'$ *prolonge* $\mathcal{A}$ *si* $Q = Q'$, $q'_o = q_o$, $Q'_f = Q_f$, $\lambda \subset \lambda'$. *Nous notons ceci* : $\mathcal{A} \subset \mathcal{A}'$

Il est clair que pour que $\mathcal{A}'$ prolonge $\mathcal{A}$, il suffit que la restriction de λ' à $Q \times X$ prolonge celle de λ.
Les résultats suivants sont immédiats.

LEMME 2. *Soient* $\mathcal{A}$ *et* $\mathcal{A}'$ *deux automates tels que* $\mathcal{A} \subset \mathcal{A}'$.
(i) $L(\mathcal{A}) \subset L(\mathcal{A}')$.
(ii) *Si* $\mathcal{A}'$ *est à transitions injectives,* $\mathcal{A}$ *l'est aussi.*
(iii) *Si* $\mathcal{A}''$ *prolonge* $\mathcal{A}'$, *alors* $\mathcal{A}''$ *prolonge* $\mathcal{A}$.

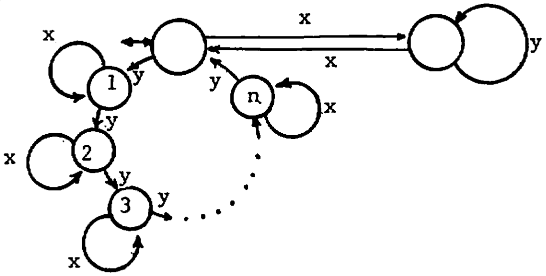
Il suit de (ii) que si $\mathcal{A}'$ est un automate à groupe et si $\mathcal{A} \subset \mathcal{A}'$, $\mathcal{A}$ est à transitions injectives. On montre aisément la réciproque de ceci, à savoir : si $\mathcal{A}$ est à transitions injectives, il existe $\mathcal{A}'$ à groupe tel que $\mathcal{A} \subset \mathcal{A}'$. Nous montrons ici un résultat plus précis lorsque $\mathcal{A}$ est fini.

LEMME 3. *Soit* $\mathcal{A} = (Q, q_o, Q_f, \lambda)$ *un automate fini à transitions injectives. Il existe alors un automate fini à groupe* $\mathcal{A}'$ *prolongeant* $\mathcal{A}$, *de la forme* $\mathcal{A}' = (Q, q_o, Q_f, \lambda')$.

En effet, Q étant fini, toute application partielle injective $Q \longrightarrow Q$ se prolonge en une bijection de Q.
Ces lemmes nous permettent de montrer une propriété remarquable des langages reconnus par les automates finis à transitions injectives.

PROPOSITION 3. Soit $\mathcal{A}$ un automate fini à transitions injectives. $L(\mathcal{A})$ est égal à l'intersection (infinie) des langages reconnus par les automates finis à groupe prolongeant $\mathcal{A}$.

Exemple. Soit $\mathcal{A}$ l'automate de l'exemple 2 du § 3. Alors $L(\mathcal{A}) = \bigcap_{n \geq 0} L(\mathcal{A}_n)$ où $\mathcal{A}_n$ est l'automate :



Preuve. Soit $\mathcal{A} = (Q, q_o, Q_f, \lambda)$. (i) Si $\mathcal{A}'$ est un automate prolongeant $\mathcal{A}$, on a $L(\mathcal{A}) \subset L(\mathcal{A}')$. (LEMME 1 (i)). (ii) Soit $w \notin L(\mathcal{A})$. Nous construisons un automate fini à groupe $\mathcal{A}'$ prolongeant $\mathcal{A}$ tel que $w \notin L(\mathcal{A}')$.

1. Soit $\lambda(q_o, w)$ est défini, mais n'appartient pas à Q_f. Alors, pour tout automate fini à groupe $\mathcal{A}'$ prolongeant $\mathcal{A}$ (et un tel $\mathcal{A}'$ existe lemme 2), on a :

   $\lambda'(q_o, w) = \lambda(q_o, w) \notin Q_f \Rightarrow w \notin L(\mathcal{A}')$.

