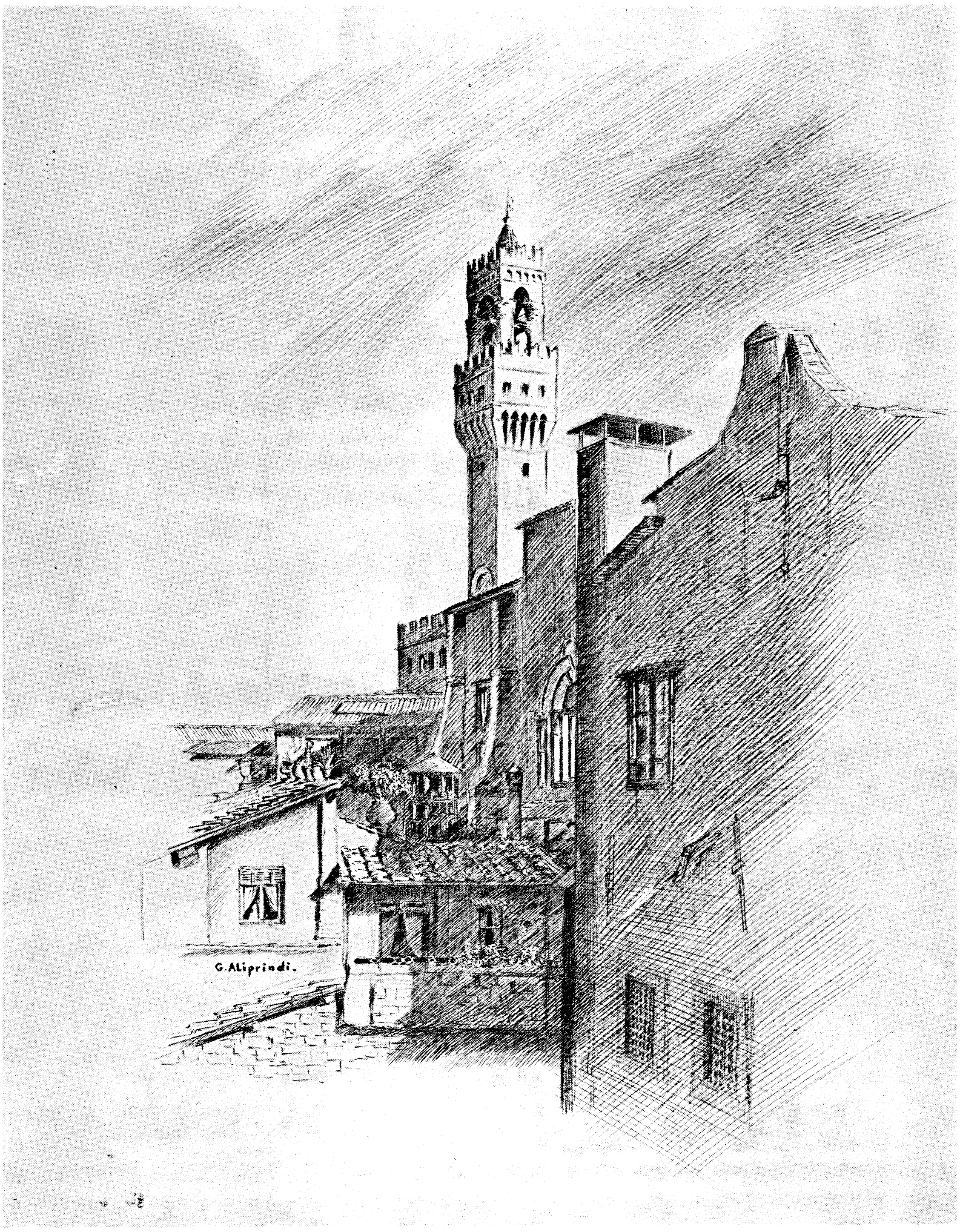
CONSIGLIO NAZIONALE DELLE RICERCHE
ISTITUTO DI ANALISI GLOBALE

ATTI DEL CONVEGNO SU

CODAGES et TRANSDUCTIONS



a cura di giuseppe pirillo

firenze, 15-17 ottobre 1979

MARCO SCHÜTZENBERGER

Université de Paris 7

Laboratoire d'Informatique Théorique et Programmation du CNRS, Paris

SUR LES SOUS GROUPES DE RANG FINI D'UN GROUPE LIBRE

Résumé: On associe à chaque sous-groupe H de rang r d'un groupe libre F des sous-groupes de F, dits annexes de H, qui sont de groupes de permutations sur les classes latérales de F. On montre que le degré d'un groupe annexe (i.e. le nombre de points sur lequels il opère) est borné en fontion du rang r de H (par le nombre 3r-1) excepté quand le groupe annexe est cyclique (et le nombre de classes de conjugaison de groupes annexes cycliques est borné par r).

Abstract: We prove that certain permutation groups, associated with a subgroup of finite rank r of a free group, have rank one (i.e. are cyclic) when their degree exceds 3r-1.

Riassunto: Sia H un sottogruppo a r generatori di un gruppo libero. Noi proviamo che alcuni gruppi di permutazioni associati ad H sono ciclici quando il numero di punti sui quali essi operano supera 3r-1.

SUR LES SOUS GROUPES DE RANG FINI D'UN GROUPE LIBRE

Le résultat principal est la Proposition 1; il est la seule motivation des énoncés précédant sa preuve donnée dans la section 3, sauf les remarques de l'Introduction 0 qui n'ont d'autre prétention que d'éclairer la définition 1. La section 1 est surtout un exposé des notations nécéssaires pour passer du Théorème de Nielsen sous sa forme classique empruntée au traité [5] de Lyndon et Schupp aux monoïdes libres.

Celles-ci sont encore plus détaillées dans la section 3. La section 4 est un exercice de traduction de la méthode des transversales de Schreier en termes de représentations de semi-groupes finis et donne un algorithme de construction des classes de groupes annexes. Il aurait dû venir avant la section 2, si nous n'avions voulu manifester des prévenances pour un eventuel lecteur plus familier, o combien!, avec les groupes libres qu'avec les concepts et les techniques exposées dans les ouvrages de S. Eilenberg [3] ou de G. Lallement [4].

Ce travail a été écrit au Centre d'Analyse Globale à Florence dont le Directeur, le Professeur Gherardelli nous a fait l'honneur de nous inviter sous les auspices du C.N.R. Que lui même et le Professeur Pucci veuillent accepter cet essai en hommage d'amicale reconnaissance.

0. Introduction

Dans tout ce qui suit F est un groupe libre et H un sous groupe de rang (= nombre de générateurs) fini r de F. On s'intéresse à l'action de F et de certains de ses sous groupes G sur les classes latérales Hf $(f \in F)$. Un sous ensemble de ces dernières sera désigné par une notation telle que HF_1 en convenant que $F_1 \subset F$ est une transversale c'est-à-dire que $Hf \neq Hf'$ pour deux quelconques de ses éléments f et $f' \neq f$.

Définition 1. Un sous groupe G de F est un groupe annexe (de la paire (H,F)) ssi il est le stabilisateur, $G = \{f \in F : HF_1 f = HF_1\}$ d'une union finie HF_1 de classes latérales telles que HfG contienne une infinité de classes pour chaque $f \notin HF_1$. Son degré est le nombre des classes latérales dans HF_1 ; son degré d'intransitivité est le nombre maximum d'éléments dans une tranversale $F_1' \subset F_1$ telle que $f'' \notin Hf'G$ pour toute paire d'éléments f' et $f'' \neq f'$ de F_1'.

