Maurice Nivat

Sur le noyau d'un homomorphisme du monoïde libre dans un groupe libre

Séminaire Schützenberger, tome 1 (1969-1970), exp. n^{o} 4, p. 1-6
<http://www.numdam.org/item?id=SMS_1969-1970__1__A4_0>

Séminaire SCHÜTZENBERGER-LENTIN-NIVAT
(Problèmes mathématiques
de la théorie des automates)
Année 1969/70, n° 4, 6 p.

SUR LE NOYAU D'UN HOMOMORPHISME DU MONOÏDE LIBRE DANS UN GROUPE LIBRE

par Maurice NIVAT

<u>Introduction</u>. - Dans [2], nous avons considéré les langages de la forme $\varphi^{-1}(1)$ où φ est un homomorphisme d'un monoïde libre dans un groupe libre. Nous démontrons en particulier qu'un tel langage est aussi la classe d'équivalence de l'élément neutre modulo une congruence finiment engendrée (si le monoïde libre est lui-même finiment engendré). Il s'agit même d'une congruence quasi-parfaite au sens de [3] qui jouit de propriétés de décidabilité remarquables.

Nous avons recherché des conditions nécessaires et suffisantes pour que, réciproquement, la classe de l'élément neutre modulo une congruence sur un monoïde libre soit le noyau d'un homomorphisme de ce monoïde dans un groupe libre. Une caractérisation, directement issue d'un théorème de R. C. LYNDON [1], fait l'objet de cet exposé.

<u>Définitions</u>. - Soit θ une congruence sur le monoïde libre finiment engendré X^*, et soit A un ensemble fini de mots de X^* dont nous supposerons que

$$X^* = \bigcup_{f \in A^*} [f]_\theta$$

($[f]_\theta$ désigne la classe de f mod θ).

Posons, pour tout $f \in X^*$:

$$\mu f = \inf \{k \in \mathbb{N} \mid A^k \cap [f]_\theta \neq \emptyset\} .$$

L'application μ de X^* dans $\mathbb{N}$ ainsi définie jouit des propriétés suivantes :

$$\mu f = 0 \iff f \in [1]_\theta ,$$
$$\mu fg \leqslant \mu f + \mu g \quad \text{pour tout } f , g \in X^* .$$

Nous appellerons μ la longueur sur X^* associée à θ par A. Nous dirons que cette longueur est <u>archimédienne</u> si, et seulement si,

$$\forall f \in X^* , \quad \mu ff \leqslant \mu f \Rightarrow \mu f = 0 .$$

Nous dirons que cette longueur est <u>réductive</u> si, et seulement si,

$$\forall f , g , h , \ell \in X^* , \quad \forall m \in \mathbb{N} ,$$

$$\mu f + \mu g - \mu fg \geqslant m$$
$$\mu f + \mu h - \mu fh \geqslant m$$
$$\mu \ell + \mu g - \mu \ell g \geqslant m$$
$$\Rightarrow \mu \ell + \mu h - \mu \ell h \geqslant m \ .$$

Nous démontrerons les théorèmes suivants :

THÉORÈME 1. - <u>Soit</u> θ <u>une congruence sur</u> X^* ; <u>s'il existe</u> $A \subset X^*$ <u>telle que la longueur associée</u> à θ <u>par</u> A <u>soit archimédienne et réductive, il existe un groupe libre</u> Γ <u>et un homomorphisme</u> φ <u>de</u> X^* <u>dans</u> Γ <u>tel que</u>

$$[1]_\theta = \varphi^{-1}(1) \ .$$

THÉORÈME 2. - <u>Soit</u> φ <u>un homomorphisme de</u> X^* <u>dans un groupe libre. Il existe une congruence</u> θ <u>(finiment engendrée), et un ensemble fini</u> $A \subset X^*$ tels que

$$[1]_\theta = \varphi^{-1}(1) \ ,$$

<u>et la longueur associée à</u> θ <u>par</u> A <u>est archimédienne et réductive</u>.

Pour démontrer le théorème 1, nous commencerons par établir le lemme suivant :

LEMME 1. - <u>Soit</u> μ <u>la longueur associée à</u> θ <u>par</u> A . <u>Si</u> μ <u>est archimédienne, il existe un groupe</u> G <u>et un homomorphisme</u> φ <u>de</u> X^* <u>dans</u> G <u>tel que</u>

$$[1]_\theta = \varphi^{-1}(1) \ .$$

<u>Démonstration</u>. - On remarque que

$$\forall\ f\ ,\ g \in X^*\ ,\quad fg \in [1]_\theta \Rightarrow gf \in [1]_\theta$$

En effet, $\mu(gf\ gf) = \mu(gf)$, puisque $gf\ gf \ \theta\ gf$. D'où μ étant archimédienne,

$$\mu(gf) = 0 \quad \text{qui entraîne} \quad gf \in [1]_\theta \ .$$

Soit alors $M = \{f \in X^* \mid X^* f X^* \cap [1]_\theta \neq \emptyset\}$.