2. Soit $\lambda(q_o, w)$ n'est pas défini ; w peut alors s'écrire $w = ux_1 \ldots x_n$ $(x_i \in X)$, $\lambda(q_o, u) = q_1 \in Q$ et $\lambda(q_1, x_1)$ n'est pas défini. Soit $p_1, \ldots, p_n$ des états supplémentaires $\notin Q$ et $\mathcal{A}_1 = (Q \cup \{p_1, \ldots, p_n\}, q_o, Q_f, \lambda_1)$ défini par :

. $\lambda_1(q_1, x_1) = p_1$, $\lambda_1(p_1, x_2) = p_2, \ldots, \lambda_1(p_{n-1}, x_n) = p_n$.

. $\forall q \in Q$, $\forall x \in X : q \neq q_1$ ou $x \neq x_1 \Rightarrow \lambda_1(q, x) = \lambda(q, x)$.

$\mathcal{A}_1$ est à transitions injectives et $\lambda_1(q_o, w) = p_n \in Q_f$. On est donc ramené à 1, moyennant le lemme 2 (iii).

II. SUR LE PLONGEMENT DU MONOIDE LIBRE DANS LE GROUPE LIBRE.

Soit X un ensemble fini, X^* le monoïde libre engendré par X et G_X le groupe libre engendré par X. On a une injection canonique $X^* \longrightarrow G_X$. Tout homomorphisme de X^* dans un groupe G se prolonge de manière unique en un homomorphisme $G_X \longrightarrow G$. Cette remarque nous permet d'établir le

LEMME 4. Un langage est rationnel à groupe si et seulement si c'est *l'intersection avec X^* d'une partie reconnaissable de G_X.*

Preuve. Si $L = K \cap X^*$ où K est un reconnaissable de G_X, il existe un monoïde fini H et un homomorphisme $\varphi : G_X \longrightarrow H$ tel que $K = \varphi^{-1}(\varphi(K))$. $\varphi(G_X)$ est un groupe, on peut donc supposer que H est un groupe. Soit ψ la restriction de φ à X^*. On a : $L = \psi^{-1}(\psi(L))$ donc L est rationnel à groupe (prop. 2 (ii)).

Soit L un langage rationnel à groupe. Il existe un groupe fini H et un homomorphisme $\psi : X^* \longrightarrow H$ tel que $L = \psi^{-1}(\psi(L))$. ψ se prolonge en un homomorphisme $\varphi : G_X \longrightarrow H$; soit $K = \varphi^{-1}(\psi(L))$. Alors $K = \varphi^{-1}(\varphi(K))$ donc K est reconnaissable dans G_X et $L = K \cap X^*$.

Remarquons qu'un sous-groupe de G_X est reconnaissable si et seulement s'il est d'index fini ; en effet, tout sous-groupe d'index fini contient un sous-groupe d'index fini distingué (voir par exemple [5] 2.3. p. 128) et il est par suite reconnaissable dans G_X. Les sous-groupes d'index fini sont entièrement définis par leur "partie positive" :

PROPOSITION 4. *Un sous-groupe d'index fini H de G_X est engendré par sa partie positive $H \cap X^*$.*

Preuve. H est reconnaissable : il existe donc un groupe fini G et un homomorphisme surjectif $\varphi : G_X \longrightarrow G$ tel que $H = \varphi^{-1}(\varphi(H))$. Soit $M = H \cap X^*$. $\varphi(X^*)$ est un sous-monoïde de G qui engendre G. G étant fini $\varphi(X^*) = G$. Par suite : $\forall u \in X^*$, $\exists v \in X^*$ tel que $\varphi(uv) \in \varphi(H)$ (resp. $\varphi(vu) \in \varphi(H)$), donc $uv \in M$ (resp. $vu \in M$) ; ce qu'on exprime en disant que M est complet à droite (resp. à gauche). Soit K le sous-groupe de G_X engendré par M ; on a clairement $K \subset H$.

Montrons que : $G_X = KX^*$. En effet, si $g = u_o v_1^{-1} u_1 \ldots v_n^{-1} u_n \in G_X$ $(u_i, v_i \in X^*)$, soit $u'_o \in X^*$ tel que $u_o u'_o \in M$ et $v'_1 \in X^*$ tel que $v'_1 v_1 u'_o \in M$. Alors

$g = (u_o u'_o)(v'_1 v_1 u'_o)^{-1}(v'_1 u_1) v_2^{-1} \ldots u_n$ et l'on conclut par récurrence sur n. Soit $g \in H$; g s'écrit kw, $k \in K$, $w \in X^*$. Alors $k \in H \Rightarrow w \in H \cap X^* = M$, donc $g \in KM = K$ et $K = H$.