Par conséquent F lui-même est le seul groupe annexe quand il n'y a qu'un nombre fini de classes latérales et pourvu que le rang r de H soit $\geqslant 2$, son degré est fourni par la formule de Schreier ([5]), $d = (r-1)/(r'-1)$ où r' reste le rang de F. Quand H est engendré par un seul élément h, tous les groupes annexes sont conjugués du groupe G, engendré par l'élément $g = \sqrt{h}$ tel que $h = g^p$ $(p \geqslant 1)$ avec p maximum et le degré de G est p.

Dans le cas général, le théorème de Nielsen [5] montre facilement (section 1) que le degré des groupes annexes est au plus égal au double de la somme k des longueurs des mots d'une base de H et que le nombre de leurs classes (sous entendu, de conjugaison) n'excède pas 4^k

Proposition 1. Tous les groupes annexes ont un degré d'intransitivité $\leqslant 3\,r-1$ et le nombre de leurs classes est inférieur à $1/2\ (3^{3r-1}-1)$; ceux dont le degré est $\geqslant 3r-1$ sont de rang un et le nombre de leurs classes est $\leqslant 3r-2$.

Pour discuter commodément ces notions, on dira que deux transversales F_1 et F'_1 sont équivalentes ssi $HF_1 = HF'_1$ et que F_1 est une transversale du groupe annexe G ssi c'est une transversale finie maximale dont G est le stabilisateur. Toutes les transversales de G sont donc équivalentes et les transversales des groupes $f^{-1}\,G\,f$ $(f \in F)$ de la classe de G sont leurs translatés $F_1\,f$.

Comme d'usage, 1 est l'élément neutre de tout monoïde et on pose $\sqrt{H} = \{\sqrt{h} : h \in H\}$ où, comme ci-dessus, $\sqrt{h}$ désigne le générateur du plus grand semi-groupe de rang un contenant h.

0.1 Si $\sqrt{H} \subset H$ chaque groupe annexe G est le fixateur $(HfG = Hf)$ des éléments de ses transversales. Réciproquement H est contenu dans l'union des groupes annexes; tout élément de ces derniers est conjugué d'une puissance d'un élément de $\sqrt{H}$ et si p est le plus petit entier tel que pour un $g^p \in H$, tout groupe annexe contenant g a un degré $\geqslant p$.

Preuve. Supposons au contraire qu'un groupe annexe G contienne un g tel que $H\,f\,g \neq H\,f$ pour un élément f d'une transversale F_1 de G. Quitte à remplacer F_1 par $F_1 f^{-1}$ et G et g par leurs conjugués $f\,G\,f^{-1}$ et $f\,g\,f^{-1}$ on peut supposer $f = 1$. Donc $Hg \neq H$, c'est-à-dire $g \notin H$.

Comme $d = \mathrm{Card}\,(F_1)$ est fini, par hypothèse chaque $d!$-ième puissance d'un élément de G est dans le fixateur de F_1, donc en particulier dans H qui est le fixateur de 1. Par conséquent g a une plus petite puissance $p \geqslant 2$ telle que $g^p = h \in H$ et, comme il est lui-même la q-ième puissance $(q \geqslant 1)$ de $x = \sqrt{h} = \sqrt{g}$, on en conclut que H ne contient pas $\sqrt{H}$. De plus $\{1, g, \ldots, g^{p-1}\}$ forme une transversale équivalente à une partie de F_1 et par conséquent $d \geqslant p$.

Considérons maintenant $x = \sqrt{h} = \sqrt{g}$ et le sous groupe X qu'il engendre. Pour chaque $f \in F_1$, $H f X$ est l'union d'au plus q classes latérales. Donc X est dans le stabilisateur de l'union finie HF_1X de classes latérales. Anticipant sur la section suivante, nous faisons appel au Théorème de Nielsen qui donne une borne supérieur $k < \infty$, ne dépendant que de H, à toute transversale finie qui est stabilisée par un sous groupe $(\neq \{1\})$ de F. Ce fait implique que F_1X soit contenu (mod H) dans une plus petite transversale F_2, stabilisée par X et telle que $H f X$ contienne une infinité de classes latérales quand $f \notin H F_2$. Son stabilisateur G' est un groupe annexe contenant X, donc g, donc h (mais non nécessairement G), ce qui achève d'établir la remarque.

Q.E.D.

0.2 Si $H \cap f^{-1} H f = \{1\}$ pour chaque $f \notin H$, tous les groupes annexes sont conjugués de H et ont degré 1. Réciproquement, chaque sous groupe $\neq \{1\}$ de la forme $H \cap f^{-1} H f$ $(f \notin H)$ est contenu dans un groupe annexe $\neq H$.

Preuve. Soit F_1 une trasversale d'un groupe annexe G; le degré local de G en $f \in F_1$ est le nombre des classes latérales dans $H f G$ et on peut supposer G choisi parmi ses conjugués de telle sorte que le degré local soit maximal pour $f = 1$. Supposons que H ait une intersection triviale avec tous ces conjugués. Ceci implique que $\sqrt{H} \subset H$, puisque $\sqrt{h}$ commute avec h. Donc le degré local de G en 1 est un, ce qui signifie que G est un sous groupe de H. Par construction le degré local est aussi 1 en tout autre $f \in F_1 \setminus \{1\}$, s'il en existe. Supposons-le. On a $Hfg = Hf$, c'est-à-dire $fgf^{-1} \in H$ où $g \in G \subset H$ en contradiction avec l'hypothèse initiale. Donc le degré de G est 1, c'est-à-dire que $G = H$.

Réciproquement tout $h \neq 1$ contenu dans l'intersection H' de H avec $f^{-1} H f$ satisfait $f h = h'f$ pour un $h' \in H$, donc $Hfh = Hf$. Supposant $f \notin H$, le même argument que dans 0.1 montre que l'ensemble des $f' \in F$ tels que H' soit de degré local fini en Hf' est contenu dans une union HF_1 d'au plus k classes latérales dont le stabilisateur est un groupe annexe contenant H'.

0.3 Le nombre des classes de H-conjugaison qui peuvent être contenues dans une classe de conjugaison de F est au plus égal au maximum des degrés des groupes annexes de rang $\geqslant 2$ et des degrés d'intransitivité des groupes annexes de rang 1.

<u>Preuve</u>. Soient $h = h_1 \in H_1$, $f_1 = 1$ et $\{h_i = f_i\, h\, f_1^{-1} \ :\ 1 \leqslant i \leqslant d\}$ un système maximal d'éléments h_i de H qui ne sont pas H-conjugués c'est-à-dire qui sont tels que $h_i = h'\, h_j\, h^{i-1}$ pour un $h' \in H$ seulement si $i = j$.

Comme précédement on voit que $\{f_i \ :\ 1 \leqslant i \leqslant d\}$ est une partie d'une transversale F_1 dont le stabilisateur G est un groupe annexe de degré $\geqslant d$ qui contient h. Supposons que G soit le groupe de rang 1 engendré par un élément g de F. On a $g = \sqrt{h}$ et l'hypothèse que les h_i ne sont pas H conjugués implique qu'aucun f_j ne soit tel que

$Hf_j = Hf_i\, g^m$ pour un $m \geqslant 1$ et $f_i \neq f_j$ car sinon on aurait $h_j = f_j\, h\, f_j^{-1} = f_i\, g^m\, h\, g^{-m}\, f_i^{-1} = h_i$.

Donc d est borné à la fois par le degré des groupes annexes et par le degré d'intransitivité de ceux qui sont de rang un.

Q.E.D.

Le groupe de permutation fini $[G]$ quotient du groupe annexe G par restriction à une de ses transversales de son action sur les classes latérales peut être arbitrairement compliqué: il suffit de prendre pour H le groupe engendré par une partie de la base d'un sous groupe d'index fini, ainsi que me l'a fait observer D. Perrin dont les avis et les suggestions sont à l'origine de ces recherches.