M est évidemment saturé pour θ .

M est un sous-monoïde de X^* : en effet, soient f , $g \in M$. Il existe u , v , u' , v' tels que

$$ufv \in [1]_\theta \quad \text{et} \quad u'gv' \in [1]_\theta \ .$$

On en déduit que $vuf \in [1]_\theta$ et $gv'u' \in [1]_\theta$, d'où $vufgv'u' \in [1]_\theta$,

$$X^* fg X^* \cap [1]_\theta \neq \emptyset \ .$$

De fait, $M = X'^*$, où $X' = X \cap M$, tout facteur d'un mot de M étant dans M .

M/θ est un groupe. Notons $\hat{\theta}$ l'homomorphisme canonique de X^* sur X^*/θ. Si $f \in M$, il existe u, v tels que $ufv \in [1]_\theta$, d'où encore $vuf \in [1]_\theta$, qui s'écrit

$$\hat{\theta}(vu)\hat{\theta}f = 1 .$$

Munissons-nous d'un groupe cyclique infini Γ_ω, de générateur ω. Pour tout mot $f \in X^*$ se factorisant (de manière unique) en

$$f = f_1\, x_{i_1}\, f_2\, x_{i_2} \dots f_k\, x_{i_k}\, f_{k+1} ,$$

où $f_1, \dots, f_{k+1} \in X'^*$ et $x_{i_1}, \dots, x_{i_k} \in X \setminus X' = X''$, posons

$$\varphi f = \hat{\theta}f_1\, \omega\, \hat{\theta}f_2\, \omega \dots \omega\, \hat{\theta}f_k\, \omega\hat{\theta}f_{k+1} .$$

On vérifie immédiatement que φ est un homomorphisme de X^* dans le produit libre $(M/\theta) \star \Gamma_\omega$, et que l'on a

$$[1]_\theta = \varphi^{-1}$$

Q. E. D.

La suite de la démonstration du théorème 1 utilise de façon cruciale le théorème suivant de LYNDON [1].

Le groupe G est un groupe libre si, et seulement si, il existe une application λ de G dans $\underset{\sim}{N}$ satisfaisant

(A_1) $\lambda g = 0 \iff g = 1$

(A_2) $\lambda gg' \leqslant \lambda g + \lambda g'$

(A_3) $\lambda g = \lambda g^{-1}$

(A_4) $\lambda gg < \lambda g \Rightarrow g = 1$

(A_5) $\begin{matrix} \lambda g + \lambda g' - \lambda gg'^{-1} \geqslant m \\ \lambda g + \lambda g'' - \lambda gg''^{-1} \geqslant m \end{matrix} \Longrightarrow \lambda g' + \lambda g'' - \lambda g' g''^{-1} \geqslant m .$

Notre démonstration va consister en la vérification que l'application de M/θ dans $\underset{\sim}{N}$, définie par $\mu(\hat{\theta}f) = \mu f$, satisfait (A_1)-(A_5), si μ associée à θ par A est archimédienne et réductive.

(A_1), (A_2) et (A_4) sont immédiates.

Pour démontrer (A_3), nous faisons une récurrence sur μf, $f \in M$. Supposons d'abord $\mu f = 1$, et considérons f' tel que $ff' \,\theta\, 1$.

On ne peut avoir $\mu f' = 0$, donc, si $\mu f' \neq \mu f$, on a $\mu f' \geqslant 2$. On peut alors prendre $f' = f'_1 f'_2$ avec

$$f'_1 \in A^{k_1} , \quad f'_2 \in A^{k_2} , \quad \text{et} \quad \mu f' = k_1 + k_2 , \quad k_1 , k_2 \neq 0 .$$

La longueur μ étant réductive, nous avons

$$\mu f = \mu f f_1' + \mu f_2' f .$$

Si ce n'était pas le cas, nous aurions en effet

$$\begin{aligned} &\mu f f_1' + \mu f_2' f - \mu f > 0 \\ &\mu f f_1' + \mu f_2' - \mu f f_1' f_2' > 0 \\ &\mu f_1' + \mu f_2' f - \mu f_1' f_2' f > 0 , \end{aligned}$$

donc $\mu f_1' + \mu f_2' - \mu f_1' f_2' > 0$, ce qui n'est pas le cas. Mais alors comme $\mu f f_1'$ et $\mu f_2' f$ ne sont pas nuls, $\mu f \geqslant 2$ contrairement à l'hypothèse.