Nous sommes maintenant en mesure de caractériser les sous-monoïdes rationnels à groupe de X^*.

Théorème 1. *Il y a bijection entre les sous-groupes d'index fini de G_X et les sous-monoïdes rationnels à groupe de X^*. Elle est donnée par $H \longmapsto H \cap X^*$ et l'application inverse est $M \longmapsto$ le sous-groupe engen-*

dré par M.

Preuve. Si H est un sous-groupe d'index fini de G_X, H est reconnaissable dans G_X, donc $H \cap X^*$ est rationnel à groupe (lemme 3) et c'est clairement un sous-monoïde. De plus $H \cap X^*$ engendre H (prop 4). Si M est un sous-monoïde rationnel à groupe de X^*, $M = \varphi^{-1}(\varphi(M))$ où φ est un homomorphisme surjectif de X^* dans un groupe fini G. $\varphi(M)$ est un sous-groupe de G ; par suite, si ψ désigne le prolongement de φ à G_X, $\psi^{-1}(\varphi(M))$ est un sous-groupe d'index fini de G_X. Il est engendré par $\psi^{-1}(\varphi(M)) \cap X^* = M$ (prop 4), donc le sous-groupe H engendré par M est d'index fini et l'on a $H \cap X^* = M$.

Plus généralement, les sous-monoïdes de X^* qui sont intersection avec X^* d'un sous-groupe de G_X sont caractérisés par leur automate minimal.

PROPOSITION 5. *Soit M un sous-monoïde de X^*. Les conditions suivantes sont équivalentes :*

(i) M est l'intersection avec X^* d'un sous-groupe de G_X.

(ii) L'automate minimal de M est pointé et à transitions injectives.

Remarque. On sait (voir [9] chap II § 4 cor 4.3) que les sous-monoïdes libres sont exactement les stabilisateurs d'un point dans une représentation de X^* par "relations non ambiguës". De même, les sous-monoïdes unitaires sont ceux qui stabilisent un point dans une représentation par applications partielles (voir I.1). Le résultat ci-dessus exprime qu'un sous-monoïde est intersection avec X^* d'un sous-groupe si et seulement s'il stabilise un point dans une représentation de X^* par applications partielles injectives ; si de plus, il est rationnel, cette représentation peut être choisie finie, comme nous le verrons. Nous avons besoin du

LEMME 5. *Soit H un sous-groupe de G_X. Alors l'automate minimal de $H \cap X^*$ est pointé et à transitions injectives.*

Preuve. Soit G_X/H l'ensemble des classes à droite modulo H et p : $G_X \longrightarrow G_X/H$ la surjection canonique. G_X opère sur G_X/H à droite : $p(u).v = p(uv)$. Soit $\mathcal{A}_1 = (G_X/H, p(1), p(1), \lambda)$ où λ est défini par l'opération de G_X sur G_X/H : $\forall w \in X^*$, $\forall u \in G_X$, $\lambda(p(u),w) = p(uw)$. On a : $\lambda(p(u),w) = \lambda(p(u'), w) \Rightarrow p(uw) = p(u'w) \Rightarrow$ $p(u) = p(uw).w^{-1} = p(u'w).w^{-1} = p(u')$. $\mathcal{A}_1$ est donc à transitions injectives. De plus : $w \in L(\mathcal{A}_1) \Leftrightarrow \lambda(p(1),w) = p(1) \Leftrightarrow p(w) = p(1) \Leftrightarrow$ $w \in H \cap X^* = M$. L'automate obtenu en émondant $\mathcal{A}_1$ est minimal (lemme 1) et reconnaît M.

Preuve de la proposition 5. Il reste à montrer que (ii) implique (i). Soit $\mathcal{A} = (Q,q_o,q_o,\lambda)$ l'automate minimal de M. Nous allons définir un nouvel automate $\mathcal{A}' = (Q',q_o,q_o,\lambda')$ prolongeant $\mathcal{A}$ tel que $L(\mathcal{A}') = L(\mathcal{A})$ et que $\mathcal{A}'$ soit un automate à groupe : ainsi l'opération de X^* sur Q' se prolonge en une opération de G_X sur Q', notée $(q,g) \mapsto q.g$ et l'on a : $M = L(\mathcal{A}') = \{w \in X^* | q_o.w = q_o\} = H \cap X^*$ où H est le sous-groupe de G_X qui stabilise q_o. Soit $x \in X$.