Les valeurs numériques indiquées dans la Proposition sont manifestement ridicules. Non pas parce que divers calcus subsidiaires permettant de les réduire de quelques unités ont été omis, mais parceque je n'ai pas trouvé le moyen d'utiliser les structure de E et du morphisme $\beta: B^* \longrightarrow A^*$ de la section 2 , ni, vraisemblablement,de voir des propriétés moins superficielles des groupes annexes que celles présentées dans l'Introduction. Certains lecteurs informaticiens auront d'ailleurs reconnu dans la section 3 l'application brutale d'une technique pour borner les groupes dans le monoïde syntaxique d'une partie rationnelle $K = V^*\varphi \subset A$ en fonction du rang d'une partie locale E dont K est l'image. Les seules propriétés spécifiques de E qui soient mises en oeuvre sont celles qui découlent de l'existence d'inversions formelles c'est-à-dire de mots réduits; elles diminuent le rang par un facteur deux. Le théorème de Cesari et Duval donnant des bornes optimales du point de vue des techniques employées,d'autres idées seraient donc nécessaires. En effet on a toute raison de penser qu'il existe r éléments de

Γ tels que, d'une part, chaque groupe annexe de degré $\geqslant r+1$ (ou peut-être $\geqslant r$) est conjugué du sous groupe engendré par l'un d'eux et que, d'autre part, une base de H est constituée d'un système de leurs puissances. Je n'ai pas pu dépasser le cas de $r = 2$ qui de toutes façons, comme on le sait, présente pour ce type de problèmes des particularités qui ne se rencontrent pas pour les rangs plus élevés.

1. Première application du théorème de Nielsen

Une $\pm$ base d'un groupe est l'union d'une base (= ensemble générateur minimal) et des inverses de ses éléments. On suppose qu'une $\pm$ base A de F a été choisie une fois pour toute ce qui fait qu'il existe un morphisme surjectif α sur F du monoïde libre A^* engendré par A. On note A^+ le semigroupe libre $A^+ = A^* \setminus \{1\}$ engendré par A. Pour chaque lettre a de A on écrit indifféremment a^{-1} ou $\bar{a}$ et l'inverse formel d'un mot $w = a_1 a_2 \ldots a_n$ ($n \geqslant 0$, $a_i \in A$) est $\bar{w} = \bar{a}_n \ldots \bar{a}_2 \bar{a}_1$ donc $\bar{\bar{w}} = w$ et $\bar{w}\alpha = (w\alpha)^{-1}$. Si X est une partie de A^*, on écrit $\bar{X} = \{\bar{x} : x \in X\}$ et on dit que X est symétrique ssi $X = \bar{X}$.

L'ensemble des mots réduits est $L^1 = \{1\} \cup L$ où

$L = A^+ \setminus \{A^* a \bar{a} A^* : a \in A\}$.

On sait que c'est une section de F en ce sens qu'il existe une bisection φ de F sur L^1 telle que $w = w\alpha\varphi$ ssi $w \in L^1$. L'expérience montre qu'il n'y a pas d'inconvénient à écrire w au lieu de $w\alpha$ pour désigner un élément de F, donc à définir $w\varphi$ pour chaque mot w comme l'unique mot réduit représentant l'élément w de F. Ce mot réduit est obtenu en effaçant dans w tous les facteurs de la forme $a\bar{a}$ et en continuant l'opération tant que le mot résultant n'est pas réduit; le mot final w ne dépend pas de la manière dont les effacements (= cancellations) sont effectués, comme le savent tous les lecteurs du beau livre de J. Berstel sur les langages algèbriques.

Pour préciser les calculs on désigne par $w \wedge w'$ le plus long facteur gauche commun de deux mots w, w'; leur plus long facteur droit commun est donc l'inverse formel de $\bar{w} \wedge \bar{w}'$.

Soient $w, w' \varepsilon L$, $u = \bar{w} \wedge \bar{w}'$ $w = v\bar{u}$, $w' = u\, v'$ $(v, v' \varepsilon A)$. On a $w\, w' = v\, v' \varepsilon L^1$ ce qui est la réalisation dans A^* du produit dans F. Considérons le cas particulier de $w' = w$. On montre facilement que l'hypothèse $w \varepsilon L$ implique $2|u|<|w|$, c.-à-d. que $w = u\, v''\, \bar{u}$ où $v'' \varepsilon A^+$; le mot v'' est le <u>facteur circulaire</u> de w et $(w^p)\varphi = u(v'')^p\, \bar{u}$: $(p \leqslant 1)$.

Le mot réduit $w = a_1 \dots a_n$ $(n \geqslant 1,\ a_i \varepsilon A)$ est <u>circulairement réduit</u> ssi $w = v''$, c'est-à-dire, de façon équivalente, ssi il est réduit et $\bar{a}_1 \neq a_n$ ou si son carré w^2 est réduit. On rappelle que les <u>conjugués</u> dans le monoïde libre A^* de w sont les mots $a_i \dots a_n\, a_1 \dots a_{i-1}$.

Un calcul bien connu montre que la classe de conjugaison $\{f\, w\, f^{-1} : f \varepsilon F\}$ de w dans le groupe F est formée des mots dont le facteur circulaire est conjugué dans A^* de celui de w.

Soient maintenant H le sous groupe donné de F et $V = \{v_i\ ,\ \bar{v}_i : 1 \leqslant i \leqslant r\} \subset L$ une $\pm$ base de H; il sera commode de désigner $\bar{v}_i$ par v_{-i} $(1 \leqslant i \leqslant r)$. H est représenté par l'ensemble de mots réduits $V^*\varphi$ (V = le sous monoïde engendré par V). Comme H est (isomorphe à) un groupe libre, chacun de ses éléments est égal de façon unique à un produit $v_{i_1} \dots v_{i_n}$ $(v_{i_j} \varepsilon V)$ qui est V-<u>réduit</u> en ce sens que $V_{-i_j} \neq V_{i_{j+1}}$ $(1 \leqslant j \leqslant n-1)$.

Le théorème suivant est la base du reste du travail. Il est prouvé dans [5] p. 7. L'enoncé est alourdi par les précisions de notations nécessaires pour la suite.

<u>Théorème de Nielsen</u>. Le groupe H a un $\pm$ base $V \subset L$ telle que chaque $v_i \in V$ ait une factorisation distinguée $v_i = y_i \, x_i \, \bar{y}_{-i}$ ayant les trois propriétés suivantes:

(1) $x_i \in A^+$ et $y_{-i} \, \bar{x}_i \, \bar{y}_i$ est la factorisation distinguée de $v_{-i} = \bar{v}_i$;

(2) y_i est le plus long facteur de v_i de la forme $v_i \wedge v_j$ $(v_j \in V \setminus v_i)$;

(3) $|y_i| \leqslant |x_i \, \bar{y}_{-i}|$;

Par conséquent si $-i \neq k$ on a $(v_i \, v_k)\varphi = y_i \, x_i \, \bar{y}'_{-i} \, y'_k \, x_k \, y''_k$ où y'_{-1} (resp. y'_h) est un facteur gauche de $\bar{y}_{-i}$ (resp. droit de y_h). Plus généralement, soit $h \in H \setminus 1$; il est de façon unique un produit V-réduit $v_1 \ldots v_n$ $(v_i \in V)$ et le mot réduit $h\varphi$ qui le représente a une factorisation $v''_1 \, v'_2 \ldots v''_n$ dont nous soulignons les propriétés:

v''_1 (resp. v''_n) est un facteur gauche (resp. droit) du $v \in V$ de même indice;

chaque v'_i est un facteur du $v_i \in V$ correspondant admettant lui-même comme facteur la partie ineffaçable x_i.