On a bien $\mu f' = 1$, si $\mu f = 1$ et $f f' \theta 1$. Soit alors f , $\mu f \geqslant 2$. On peut écrire $f = f_1 f_2$ avec

$$\mu f_1 + \mu f_2 = \mu f , \quad \mu f_1 , \mu f_2 \neq 0 .$$

Introduisons f_1' et f_2' tels que $f_1 f_1' \theta 1$, $f_2 f_2' \theta 1$, et f' tel que $f f' \theta 1$. Nous pouvons supposer par récurrence

$$\mu f_1' = \mu f_1 , \quad \mu f_2' = \mu f_2 .$$

Or nous avons $\mu(f_2' f_1' f_1) + \mu(f_2 f_2' f_1') - \mu(f_2' f_1' f_1 f_2 f_2' f_1') = 0$, car si cette quantité était strictement positive, de

$\mu(f_2' f_1' f_1) + \mu(f_2) - \mu(f_2' f_1' f_1 f_2) > 0$ et $\mu(f_1) + \mu(f_2 f_2' f_1') - \mu(f_1 f_2 f_2' f_1') > 0$,

on déduirait $\mu(f_1) + \mu(f_2) - \mu(f_1 f_2) > 0$,ce qui n'est pas.

Ainsi $\mu(f_2') + \mu(f_1') = \mu(f_2' f_1')$, d'où

$$\mu(f') = \mu(f_2' f_1') = \mu(f_1) + \mu(f_2) = \mu(f) .$$

La vérification de (A_5) est immédiate.

Considérons $f , g , h \in M$, et f' , g' , h' tels que

$$f f' \theta 1 , \quad g g' \theta 1 , \quad h h' \theta 1 .$$

Supposons $\qquad \mu f + \mu g - \mu f g' \geqslant m$ et $\mu f + \mu h - \mu f h' \geqslant m$.

Nous avons aussi

$$\mu g + \mu g' - \mu g g' = 2\mu g , \quad \mu h + \mu h' - \mu h h' = 2\mu h$$

d'où, μ étant réductive, on déduit

$$\mu g + \mu h' - \mu g h' \geqslant \min (2\mu g , m) \quad \text{et} \quad \mu h + \mu g' - \mu h g' \geqslant \min (2\mu h , m) .$$

Les deux premiers membres étant identiques, il vient

$$\mu g + \mu h - \mu g h' \geqslant \min (2\mu g , 2\mu h , m) .$$

Mais $\mu f \leqslant \mu f g' + \mu g$ puisque $f \theta f g' g$, d'où $m \leqslant 2\mu g$. De la même façon, $m \leqslant 2\mu h$

$$\min(2\mu g\ ,\ 2\mu h\ ,\ m) = m \quad \text{et} \quad \mu g + \mu h - \mu g h' \geqslant m\ .$$

En vertu du théorème de Lyndon, M/θ est alors un groupe libre. Le produit libre $(M/\theta) \star \Gamma_\omega$ est encore libre, et le théorème 1 est établi.

<u>Démonstration du théorème 2</u>. – Considérons l'homomorphisme φ de X^* dans Γ, où Γ est un groupe libre. L'ensemble $M = \{f \in X^* \mid X^*fX^* \cap \varphi^{-1}(1) \neq \emptyset\}$ est un sous-monoïde de X^* de la forme

$$M = X'^*,\ \ X' \subset X\ .$$

Il est immédiat que $\varphi(M)$ est un sous-groupe Γ' de Γ, et Γ' est libre (comme tout sous-groupe d'un groupe libre). Si Γ_ω est un groupe cyclique infini à un générateur ω, définissons Ψ, homomorphisme de X^* dans le produit libre $\Gamma' \star \Gamma_\omega$ par

$$\Psi f = \varphi f \quad \text{si} \quad f \in X'^*\ ,$$

$$\Psi f = \omega^{|f|} \ \text{si} \quad f \in (X \setminus X')\ .$$

On a la propriété $\qquad \varphi^{-1}(1) = \Psi^{-1}(1)\ .$

Considérons un système de générateurs libres $\{\gamma_1\ , \ldots\ , \gamma_p\}$ de Γ'. L'homomorphisme φ étant une surjection de M sur Γ', il existe des mots $f_1\ , \ldots\ , f_p\ , f_1^{-1}\ , \ldots\ , f_p^{-1}$ de M tels que, pour tout $i = 1\ , \ldots\ , p$,