1. Soit $q \in Q$ tel que $\lambda(q,x) = \emptyset$. Nous ajoutons à Q les états $\{a_{x,q,n}\}_{n \geq 1}$ et définissons λ' par : $\lambda'(q,x) = a_{x,q,1}$; $\forall\, n \geq 1$, $\lambda'(a_{x,q,n},x) = a_{x,q,n+1}$ et $\forall y \in X\setminus x$, $\lambda'(a_{x,q,n},y) = a_{x,q,n}$.
2. Soit $q \in Q$ tel que $q \notin \lambda(Q,x)$. Nous ajoutons à Q les états $\{b_{x,q,n}\}_{n \geq 1}$ et définissons λ' par : $\lambda'(b_{x,q,1},x) = q$; $\forall n \geq 1$, $\lambda'(b_{x,q,n+1},x) = b_{x,q,n}$ et $\forall y \in X\setminus x$, $\lambda'(b_{x,q,n},y) = b_{x,q,n}$.

L'automate ainsi défini vérifie : pour tout $x, q \mapsto \lambda'(q,x)$ est une bijection de Q' et l'on a $L(\mathcal{A}') = L(\mathcal{A})$.

III. UNE TOPOLOGIE DU MONOIDE LIBRE.

X est un ensemble fini, G_X le groupe libre engendré par X, X^* le monoïde libre engendré par X : X^* est un sous-monoïde de G_X. M. Hall [6] a considéré sur G_X la topologie $\mathcal{T}_G$ pour laquelle les sous-groupes d'index fini de G_X forment un système fondamental de voisinages de 1. G_X devient ainsi un groupe topologique non discret [6] (voir aussi [3] chap. III § 1 n° 2), cette topologie est séparée puisque G_X est résiduellement fini (théorème d'Iwasawa voir [6] 2.A. p. 128) i.e. : $\forall\, g \in G_X, g \neq 1$, il existe un sous-groupe H d'index fini de G_X tel que $g \notin H$. Comme tout sous-groupe d'index fini contient un sous-groupe distingué d'index fini, on a :

LEMME 6. *$\mathcal{T}_G$ est caractérisé des deux manières équivalentes suivantes*
(i) Les parties reconnaissables de G_X forment une base d'ouverts (i.e. tout ouvert de $\mathcal{T}_G$ est réunion (infinie) de parties reconnaissables).
(ii) $\mathcal{T}_G$ est la topologie de G_X la moins fine rendant continu tout homomorphisme de G_X dans un groupe fini discret.

(pour (ii) voir [3] chap. 1 § 2 n° 3 prop. 4)
Observons que, puisque le complémentaire d'une partie reconnaissable l'est aussi, une telle partie est à la fois ouverte et fermée.

$\mathcal{T}_G$ peut aussi être définie par une distance ultramétrique invariante par translation comme l'a montré M. Hall.
Nous nous intéressons dans la suite à la topologie de X^* obtenue par restriction (en vertu de l'injection $X^* \to G_X$).

PROPOSITION 6. Soit $\mathcal{T}$ une topologie de X^*. Les conditions suivantes sont équivalentes :
(i) $\mathcal{T}$ est la restriction à X^* de $\mathcal{T}_G$.
(ii) Les parties rationnelles à groupe de X^* forment une base d'ouverts de $\mathcal{T}$.
(iii) $\mathcal{T}$ est la topologie de X^* la moins fine rendant continu tout homomorphisme de X^* dans un groupe fini discret.

Preuve D'après le lemme 6, l'ensemble des parties reconnaissables de G_X forme une base d'ouverts de $\mathcal{T}_G$. Par suite [3] (chap. I § 1 n° 1) l'ensemble $\{ R \cap X^* \mid R \text{ reconnaissable dans } G_X \}$ forme une base d'ouverts de la topologie induite par $\mathcal{T}_G$ sur X^*. Or cet ensemble n'est autre que l'ensemble des parties reconnaissables à groupe de X^*(lemme 4). D'où l'équivalence de (i) et de (ii), puisque deux topologies qui ont même base d'ouverts sont égales. L'équivalence de (ii) et (iii) résulte des théorèmes de topologie [3](chap. I § 2 n° 3).