Nous appellerons cette factorisation la <u>factorisation de Nielsen</u> de h et n sera la <u>V-longueur</u> de h. On notera que la factorisation de Nielsen de $v_2 \ldots v_n$ est $v''_2 \ldots v''_n$ où v''_2 admet v'_2 comme facteur droit et que si h est <u>circulairement</u> V-<u>réduit</u> en ce sens que $\bar{v}_1 \neq v_n$, le facteur circulaire de $h\varphi$ est $v'_1 \ldots v'_n$ avec v'_1, v'_n comme ci-dessus.

La base de Nielsen V sera désormais supposée être choisie et on notera P l'ensemble des mots $\neq 1$ qui sont des facteurs gauches de ses éléments. Donc $V \subset P \subset L$.

Remarque 1.1 Soient $u \neq 1$ circulairement réduit et f tels que $H\,f\,u = H\,f$. Il y a un $p \in P$ tel que $H\,f = H\,p = H\,p\,u$ avec $pu \in L$.

Preuve L'équation $H\,f\,u = H\,f$ signifie que $(f\,u\,\bar{f})\varphi = h \in H$. Si l'on remplace f par $(f\,u^n)\varphi$ pour n assez grand on obtient un mot f' de la même classe latérale que f qui satisfait f', $f'u \in L$. On peut donc supposer que f lui-même a été choisi dans sa classe latérale de façon à satisfaire cette condition et à minimiser la longueur de $(f\,u\,\bar{f})\varphi$. Ceci entraine que le plus long facteur droit commun u' de f et de u soit de longueur $|u'| < |u|$. Il existe donc $y \in A^*$ et $u'' \neq 1$ tels que $f = y\,u'$; $u = u''u'$ et enfin $(f\,u\,\bar{f})\varphi = y\,u'u''\bar{y}$.

Soit $v''_1 \ldots v''_n$ la factorisation de Nielsen de ce mot. Il existe un indice j, un mot $t \neq 1$ et un mot t' tels que
$f = v''_1 \ldots v'_{j-1}\,t$, $v'_j = t\,t'$.

Soient $h' = (v_1 \ldots v_{j-1})\varphi \in H$ et $v''_j \ldots v''_n$ la factorisation de Nielsen de $(\bar{h}'\,h)\varphi = (v_j \ldots v_n)\varphi \in H$.

On a vu que v'_j est un facteur droit de v''_j et que ce dernier mot est un facteur gauche de $v_j \in V$. Il y a donc un $p' \in A^*$ tel que $v''_j = p'\,v'_j = p'\,t\,t'$, ce qui fait que $p = p'\,t$ est un facteur gauche d'un mot v_j de V et qu'il appartient à P puisque $|p| \geqslant |y| \geqslant |0|$ par construction. D'après le choix de l'indice j on a $(\bar{h}'\,f)\varphi = p'\,y = p$, ce qui montre que $H\,p = H\,f$ et la relation $p\,u \in L$ découle de ce que $y\,u'' \in L$ où $u'' \neq 1$ est un facteur gauche de u.

Q.E.D.

Remarque 1.2 Soient $G \neq \{1\}$ un sous groupe de F et F_1 une transversale telle que $H\,f\,G$ soit une union finie de classes pour chaque $f \in F_1$. On a $\mathrm{Card}\,(F_1) \leqslant \mathrm{Card}\,(P)$ et le stabilisateur de $H\,F_1$ est un groupe annexe contenant G .

Preuve On prend un élément arbitraire $x u \bar{x}$ ($x \in A^*$, u circulairement réduit) dans $G \setminus 1$. Quitte à remplacer G par $x^{-1} G x$ et F_1 par $F_1 x$ on peut supposer $x = 1$.

Pour chaque $f \in F_1$ il existe un plus petit p positif fini tel que $H f u^p = H f$. La même relation vaut pour chaque $f u^j$ $(0 \leqslant j \leqslant p - 1)$. D'après la remarque précédente cet ensemble d'éléments forme une transversale équivalente à une partie P_{1i} de P, et la conclusion en découle puisque P est fini.

Q.E.D.

On rappelle qu'un mot s est dit primitif ssi $s = \sqrt{s}$ et que s^+ désigne le semigroupe engendré par s.

Lemme 1.3 Il existe un ensemble S de mots primitifs circulairement réduits en bijection avec les classes C de groupes annexes, et pour chaque classe C un groupe $G \in C$ contenant $s = s(C) \in S$, et une transversale $P_s \subset P$ de G tels que $P_s s^+ \subset L$ et qu'en outre :

(i) Si G n'est pas de rang un, la longueur de s excède celle des mots de V;

(ii) Si $C' \neq C$ est une autre classe, $s(C')$ n'est conjugué d'aucune puissance de s ni de $\bar{s}$.

Preuve Soit $q = (\text{Card } P)\,!$ On peut choisir $G \in C$ contenant au moins un mot circulairement réduit $u \neq 1$. Comme l'ensemble des $f \in F$ pour lesquels $H f u^+$ est une union finie de classes est le même que pour $\sqrt{u}$, on peut supposer $u = \sqrt{u}$, donc u primitif. Appliquant la construction de la remarque 1.1 à u^q , on obtient une transversale $P_1 \subset P$ de G avec $P_1 u \in L$

et on peut trouver pour chaque $p \in P_1$ un p'' satisfaisant la condition indiquée pour s.

Nous montrons maintenant que l'on peut choisir u au départ de façon à satisfaire (i) et (ii).

Si G a rang $\geqslant 2$ il existe un $g \in G$ qui n'est pas une puissance de s. La même chose vaut pour les mots $(u^n g u^n)\varphi = g'$ et il suffit de vérifier que pour tout n assez grand $u^n g'^n$ est un mot primitif circulairement réduit aussi long qu'on le veut.

En raison des rapports entre la conjugaison des groupes et la translation des transversales et du fait que chaque groupe annexe est défini comme le stabilisateur de sa transversale, il suffit pour établir (ii), de montrer que l'on peut choisir u de telle sorte que $H f u^q \neq H f$ pour tout $f \in H P_1$. Supposons que cela ne soit pas le cas pour $p \notin H P_1$. Il existe un $y \in G$ tel que $H p g^m \cap H P_1 \neq \emptyset$ pour tout m assez grand; on peut trouver un n tel que $(u^{nq} g^m u^{nq})$ soit circulairement réduit quelque soit m. Remplaçant u par ce nouvel élément, diminue d'au moins une unité le nombre des classes Hp $(p \in P_1)$.

2. Un corollaire du théorème de Nielsen

On se propose de construire un nouvel alphabet $B = B_1 \cup B_2 \cup \bar{B}_2$ et un morphisme $\beta : B^* \longrightarrow A^*$ de façon à satisfaire les conditions énoncées dans le Lemme 2.1 ci-dessous.

Comme la Proposition 1 ne dépend pas du choix du groupe H dans sa classe de conjugaison, on fera désormais l'hypothèse que H est réduit en ce sens que 1 est le plus long facteur gauche commun des mots de la base de Nielsen V. On peut toujours se ramener à ce cas. En effet, soit

$f = \wedge\{v : v \in V\}$. Comme V est symétrique $(V = \overline{V} = \{\overline{v} : v \in V\})$ chaque $v_i \in V$ a la forme $f\, v_1'\, \overline{f}$ et d'après la définition même, de sa factorisation distinguée, $y_i\, x_i\, \overline{y}_{-i}$, f (resp. $\overline{f}$) est un facteur gauche (resp. droit) de y_i (resp. $\overline{y}_{-i}$). Donc $V' = (\overline{f}\, V\, f)\varphi$ est une base de Nielsen du sous groupe conjugué $f^{-1}\, H\, f$ et 1 est le seul facteur gauche commun de ses mots.