$$\varphi(f_i) = \gamma_i\ ,\quad \varphi(f_i^{-1}) = \gamma_i^{-1}\ .$$

Soit alors θ la congruence sur X^*, définie par

$$f\ \theta\ g \iff \Psi f = \Psi g\ ,$$

qui vérifie évidemment la condtion

$$[1]_\theta = \varphi^{-1}(1) = \Psi^{-1}(1)\ .$$

Définissons A comme l'ensemble

$$A = \{f_i\ ,\ f_i^{-1} \mid i = 1, \ldots , p\} \cup \{x\}\ ,\ x \in X \setminus X'\ .$$

Nous avons $\qquad X^* = \bigcup_{f \in A^*} [f]_\theta :$

en effet, tout élément γ' de Γ' s'écrit comme un produit des $\gamma_1\ , \ldots\ , \gamma_p$ et et de leurs inverses, soit $\quad \gamma' = \gamma_{i_1}^{\varepsilon_1} \cdots \gamma_{i_k}^{\varepsilon_k}\ .$

D'où, si $\Psi(f) = \gamma'$, $\ f\ \theta\ f_{i_1}^{\varepsilon_1} \cdots f_{i_k}^{\varepsilon_k}$ avec $f_{i_1}^{\varepsilon_1} \cdots f_{i_k}^{\varepsilon_k} \in A^*$.

Si maintenant $\gamma \in \Gamma' \star \Gamma_\omega$ s'écrit

$$\gamma = \gamma'_1\ \omega\ \gamma'_2\ \omega \ldots \omega\ \gamma'_{\ell+1} \quad \text{avec} \quad \gamma'_1\ , \ldots,\ \gamma'_{\ell+1} \in \Gamma'\ ,$$

et si $\Psi(f) = \gamma$, on a

$$f = g_1 x_{i_1} g_2 x_{i_2} \dots x_{i_\ell} g_{\ell+1} \quad \text{avec} \quad \varphi(g_j) = \gamma'_j \quad \text{et} \quad x_{i_1} \dots x_{i_\ell} \in X \setminus X' .$$

Pour tout $j = 1, \dots, \ell + 1$, il existe $g'_j \in A^*$: $g_j \ \theta \ g'_j$, d'où

$$f \ \theta \ g'_1 \, x \, g'_2 \, x \dots x \, g'_{\ell+1} ,$$

ce dernier mot étant dans A^* .

Nous venons en fait de calculer $\mu(f) = \min \{k \in \mathbb{N} \mid A^k \cap [f]_\theta \neq \emptyset\}$.

Si en effet, λ est la longueur sur Γ' , définie par

$$\forall \gamma' \in \Gamma' , \quad \lambda\gamma' = \min \{k \in \mathbb{N} \mid \gamma' = \gamma_{i_1}^{\varepsilon_1} \dots \gamma_{i_k}^{\varepsilon_k}\} ,$$

nous avons, si $f = g_1 x_{i_1} g_2 x_{i_2} \dots x_{i_\ell} g_{\ell+1}$,

$$\mu f = \ell + \sum_{j=1}^{j=\ell+1} \lambda\Psi(g_j)$$

Sachant (cf. [1]) que λ est archimédienne sur Γ' , il est immédiat de vérifier que μ est archimédienne sur X^* . On vérifie aussi aisément que μ est réductive sachant que λ sur Γ' vérifie, $\forall \gamma , \gamma' , \gamma'' \in \Gamma'$ et $\forall m \in \mathbb{N}$,

$$\lambda\gamma + \lambda\gamma' - \lambda\gamma\gamma'^{-1} \geq m$$

$$\lambda\gamma + \lambda\gamma'' - \lambda\gamma\gamma''^{-1} \geq m$$

$$\Longrightarrow \lambda\gamma' + \lambda\gamma'' - \lambda\gamma'\gamma''^{-1} \geq m$$

Q. E. D.

BIBLIOGRAPHIE

[1] LYNDON (R.). - Length functions in groups, Math. Scand. , Kobenhavn, **t. 12, 1963,** p. 209-234.

[2] NIVAT (M.). - Congruences de Thue et t-langages, **Studia scient. Math. Hungar.** (à paraître).

[3] NIVAT (M.). - On a family of languages related to the Dyck set, Proceedings of the ACM Conference on the theory of computation [1970. Northampton], p. 221-225. - New York, Association for Computing Machinery, 1970.

(Texte reçu le 3 juillet 1970)

Maurice NIVAT
9 rue Portalis
75 - PARIS 08