Dans la suite, nous noterons $\mathcal{T}$ la topologie de X^*définie par les conditions de la proposition 6. X^* devient ainsi un monoïde topologique (i.e; l'application $X^* \times X^* \to X^*$, $(w,w') \mapsto ww'$ est continue) séparé puisque G_X est un groupe topologique séparé. Observons aussi que $\mathcal{T}$ n'est pas la topologie discrète.

COROLLAIRE 1. Toute partie rationnelle à groupe de X^* est ouverte et fermée.
En effet, le complémentaire d'un rationnel à groupe est rationnel à groupe (prop 2).
COROLLAIRE 2. Toute partie de X^* qui est reconnue par un automate fini à transitions injectives est fermée.
Celà résulte du cor. 1 et de la prop. 3.

Nous donnons maintenant quelques résultats techniques simples qui nous serviront par la suite. Rappelons d'abord que dans un monoïde topologique, la fermeture (i.e. l'adhérence) d'un sous-monoïde est encore un sous-monoïde.

LEMME 7. Soit $u \in G_X$. Alors $\lim_{n \to \infty} u^{n!} = 1$.

Preuve. Soit V un voisinage de 1 dans G_X ; V contient un sous-groupe distingué d'index fini H. Soit $n \geqslant \mathrm{Card}(G/H)$; alors Card (G/H) divise n! donc $u^{n!} \in H \subset V$.

PROPOSITION 7.

(i) Tout sous-monoïde fermé de G_X est un sous-groupe.

(ii) X^* est dense dans G_X.

Remarque : Un sous-monoïde fermé de G_X" signifie un sous-monoïde de G_X fermé pour $\mathcal{C}_G$; de même nous dirons "sous-monoïde fermé de X^*" au lieu de sous-monoïde de X^* fermé pour $\mathcal{C}$.

Preuve.

(i) Soit M un sous-monoïde fermé de G_X et $u \in M$. Alors : $\forall n \in N$, $u^{n!-1} \in M$. D'après le lemme 7 : $u^{-1} = \lim u^{n!-1}$. Donc $u^{-1} \in M$.

(ii) La fermeture de X^* dans G_X est un sous-monoïde fermé de G_X. C'est donc un sous-groupe de G_X d'après (i), contenant X, donc égal à G_X.

IV. SOUS MONOIDES FERMES DU MONOIDE LIBRE.

Nous commençons par quelques exemples de sous-monoïdes fermés.

Exemples. 1. Les sous-monoïdes rationnels à groupe sont fermés (cor.1 à la prop. 6).

2. Si Y est une partie de X, le sous-monoïde Y^* engendré par Y est fermé. En effet, soit $\varphi: X^* \to (X \setminus Y)^*$ l'homomorphisme projection i.e: $\forall x \in Y$, $\varphi(x) = 1$ et $\forall x \in X\setminus Y$, $\varphi(x) = x$. Alors $Y^* = \varphi^{-1}(1)$. Or, φ est continue (d'après prop. 6 (iii) et [3] chap. I § 2 prop. 4) et $\{1\}$ est fermé dans $(X\setminus Y)^*$, puisque $(X\setminus Y)^*$ est séparé. Donc Y^* est fermé dans X^*.

3. Soit $\bar{X}$ une copie distincte de X et $x \mapsto \bar{x}$ une bijection $X \to \bar{X}$. Soit $\varphi : (X \cup \bar{X})^* \to G_X$ l'homomorphisme tel que : $\varphi(x) = x$ et $\varphi(\bar{x}) = x^{-1}$. Alors $\varphi^{-1}(1)$ est le langage de Dyck sur X, bien connu en théorie des langages algébriques. Comme pour l'exemple 2, $\varphi^{-1}(1)$est fermé dans $(X \cup \bar{X})^*$.

4. Lorsque Card(X) = 1, X^* est isomorphe à N et G_X à Z. $\mathcal{C}$ (resp.$\mathcal{C}_G$) n'est autre que la topologie borne supérieure de toutes les topologies p-adiques. Tous les sous-groupes non nuls de Z sont ouverts et fermés ; les sous-monoïdes fermés de N sont les a N (cf. lemme 6 par exemple) et si $a \neq 0$, a N est ouvert ; par suite, tout sous-monoïde

non nul de N est aussi ouvert.