Pour obtenir B, on commence par définir la famille T des parties $V' \neq \emptyset$ de V telles que le mot $w(V') = \wedge\{v' \in V'\}$ soit $\neq 1$ et ne soit facteur gauche d'aucun mot de $V \setminus V'$; le sous ensemble T_1 des éléments minimaux de T est donc constitué par les $2r$ singolets $\{v_i\}$ $(v_i \in V)$.

Pour chaque $V' \in T$ le mot $y' = w\,(V')$ a un plus long facteur gauche $y'' \neq y'$ qui est 1 ou de la forme $y'' = w\,(V'')$ avec $V'' \in T$; dans le premier cas on pose $V'\vartheta = V$; dans le second $V'\vartheta = V''$.

Si V' n'est pas un singolet on lui attache une lettre de B que l'on note $b\,(V'\vartheta, V')$ et dont l'image par B est le mot z tel que $y''z = y'$; l'inverse formel de cette lettre sera la lettre $b\,(\overline{V}', \overline{V'\vartheta})$ d'image $\overline{z}$ par B. L'ensemble de ces lettres forme le sous alphabet $B_2 \cup \overline{B}_2$ de B; on a $B_2 \cap \overline{B}_2 = \emptyset$ puisque l'indice gauche $V'\vartheta$ contient strictement l'indice droit V' pour les lettres de B_2 alors que c'est le contraire qui se produit pour l'ensemble $\overline{B}_2$ de leurs inverses formels.

Dans le cas opposé où V' est un singolet $\{v_i\}$ on définit une lettre $b \in B_1$ dont l'indice gauche est $\{v_i\}\vartheta$, l'indice droit $\overline{\{v_{-i}\}\vartheta}$ et qui a un indice intermédiaire v_i . Son inverse formel est la lettre du même sous alphabet B_1 qui est définie par le singolet $\{v_{-i}\}$ et son image par β est le facteur ineffaçable x_i de v_i . Par conséquent $B = B_1 \cup B_2 \cup \overline{B}_2$ est muni d'une inversion formelle et le morphisme

β: $B^* \longrightarrow A^*$ qui prolonge β commute avec celle-ci. Le lecteur pourra noter que la construction est invariante pour l'échange de la gauche et de la droite. En effet, en raison de $V = \bar{V}$ et de la symétrie des factorisations distinguées $y_i\ x_i\ \bar{y}_{-i}$ des mots de Nielsen, cet échange remplacerait l'opération $\wedge$ par l'opération correspondante sur les facteurs communs droits.

On désignera par les mêmes symboles α et φ que pour A^* le morphisme naturel ($\bar{b}\alpha = (b\alpha)^{-1}$) envoyant B^* sur le groupe libre de $\pm$ base B et l'opération de réduction envoyant chaque mot sur l'unique mot réduit qui représente le même élément de $B^*\alpha$.

Nous construisons maintenant un ensemble $W \subset B^+$ qui constitue une base de Nielsen d'un sous groupe H' de $B^*\alpha$ de rang 2 tel que B envoie $W^*\varphi$ sur $V^*\varphi$.

Reprenant la construction de B, on voit que W est l'ensemble des mots w de B^+ qui satisfont les cinq conditions suivantes dont les quatre premières portent sur tous leurs facteurs de la forme b ou bb' (b, b' ε B) :

(1) w est réduit, c'est-à-dire $b' \neq \bar{b}$;

(2) Si $b\ \varepsilon\ B_2$ alors $b' \not\varepsilon\ \bar{B}_2$;

(3) L'indice droit de b est égal à l'indice gauche de b';

(4) L'indice gauche de la première lettre est V et il en est de même de l'indice droit de la dernière;

(5) w a exactement une occurence d'une lettre de B_1 ;

Il suffit d'examiner le réduction de $w\ w' \longrightarrow (w\ w')\varphi$ (w, w' ε W) pour constater que $W^+\varphi$ est formé des mots qui satisfont les quatre premières conditions.

Puisque les groupes H et H' sont isomorphes (en tant que groupes libres de même rang) la restriction de β à $W^*\varphi$ est une bijection sur $V^*\varphi$.

De plus en raison du théorème de Nielsen l'image de B^* par β dans A^* (qui peut d'ailleurs se trouver être égale à A^*) est par construction le plus petit sous monoïde de A^* qui contienne le plus long facteur gauche commun de deux mots de $V^*\varphi = H$ ce qui a pour conséquence que cette image ne dépend que de H et non de la base de Nielsen V qui a été choisie.

Pour disposer plus tard de toutes les notations, nous supposons donné un ordre total $\leqslant$ sur B tel que chaque lettre b soit contiguë de son inverse formel et que l'on ait $b' < b$ toutes les fois que $b'\beta < b\beta$. A chaque lettre b on associe l'ensemble $S(b)$ des mots $s \in S$ pour lesquels b (c'est-à-dire $b\alpha$) est un facteur de s^+ (c'est-à-dire d'un mot de s^+) et pour lesquels ceci n'est vrai d'aucun $b' > b, \bar{b}$. Si l'on avait un $s \in S(b) \setminus S(\bar{b})$ et un $s' \in S(\bar{b}) \setminus S(b)$ on pourrait remplacer s' par $\bar{s}$ dans la construction du Lemme 1.3. On peut donc supposer donnée une <u>moitié</u> B_+ de B (c'est-à-dire B = l'union disjointe de B_+ et $\bar{B}_+$) telle que les blocs $S(b)$ $(b \in B_+)$ constituent une partition de l'ensemble S de tous les mots s du lemme 1.3

<u>Corollaire du Théorème de Nielsen 2.1</u> Il existe un monoïde libre $(B_+ \cup \bar{B}_+)^*$ un morphisme $\beta : B^* \longrightarrow A^*$ commutant avec l'inversion formelle et une partie E de B^* contenant les facteurs gauches de ses mots tels que pour tout $s = s\ (C)$ on ait :

(i) Card $(B_+) \leqslant 3r - 2$;

(ii) $P_s\, s^+$ est contenu dans l'ensemble des facteurs gauches des mots de $E\beta$;

(iii) Si $f' \neq 1$ est un facteur gauche de s, $m \geqslant 0$, et $p_1 \neq p_2$ deux éléments de P_s, il n'existe pas de lettre $b \in B$ telle que

$p_1\ s^m\ f'$ et $p_2\ s^m\ f'$ soient contenus dans $(E \cap B^*b)$

Preuve (i). Le sous alphabet $B_1 = \overline{B}_1$ a 2r lettres, et les lettres de B_2 sont en bisection avec les membres de T qui ne sont pas des singolets. Comme $T \cup \{V\}$ est engendré à partir de ces derniers par itération de l'application strictement croissante ϑ, le nombre des membres de $T \cup \{V\}$ est au plus égal au nombre des singolets moins un.

Donc $\mathrm{Card}\ (B_2) \leqslant 2r - 2$ et

$\mathrm{Card}\ (B) \leqslant 2r + 2\ (2r - 2) = 2\ (3r - 2)$;

(ii) est la conséquence immédiate de ce que les mots de $P_s\ s^+$ sont des facteurs gauches de ceux de $V^*\varphi$ et de ce que $V^*\varphi \subset W^*\varphi \subset E$

(iii) Le caractère local des conditions définissant $W^*\varphi$ implique que si $w \in E$ l'ensemble des $w'' \in B^*$ tels que $w\,w'' \in W^*\varphi$ ne dépend que de la dernière lettre de w. Par conséquent chaque $(E \cap B\ b)\beta$ est contenu dans une classe latérale de H ne dépendant que de b $(b \in B)$ et le résultat en découle puisque P_s est une transversale, c'est-à-dire puisque par hypothèse p_1 et p_2 appartiennent à des classes latérales distinctes.

Q.E.D.

Question. Existe-t'il des propriétés de la paire de groupes (H, F) que l'on puisse attacher à la structure (T, ϑ) ?