LEMME 8. *Soit M un sous-monoïde fermé de X^*. Alors la fermeture H de M dans G_X est un sous-groupe fermé de G_X et $M = H \cap X^*$.*

Preuve. La fermeture H de M dans G_X est un sous-monoïde fermé de G_X, donc un sous-groupe (prop. 7 (i)). De plus, comme $\mathcal{C}$ est la restriction de $\mathcal{C}_G$ à X^*, la fermeture de M dans X^* (c'est-à-dire M) est égale à l'intersection de X avec la fermeture de M dans G_X [3] (chap. I § 3 prop. 1).

PROPOSITION 8. *Soit M une partie de X^*. Les conditions suivantes sont équivalentes :*

(i) M est un sous-monoïde fermé de X^*

(ii) M est intersection avec X^* d'un sous-groupe fermé de G_X.

(iii) M est intersection (en général infinie) de sous-monoïdes rationnels à groupe.

Preuve. (i) $\Rightarrow$ (ii) résulte du lemme 8.

(ii) $\Rightarrow$ (iii) : Soit $M = H \cap X^*$ où H est un sous-groupe fermé de G_X. Soit $(G_i, \varphi_i)_{i \in I}$ la famille des couples de groupes finis G_i et d'homomorphismes $\varphi_i : G_X \rightarrow G_i$. D'après le lemme 6, tout fermé de G_X est intersection de parties reconnaissables de G_X, donc de la forme $\bigcap_{i \in I} \varphi_i^{-1}(R_i)$ où $R_i \subset G_i$. Donc $H = \cap \varphi_i^{-1}(R_i)$. Par suite, $H = \cap \varphi_i^{-1}(\varphi_i(H))$ donc H est intersection de sous-groupes d'index fini, donc M est intersections de sous-monoïdes rationnels à groupe (th. 1).

(iii) $\Rightarrow$ (i) résulte du cor. 1 à la prop. 6.

Remarque : comme X est fini, l'intersection (iii) peut être choisie au plus dénombrable.

Corollaire. Un sous-monoïde fermé de X^* est biunitaire et en particulier libre.

Preuve. Un tel sous-monoïde est de la forme $H \cap X^*$ où H est un sous-groupe de G_X (cf. I § 1).

Remarques. 1. Si H est un sous-groupe de G_X, $H \cap X^*$ n'est pas nécessairement fermé dans X^* comme le montre l'exemple suivant (inspiré de M. Hall [6] p. 131) : soit H le sous-groupe engendré par $B = \{ x^n y x^n | n \geq 1 \}$. B en est une base, car dans tout produit de la forme $g_1 \ldots g_p$ où $\forall i$ g_i ou $g_i^{-1} \in B$ et $g_i \neq g_{i+1}$, les simplifications entre g_i et g_{i+1} n'atteignent ni dans g_i, ni dans g_{i+1} la lettre centrale y ou y^{-1}. Le même argument montre que $H \cap X^* = B^*$. Or, $\lim x^{n!} y x^{n!} = y$ (lemme 7) et $y \notin H \cap X^*$.

2. La réciproque du corollaire n'est pas vraie : en effet, soit $C = \{ x^2, xyx \}$. C est un code bipréfixe donc $M = C^*$ est un sous-monoïde biunitaire, Si M était fermé, M serait de la forme $H \cap X^*$ où H est un sous-groupe de G_X (prop. 8) et $xy^2x = (xyx)\ (x^2)^{-1}(xyx) \in H \cap X^* = M$, ce qui n'est pas.

Le théorème qui suit est un de nos résultats principaux. Il caractérise les sous-monoïdes rationnels fermés de X^*.

<u>Théorème 2</u>. <u>Soit</u> M <u>un sous-monoïde rationnel de</u> X^*. <u>Les trois conditions suivantes sont équivalentes</u> :

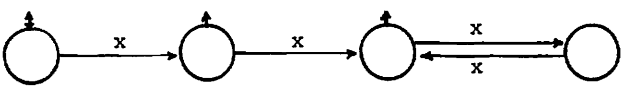
(i) M <u>est fermé dans</u> X^*.

(ii) M <u>est intersection avec</u> X^* <u>d'un sous-groupe de</u> G_X.

(iii) <u>L'automate minimal de</u> M <u>est à transitions injectives</u>.

<u>Preuve</u>. (i) $\Longrightarrow$ (ii) résulte de la prop 8. (ii) $\Longrightarrow$ (iii) résulte de la prop. 5. (iii) $\Longrightarrow$ (i) résulte du cor. 2 à la prop. 6. puisque M est rationnel donc son automate minimal est fini.

<u>Remarque</u>. D'après le cor. 2 à la prop. 6, toute partie rationnelle de X^* dont l'automate minimal est à transitions injectives est fermée dans X^*. La réciproque n'est pas vraie : soit $X = \{x\}$ et $\mathcal{A}$ l'automate suivant :



$L(\mathcal{A}) = (x^2)^* \cup \{x\}$ est fermé, $\mathcal{A}$ est minimal mais n'est pas à transitions injectives.

Du théorème 2 se déduit un résultat de théorie des automates que nous formulons indépendamment.

<u>PROPOSITION 9</u>. <u>Soit</u> $\mathcal{A}$ <u>un automate fini à transitions injectives. Les deux conditions suivantes sont équivalentes</u>.

(i) $\mathcal{A}$ <u>est pointé et émondé</u>.

(ii) $L(\mathcal{A})$ <u>est un sous-monoïde et</u> $\mathcal{A}$ <u>est minimal</u>.

<u>Preuve</u>. (i) $\Longrightarrow$ (ii) : comme $\mathcal{A}$ est pointé, $L(\mathcal{A})$ est un sous-monoïde ; $\mathcal{A}$ est minimal d'après le lemme 1. (ii) $\Rightarrow$ (i) : $L(\mathcal{A})$ est un sous-mo-

noïde fermé de X^* (th. 2) donc s'écrit $H \cap X^*$ où H est un sous-groupe de G_X (prop. 8). Par suite $\mathcal{A}$ est pointé (prop. 5) et émondé puisque $\mathcal{A}$ est minimal.

PROPOSITION 10. Soit M un sous-monoïde rationnel fermé de X^*. Alors sa base est également fermée dans X^*.

(rappelons que M est libre : cor. à la prop. 8).

Preuve. Soit $\mathcal{A} = (Q,q_0,q_0,\lambda)$ l'automate minimal de M et B la base de M. On définit comme suit un automate $\mathcal{A}'$ reconnaissant B [4] (chap IV § 5) : soit $p \in Q$ et $\mathcal{A}' = (Q \cup p,\ q_0,\ p,\ \lambda')$ où λ' est défini par : $\forall\, q \in Q,\ \forall\, x \in X$

. $\lambda(q,x) = q_0 \Rightarrow \lambda'(q,x) = p$.

. $\lambda(q,x) \neq q_0 \Rightarrow \lambda'(q,x) = \lambda(q,x)$.

. $\lambda(p,x) = \emptyset$.

Comme $\mathcal{A}$ est fini à transitions injectives, $\mathcal{A}'$ l'est aussi. Donc $B = L(\mathcal{A}')$ est fermé (cor. à la prop. 6).

Remarque. Ce résultat n'est plus vrai pour un sous-monoïde fermé quelconque. Soit $\varphi : (X \cup \bar{X})^* \to G_X$, $\varphi(x) = x$, $\varphi(\bar{x}) = x^{-1}$ (voir l'exemple 3). $\varphi^{-1}(1)$ est un sous-monoïde fermé de $(X \cup \bar{X})^*$, donc libre. Sa base B est appelé le langage de Dyck premier : c'est l'ensemble des $w \in \varphi^{-1}(1)$ tels que $w = uv$, $u,v \in \varphi^{-1}(1) \Rightarrow u$ ou $v = 1$

Soit $w \in \varphi^{-1}(1)$ et n tel que $n! > |w|$. ($|w|$ est la longueur de w). On vérifie sans peine qu'alors $x^{n!}w\bar{x}^{n!} \in B$. Or, d'après le lemme 5, $\lim x^{n!}w\bar{x}^{n!} = w$. Par suite, le langage de Dyck premier est dense dans le langage de Dyck et ne peut être fermé.

Il est bien connu qu'un sous-groupe ouvert d'un groupe topologique est aussi fermé. Dans le cas de G_X, les sous-groupes ouverts sont exactement les sous-groupes d'index fini. Nous obtenons ici un résultat analogue pour le monoïde libre.

PROPOSITION 11. Il y a identité entre les sous-monoïdes rationnels à groupe de X^* et les sous-monoïdes ouverts et fermés de X^*

Remarque. Comme va le montrer la preuve, la condition "ouverts" peut être remplacée par celle, plus faible, "contenant 1 en leur intérieur" donc aussi par la condition "d'intérieur non vide".