3. Preuve de la Proposition

On aura besoin de distinguer les diverses occurrences d'un même mot comme facteur d'un mot donné $w = a_1 \dots a_n$ $(a_i \in A)$ de longueur positive n. Pour cela on considérera w comme une application dans A de l'intervalle de base $[1, n]$, et on dira qu'un sous intervalle $I = [i, j]$ est un <u>support</u> du mot f ssi $f = a_i \ldots a_j$ que l'on notera $f = I\,w$. Ceci justifie que l'on dise que I (ou le mot Iw) a la <u>périodicité</u> p ssi $1 \leqslant p \leqslant j + 1 - i$ et $a_k = a_{k+p}$ pour $i \leqslant k \leqslant k + p \leqslant j$; p sera une <u>période</u> (de I ou de Iw) ssi de plus I n'a pas une périodicité p' où $p' \neq p$ est un diviseur de p.

Il est clair qu'un mot f a une période egale à sa longueur ssi il est primitif ($f = \sqrt{f}$). On dit qu'il est <u>périodique</u> ssi il a une période p telle que $2\,p \leqslant |f|$ et on sait qu'il a au plus une telle période. Une <u>racine</u> de f est un facteur gauche de longueur égale à une période. Donc les conjugués des racines de f sont tous les mots primitifs g tels que $|g| \leqslant |f|$ et que f soient un facteur d'une de leurs puissances.

L'énoncé qui suit (connu de tous, sous une forme ou une autre) résume les propriétés élémentaires de ces notions.

<u>Lemme de conjugaison</u>. Les propriétés suivantes d'un mot w de longueur positive n sont équivalentes;

(1) w a une périodicité $m' < n$;

(2) Il existe un mot g de longueur $n - m'$ qui est à la fois facteur gauche et facteur droit de w ($w \in g\,A^* \cap A^*g$);

(3) w a une racine dont la longueur m divise m';

(4) $w = (uv)^p u$ où $p \geqslant 1$, $u \in A^+, v \in A^*$ uv est primitif de longueur m et $p\,m = m'$.

<u>Preuve</u>. (1) implique que $a_i = a_{i+m'}$ pour $1 \leqslant i < i + m' \leqslant n$, donc (2) avec $g = [1, n-m']\;w = [1+m', n]\;w$. Réciproquement si $w = g\,f' = f\,g$ ($f, f' \in A^*$) on a $a_i = a_{i+q}$ pour $1 \leqslant i \leqslant i + q \leqslant n$ où $q = |f| = |f'| = n - |g|$ donc (1).

Soit maintenant m le plus petit diviseur de m' tel que w ait périodicité m; on pose $n = m p + q$ où $1 \leqslant q \leqslant p$ et on considère le mot $[1, m]\, w = u\, v$ où $u = [1, q]\, w$ est le facteur gauche de f de longueur q. L'hypothèse que w a périodicité m équivaut à $w = (u\, v)^p\, u$. Si uv n'était pas primitif, c'est-à-dire si on avait $u\, v = s^r$ avec $s \in A^+$, $r \geqslant 2$ on aurait $w = s^{rp+p'} s_1$ avec s_1 un facteur gauche de s et par conséquent w aurait une périodicité $|s| < m$ divisant m' en contradiction avec le caractère minimal de m. Donc $f = u\, v$ est primitif et, comme $w\, v = f^{p+1}$, c'est une racine de w. Par construction tous les mots $g' = (u\, v)^{p'} u$ $(0 \leqslant p' \leqslant p)$ sont à la fois des facteurs gauches et des facteurs droits de w, ce qui conclut la preuve.

Q.E.D.

Une notion moins immédiate est la suivante. La <u>période locale</u> de w en j $(1 \leqslant j \leqslant n)$ est le minimum p de la longueur des mots z tels que l'on puisse trouver $g', g'' \in A^*$ pour lesquels z est facteur gauche de $g' a_1 \ldots a_j$ et facteur droit de $a_{j+1} \ldots a_n\, g''$.

On vérifie sans difficulté qu'il existe un z de longueur minimale p et que $p \leqslant n$, et, plus précisément $p \leqslant \pi(w)$, en notant $\pi(w)$ la période minima de w. L'indice j est dit <u>critique</u> ssi $p = \pi(w)$. La réciproque est l'objet d'un théorème découvert par Césari ([1]) dont la version optimale a été obtenue par Duval ([2]) auquel nous faisons référence pour la preuve et que nous utiliserons sous la forme suivante dans laquelle on suppose évidemment que la période p est $\geqslant 2$ c'est-à-dire que w n'est pas une puissance d'une lettre.

<u>Théorème de Cesari et Duval</u>. Tout mot w a un indice critique $k < p$ où $p = \pi(w)$ est la période minima de w.

On procède maintenant à une série de calculs qui sont loin d'être nouveaux mais auxquels l'emploi de l'indice critique apporte une clarté qu'apprécieront les rares amateurs. On note h la racine minima $a_1 \ldots . a_p$ de w, et $k \leqslant p$ un indice critique de w.

3.1 Si w admet des périodes $\neq n$ autres que p, on a $k \geqslant n - p'$ où p' est la plus petite de ces dernières.

<u>Preuve</u>. Soit $p < p' < n$. Comme w est facteur gauche de puissances de ses racines, on a $w = h\, h_1$ où $q \geqslant 1$ et h_1 un facteur gauche propre (c'est-à-dire $\neq h$) de h. De même $w = h'^{q'}\, h'_1$. Si w n'est pas périodique, $q = 1$ c'est-à-dire $h = h_1\, h_2$; $w = h\, h_1$, et aussi $w = h'_1\, h'_2\, h'_1$. Si w est périodique, $q \geqslant 2$ et $q' = 1$ puisqu'un mot n'a qu'une seule racine de longueur inférieure ou égale à la moitié de sa longueur. Donc $w = (h_1\, h_2)^q\, h_1 = h'_1\, h'_2\, h'_1$ avec dans tous les cas h_1 et h'_1 des facteurs gauches de h et le plus court de ces deux mots, disons g, un facteur droit de l'autre. Cette relation, comme on sait, implique l'existence d'un $m \geqslant 0$ et de mots $x \in A^+$, $y \in A^*$ tels que $g = (x\, y)^m x$, $g' = g\, y\, x$.

Soit $d = |x\, y|$. Si $j \leqslant |g|$, le mot $a_{j+1} \ldots a_{j+d}$ est facteur droit de $a_1 \ldots a_j$ ou il a ce mot comme facteur droit. Donc la période en j de w est $\leqslant d$ où $d < p$ ce qui achève la preuve puisque dans les deux cas $|g| \leqslant n - p'$.

Q.E.D.

3.2 Supposant $n \geqslant k + p$, p est la période minima de tout facteur g de w dont le support contient les indices k et $k + p$.

<u>Preuve</u>. Supposons au contraire que g a une période $p' \leqslant p$. La même chose est vraie de son facteur g' dont le support est $[k,\ p+k]$. On peut donc

supposer $g = g'$. En raison de la périodicité p on a $x = a_k = a_{p+k} \varepsilon A$. Le calcul précédent montre que $g = x\ z\ x\ y\ x\ z\ x$. De nouveau à cause de la périodicité p de w, $z\ x$ est facteur droit d'un mot de $A^* a_1 \dots a_k$. La période locale de w en k est donc $\leqslant |z\ x|$ où $|z\ x| < p$. Contradiction.

Q.E.D.

3.3 Soient h' et h'' deux facteurs gauches de h tels que $k \leqslant |h'| \leqslant |h''|$. Alors h' n'est <u>pas</u> facteur droit de h''.