Preuve. Si M est rationnel à groupe, M est ouvert et fermé (cor. 1 à la prop. 6). Si M est un sous-monoïde fermé contenant 1 en son inté-

rieur, il contient un rationnel à groupe contenant 1, donc un sous-monoïde rationnel à groupe M_1. Par suite, la fermeture H de M dans G_X, qui est un sous-groupe, contient le sous-groupe engendré par M_1, lequel est d'index fini (th. 1). Donc H est aussi d'index fini et l'on a $M = H \cap X^*$, donc M est rationnel à groupe (th. 1).
Si M est un sous-monoïde fermé de X^*, sa fermeture dans G_X est un sous-groupe de G_X. Ce sous-groupe contient le sous-groupe engendré par M. Ces deux sous-groupes coïncident-ils ? Le résultat suivant apporte un élément de réponse.

PROPOSITION 12. Soit M un sous-monoïde rationnel fermé de X^* et H le sous-groupe qu'il engendre dans G_X. H est égal à la fermeture de M dans G_X.

Preuve. Soit K l'adhérence de M dans G_X. D'après le lemme 8, $H \subset K$. Réciproquement, M est rationnel dans X^*, donc H est rationel dans G_X. Par suite H est un sous-groupe de type fini [1] (lemme 3.1.), donc fermé [5] (th. 5.1.), ce qui implique $K \subset H$.

Remarques. 1. Dans [12], nous avons montré ce résultat d'une autre manière : nous prouvons là que si $\mathcal{A}$ désigne l'automate minimal de M, alors H est égal à l'intersection de tous les $GL(\mathcal{A}')$ lorsque $\mathcal{A}'$ parcourt la famille des automates finis à groupe prolongeant $\mathcal{A}$ (GN désigne le sous-groupe engendré par N). Or $L(\mathcal{A}')$ est un sous-monoïde rationnel à groupe, donc $GL(\mathcal{A}')$ est un sous-groupe d'index fini de G_X (th. 1), donc fermé.
2. Si M est un sous-monoïde fermé de X^* qui vérifie : $\forall u, \exists v, v' \in X^*$ tels que $uv, v'u \in M$ (i.e. M est complet à gauche et à droite) alors le sous-groupe qu'il engendre est fermé : la preuve est calquée sur celle de la proposition 4.
3. L'auteur ne sait pas répondre à la question suivante : si M est un sous-monoïde fermé quelconque de X^*, le sous-groupe de G_X qu'il engendre est-il fermé ?

L'auteur tient à remercier J.F. Perrot pour son aide pendant la rédaction de cet article.

REFERENCES.

1. Anisimov, A.V. et F.D., Seiffert, Zur algebraischen Charakteristik der durch kontext-freie Sprachen definierten Gruppen, Elektronische Informationsverarbeitung und Kybernetik 11 (1975) 695-702.

2. Berstel, J., Factorisations de fractions rationnelles et de suites récurrentes, Acta Arithmetica XXX (1976) 5-17.

3. Bourbaki, N., Topologie générale, Hermann Paris (1960).

4. Eilenberg, S., Automata, languages and machines A, Acad. Press, New York (1974).

5. Hall, M. Jr, Coset representations in free groups, Trans. Amer. Math. Soc. 67 (1949) 421-432.

6. Hall, M. Jr, A topology for free groups and related groups, Ann. Math. 52 (1950) 127-139.

7. Keenan, M. et G. Lallement, On certain codes admitting inverse semigroups as syntactic monoids, Semigroup Forum 8 (1974) 312-331.

8. Perrot, J.F., article en préparation.

9. Perrin, D., Codes et combinatoire du monoïde libre, Cours de DEA, Université Paris 7, Département de Mathématiques (1976-77).

10. Thierrin, G., Permutation automata, Math. System Theory 2 (1968) 83.

11. Rauzy, G., Ensembles arithmétiquement denses ; C.R. Acad. Sci. Paris Sér. A 265 (1967) 37-38.

12. Reutenauer, C., Propriétés arithmétiques et topologiques de séries rationnelles, Thèse 3ème cycle. Paris (1977).

13. Schützenberger, M.P., Sur les relations rationnelles entre monoïdes libres, Théor. Comput. Sci. 3 (1976), 243-259.

Institut de Programmation
et Laboratoire d'Informatique Théorique
Université Pierre et Marie Curie
Paris

Received June 15, 1978 and in final form November 1, 1978.