<u>Preuve</u>. Sinon on aurait $h' = (x\ y)^q\ x$, $h'' = (x\ y)^r\ x$ avec $x \varepsilon A^+$, $r > q$ et w aurait donc période locale $\leqslant |x\ y| < p$ en tout $j \leqslant |h_1|$.

Q.E.D.

Afin d'appliquer le Théorème de Césari et Duval, on dira qu'un mot f <u>rencontre</u> w <u>selon l'intervalle</u> $I = [i, j]$ de $[1, n]$ $(n = |w|)$ ssi $k \varepsilon I$ et si posant $f' = I\ w$ l'une des trois éventualités mutuellement exclusives suivantes se produit:

(1) $f = f'$;

(2) $j = n$ et $f = f'g'$ avec $y' \varepsilon A^+$;

(3) $i = 1$ et $f = g\ f'$ avec $g \varepsilon A^+$;

Pour alléger le discours on parlera de rencontre <u>interne</u>, <u>droite</u> ou <u>gauche</u> selon ces trois cas et une rencontre sera <u>propre</u> si c'est une rencontre interne ou droite ou si c'est une rencontre gauche telle que $h\ f'$ n'est pas un facteur droit de f.

On conviendra que si f rencontre w selon les intervalles $I_1 = [i_1, j_1]$, $I_2 = [i_2, j_2]$ ... etc., l'indexage de ceux-ci est tel que $i_1 \leqslant i_2$ ... et $j_1 \leqslant j_2 \leqslant \dots$.

3.4 Soit f de longueur $\leqslant n$ rencontrant w en I_1 et $I_2 \neq I_1$. Alors:

(1) La rencontre I_1 est une rencontre gauche;

(2) Si I_2 est une rencontre droite, on a $2|f| > n$;

Dans le cas contraire:

(3) La différence $d = j_2 - j_1$ est un multiple de p;

(4) La rencontre I_1 est impropre quand I_2 est une rencontre gauche ou quand $d > p$;

(5) Quand I_2 est une rencontre interne, p est la période minima de f et sinon c'est celle de son facteur droit $f_2 = I_2\, w$.

Preuve. Par hypothèse on a $i_1 \leqslant i_2 \leqslant h \leqslant j_1 \leqslant j_2$ avec $i_1 = i_2$ ssi la valeur commune des deux indices est 1 et symétriquement pour $j_1 = j_2$.

Montrons d'abord que l'hypothèse que I_1 n'est pas une rencontre gauche contredit l'hypothèse que $k < P$ est un indice critique. En effet elle implique que $f_1 = I_1\, w$ et $f_2 = I_2\, w$ soient deux facteurs gauches de f et par conséquent que $d' = i_2 - i_1 > 0$ soit une périodicité de l'intervalle $[i_1 , j_2]$. Comme dans les calculs précédents, on vérifie que ceci entraine que la période locale en k soit $\leqslant d'$, ce qui est impossible puisque $i_1 < i_2 = i_1 + d' \leqslant k \leqslant p$ et par conséquent $d' \leqslant p$.

On suppose donc désormais que I_1 est une rencontre gauche. Quand I_2 est une rencontre droite on a $2\,|f| \geqslant |f_1| + |f_2| = j_1 + n+1 - j_2 > n$. Donc (1) et (2) sont établis. Désormais I_2 n'est pas une rencontre droite. Donc f_1 et f_2 sont deux facteurs droits de f et on a une équation $f_2 = g\, f_1$ où $|g| \geqslant d = j_2 - j_1$. On note f''_2 le mot de support $[1, j_2]$.

Comme w est facteur gauche d'une puissance de sa racine h, ce dernier mot a des facteurs gauches h_1 , $h_2 \neq h$ tels que $f_1 = h^r\, h$, $f_2 = h^{r'}\, h_2$. Puisque f_1 est facteur droit de f_2 qui est lui-même facteur droit

f_2' , on a $h_1 = h_2$ d'après 3.3 ce qui établit (3).

Quand I_2 est une rencontre gauche on a $f_2 = f_2'$ donc $f_2 = h^q f_1$ avec $q > 1$. Il en est de même quand $d > p$ puisque d'après (3) on a alors $d = m\, p$ avec $m \geqslant 2$. Quand tel n'est pas le cas, on a $f = f_2$ et (5) résulte de 3.2 puisque $i_2 \leqslant k$ par hypothèse et que

$$k \leqslant j_i < k + p \leqslant j_2 = j_1 + d$$

en raison de $d \geqslant p$.

Q.E.D.

On pourrait préciser un peu ce qui se produit dans le cas (2) mais je n'ai pas vu comment utiliser cette information supplémentaire pour diminuer substantiellement les valeurs numériques données dans la Proposition.

Nous supposons maintenant que w est un mot réduit.

3.5 Le mot w a au plus <u>deux</u> rencontres propres avec f <u>et</u> son inverse formel $\bar{f}$.

<u>Preuve</u>. Si f a plusieurs rencontres avec I les points (1) et (2) de la remarque précédente montrent qu'au plus une d'entre elles peut être une rencontre droite et que toutes les autres sont des rencontres gauches. Donc d'après le point (4) au plus une de ces dernières est une rencontre propre.

Supposons maintemant que $\bar{f}$ rencontre w selon l'intervalle J et f selon I et I'. Daprès (1) de 3.4 on peut supposer que I est une rencontre gauche. Donc $f = g\, f'$ où $f' = I'w$, $g \in A^+$. On a $\bar{f} = \bar{f}'\bar{g}$. Comme les intervalles I et J contiennent tous les deux k et comme l'hypothèse que w est réduit fait qu'aucun de ses intervalles ne peut être support d'un mot et de son inverse formel, on voit que Jw doit être un facteur de $\bar{g}$, ce qui implique que J soit aussi une rencontre gauche.

Appliquant le même raisonnement à I', à partir de J, montre que I' est aussi une rencontre gauche, donc qu'au plus une des rencontres I et I' peut être propre.

Q.E.D.

Nous en venons maintenant à la preuve proprement dite de la Proposition et nous considérons un $b \in B_+$ donné, les conventions étant celles introduites à la fin de la Section 2.

Soient $w \in A^+$ de longueur $n \geqslant |b\beta|$ et $s \in S(b)$. On suppose $g\ w\ g' = s^q$ où $g, g' \in A^*$ sont de longueur strictement inférieure à s. Comme dans les remarques précédentes $k < p$ est un indice critique de w et on suppose toujours que m est un entier assez grand pour que s^m soit plus long que b (c'est-à-dire que $b\beta$).

Si $p \in P_s$ le corollaire 2.1 du théorème de Nielsen implique l'existence d'une lettre $b' = b'(p)$ et de mots e, e' tels que $e\ b'e' \in E$, $p\ s^{m+q}$ est facteur gauche de $e\ b'e'$ et $|e'\beta| < |p\ s^m\ g| + k \leqslant |e'\beta| + |b'\beta|$.

On a évidement $b' \leqslant b$ et ces relations définissent une rencontre de b' (c'est-à-dire de $f = b'\beta$) avec w selon un certain intervalle I_p . L'ensemble des paires $(b'(p), I_p)$ pour p parcourant P_s a les deux propriétés essentielles suivantes:

(1) Au plus un membre de chaque paire $(b', \bar{b}')$ peut y figurer;

(2) Si $p \neq p'$ et $b'(p) = b'(p')$ on a $I_p \neq I_{p'}$.

Compte tenu de l'identité $\bar{b}'\beta = \overline{b'\beta}$, la première est la conséquence immédiate de ce que j^{m+q} est un mot réduit puisque les intervalles de rencontre ont une intersection non vide (contenant k) . La seconde résulte tout aussi immédiatement du corollaire 2.1.

Ce sera d'ailleurs notre seule référence à celui-ci hormis l'inégalité Card $(B_+) = r' \leqslant 3r - 2$.

4. Construction des groupes annexes

On revient aux notations de la section 1. En particulier V est une base de Nielsen et P est l'ensemble des facteurs gauches $\neq 1$ des mots de V. On suppose toujours H réduit c'est-à-dire que 1 est le seul facteur gauche commun des mots V.

Soit Q l'ensemble des paires (Hp, a) où a est une lettre et Hp une classe latérale contenant au moins un $p \in P$ qui se termine par a. On définit un morphisme μ de A^* dans le monoïde des fonctions $Q \longrightarrow Q$ en posant pour chaque $b \in B$ et $q = (Hp, a)$

$q.\, b\mu =$ $(Hp', b) \in Q$ si $\bar{a} \neq b$ et si la classe latérale $Hp\,b$ contient un $p' \in P \cap A^* b$;

$= \emptyset$ sinon.

Soit désormais, $K = V^*\varphi$ l'ensemble des mots réduits représentant les éléments de H.

3.1 Le morphisme μ est un morphisme syntaxique de K.

<u>Preuve</u>. On considère l'ensemble Q' formé des paires (p, a) où $a \in A$ et $p \in P \cap A^* a$ et pour chaque $q' = (p, a) \notin Q'$ et $b \in A$

on pose

$$q'.b\mu' \begin{cases} = (p', b) & \text{si } p\,b = p' \in P; \\ = (b, b) & \text{si } \bar{a} \neq b,\ p \in V \text{ et } b \in P; \\ = \emptyset & \text{sinon.} \end{cases}$$

L'hypothèse que H est réduit implique que pour chaque $b \varepsilon P \cap A$ il existe une lettre $a \neq \bar{b}$ telle $V \cap A^* a \neq \emptyset$. Il en résulte immédiatement que K est l'image inverse par μ' des mots f tels que $Q_1' . f \mu' \cap Q_1' \neq \emptyset$ où $Q_1' = Q' \cap (V \times A)$. Il suffit maintenant de vérifier que l'équivalence $(p, a) \sim (p', b)$ ssi $a = b$ et $H p = H p'$ est compatible avec la multiplication pour voir que $Q = Q'/\sim$ et $\mu = \mu'/\sim$ reconnaissent K.

Il n'existe pas de congruence $\approx$ sur Q qui soit compatible avec la reconnaissance de K et pour laquel on ait $(p, a) \approx (p', a')$ avec $H p \neq H p'$. Il faut encore vérifier que quand $H p = H p'$ et $a \neq a'$, il existe au moins une lettre b telle que un et un seul de $(p, a). b \mu$ et $(p', a'), b \mu$ est $\neq \emptyset$. Supposons qu'il n'en soit pas ainsi c'est-à-dire que ces deux produits soient des états. Comme $H p = H p'$, ils seraient le même état $(H p'', b) = q$ et l'on pourrait trouver un mot x tel que $q. x \mu \; \varepsilon \; Q \times (H \times A)$. Considérant $(p b x \; \bar{x} \bar{b} p')\varphi$, on voit que ce mot a le facteur $a \bar{a}'$. Comme il appartient à K, on en conclut que $(p. a) . \bar{a}' \mu \neq \emptyset$ alors que $(p', a') . \bar{a}' \mu = \emptyset$.

Q.E.D.

On montre sans difficulté que l'action $\mu: Q \times A^* \longrightarrow Q$ est transitive, quelle reconnait 1 et que $0 \mu^{-1}$ est le complément dans A^* des facteurs des mots de K. Il est claire qu'elle est le produit en couronne d'un monoïde de constantes dans un groupe de permutations. Le cas où H n'a qu'un nombre fini de classes latérales correspond à celui où ce produit est un produit direct, le groupe étant alors le quotient $[F]$ de l'action de F sur les classes latérales et étant le seul groupe maximal $\neq \{0\}$ dans le semigroupe $A^+ \mu$.

Dans le cas général soit $M = A^* \mu$. Nous rappelons que chaque groupe maximal S' est défini par une partie monoïde Q_S de Q telle que $Q\,M = Q_S\,M = Q_S$ et qu'il est conjugué de S' ssi il existe $m, m' \varepsilon M$ tels que $Q_S.m = Q_{S'}$; $Q_{S'} = Q_S.m'$. Il est clair qu'une partie Q_S est définie par une transversale $P_S \subset P_1$ et une lettre a, c'est-à-dire que $Q_S = \{(H\,p, a) : p \varepsilon S\}$. On dira qu'un autre groupe S' est F-conjugué de S ssi il existe un $f \varepsilon F$ tel que $P_{S'} = (P_S\,f)\varphi$. On peut montrer que si S' n'était pas conjugué de S (au sens usuel), S et S' seraient cycliques (= $S\mu^{-1}$ engendré par un seul mot et S transitif sur Q_S) et qu'il existerait S'' conjugué de S' tel que le générateur de $S''\mu^{-1}$ soit l'inverse formel de celui de $S\mu^{-1}$. Cette observation n'est pas nécessaire pour la vérification de la propriété suivante qui est une simple reformulation des définitions.

Propriété 2. Il existe une bijection naturelle entre les classes de F-conjugaisons de groupes maximaux dans $(Q, A^+\mu)$ et les classes de groupes annexes. Si la classe de (Q_S, S) correspond à celle de G, le groupe (Q_S, S) est isomorphe (en tant que groupe de permutations) au groupe quotient $[G]$ de G.

Naturellement cette bijection est celle qui est induite par μ. On notera qu'elle inverse l'inclusion: si les groupes maximaux S et S' ne sont pas conjugués et si S' est contenu dans l'idéal (de $A^*\mu$) engendré par S, il existe un groupe annexe G' correspondant à S' qui admet comme sous groupe un groupe annexe G correspondant à S et réciproquement; les groupes annexes de rang un correspondent donc à des idéaux maximaux.

Avec un peu plus de travail on pourrait montrer qu'il existe un alphabet C (de cardinalité finie bornée en fonction du seul rang r), un morphisme $\gamma: C^* \longrightarrow A^*$ et une partie locale $E' \subset C^*$ telle que $E'\gamma$ soit le plus petit sous monoïde X^+ de A^* qui contienne $\sqrt{K}$. Il résulte de ce que l'on vient de voir que le sous groupe H' de F engendré par $X^* \mu^{-1}$ contient H et au moins un membre de chaque classe des groupes annexes.

Pour conclure, considérons maintenant les sous groupes G du groupe libre F définis par la condition d'être le stabilisateur d'une transversale F_1 telle qu'au moins un $y \in G$ a la propriété que pour tout $f \in F$ on a $H f g = H f$ ssi $f \in H F_1$. Dans le cas où $[F]$ est infini, ces groupes sont évidemment les groupes annexes. Il n'en est pas de même quand $[F]$ est fini. Leurs propriétés se rattachent de façon assez évidentes aux rapports entre la H-conjugaison et la conjugaison dans F.

<u>Question</u>. Est-il possible d'associer à (H, F) un monoïde fini de façon à ce qu'une Propriété analogue à 2 soit vraie pour cette famille de sous groupes?

R E F E R E N C E S

(1) Y. CESARI et M. VINCENT, Une caractérisation des mots périodiques. Comptes Rendus Acad. Sci., Paris, 286 (1978) pp.1175-77.

(2) J.P. DUVAL, Périodes et répétitions. Theoretical Computer Science 9 (1979), pp. 17-26.

(3) S. EILENBERG, Automata, Languages and Machines. Academic Press, New York, 1974.

(4) G. LALLEMENT, Semigroups and Combinatorial Applications, J. Wiley and Sons, New York, 1979.

(5) R.C. LYNDON et P.E. SCHUPP, Combinatorial Group Theory, Springer Verlag, Berlin, 1977.