Séminaire Dubreil.
Algèbre et théorie
des nombres

J. Petresco

Sur les groupes libres. I - Identité ; théorème de Nielsen-Schreier

Séminaire Dubreil. Algèbre et théorie des nombres, tome 8 (1954-1955), exp. n° 21, p. 1-12

<http://www.numdam.org/item?id=SD_1954-1955__8__A10_0>

Faculté des Sciences de Paris

Séminaire P. DUBREIL

(ALGÈBRE et TRÉORIE DES NOMBRES)

Année 1954/55

Exposé n° 21

SUR LES GROUPES LIBRES.

I- IDENTITÉ ; THÉORÈME DE NIELSEN-SCHREIER

(Exposé de J. PETRESCO, le 18 avril 1955).

Une bonne partie des considérations qu'on fait en théorie des groupes libres sont rassemblées autour de l'énoncé très simple : " tout sous-groupe d'un groupe libre est un groupe libre ", appelé théorème de Nielsen-Schreier. La démonstration de ce théorème est moins simple ; il s'agit en effet d'indiquer un procédé de construction pour les bases libres de chaque sous-groupe H, d'un groupe libre G. On connaît deux méthodes de construction :

1) L'une, opérant directement dans H, a été d'abord utilisée par Nielsen dans le cas des groupes engendrés par un nombre fini d'éléments ; cette construction a été adaptée au cas général, à l'aide du théorème du bon ordre, par F. Levi (Math. Zeitschr. 32, 1930). Plus récemment, l'ensemble des bases libres de H, obtenues par cette méthode, est amené à un degré de généralité, probablement dernière, par H.Federer et B.Jousson (Trans. Amer. Math. Soc. 68, 1950).

2) Une deuxième méthode, qui opère à partir de représentants convenablement choisis des classes, par exemple à gauche, de G mod. H, et qui utilise l'axiome du choix, a été décrite par Schreier (Abh. math. Sem. Hamburg, 5, 1927) et améliorée par W.Hurewicz (Abh. Hamburg, 8, 1930).

Nous nous occuperons des deux méthodes de construction, tout en généralisant celle de Schreier, ainsi que d'une troisième qui opère directement dans H et utilise le théorème de Zorn, et nous montrerons (dans la deuxième partie de cet exposé) que, dans les trois cas, on obtient en fait les mêmes bases libres; celles-ci peuvent d'ailleurs être caractérisés par deux autres propriétés remarquables (sans qu'on puisse cependant en déduire l'existence).

Nos démonstration s'appuiront principalement sur une définition forte de la notion de groupe libre, qui consiste en une description complète des

relations intervenant entre les éléments de la base : les identités. Il s'agit en fait d'une solution du "problème des mots" dans le cas des groupes libres, différente de celle triviale bien connue, en ceci qu'elle n'est pas récurrente ; elle est ainsi immédiatement utilisable dans les calculs.

1. Segmentations. Soit $P = \{a_1 , a_2 , \dots , a_n\}$ une suite finie ; nous dirons que P est une n-suite et noterons $\omega(P) = n$. Si $1 \leq i \leq j \leq n$, la sous-suite $S(a_i , a_j) = \{a_k\}$, $i \leq k \leq j$, sera dite segment de P , d'extrémité à gauche a_i et d'extrémité à droite a_j ; si $\omega[S(a_i\ a_j)] = m$, nous dirons que $S(a_i\ a_j)$ est un m-segment de P . Le 1-segment $S(a_i\ a_i)$ se réduit à sa seule extrémité a_i ; on considère également le segment vide 0 .

Nous appelons segmentation de P un ensemble ρ de segment de P , tel que :

(1). Tout élément de P est extrémité d'un segment appartenant à ρ et d'un seul. Notons $S_\rho(a_i)$, le segment d'extrémité a_i , unique, appartenant à ρ .

Deux segments S_1 et S_2 de P , sont dits concordants si :

$$(2) \quad S_1 \cap S_2 = \begin{cases} S_1 \\ S_2 \\ 0 \end{cases}$$

et ρ est une segmentation concordante, si deux de ses segments sont toujours concordants.

1-1. Pour qu'une segmentation ρ de P , soit concordante, il faut et il suffit que pour chaque $S \in \rho$:

$$(2') \quad a_i \in S \longrightarrow S_\rho(a_i) \subseteq S .$$

$a_i \in S$ entraîne $S \cap S_\rho(a_i) \neq 0$, $S \not\subset S_\rho(a_i)$, donc si (2) est valable $S_\rho(a_i) \subseteq S$.

Réciproquement si $S_1 , S_2 \in \rho$ et (2') est valable, deux cas sont à distinguer :

1) une extrémité de S_1 , appartient à S_2 ; dans ce cas, d'après (1) , $S_1 = S_\rho(a_i)$ et par conséquent, d'après (2') , $S_1 \cap S_2 = S_1$.

2) les extrémités de S_1 n'appartiennent pas à S_2 ; dans ce cas, on a évidemment, soit $S_1 \cap S_2 = S_2$, soit $S_1 \cap S_2 = 0$.

1-2. Si ρ est concordante et $S \in \rho$, l'ensemble σ des $S' \in \rho$ dont une extrémité au moins appartient à S , constitue une segmentation concordante de S .

D'après 1-1 , $S' \subseteq S$, de sorte que σ est une segmentation de S , et puisque $\sigma \subseteq \rho$, elle est concordante.

1-3. Si ρ est concordante, $S \in \rho$ et $S^* \in \rho - \sigma$, l'ensemble σ^* des segments de $P - S$, de la forme $S^* \quad S$, constitue une segmentation concordante de $P - S$.(1)

D'après 1-1 , $S^* = S(a_i\ a_j) \in \rho - \sigma$ entraîne a_i , $a_j \in P - S$, de sorte que $S^* - S \in \sigma^*$ est un segment de $P - S$ de mêmes extrémités que S^*. D'après 1-2 , $a_i \in P - S$ entraîne $S^* = S_\rho(a_i) \in \rho - \sigma$, donc $S^* - S \in \sigma^*$. En tenant compte de (1) , il apparaît que σ^* est bien une segmentation de $P - S$. σ^* est d'autre part concordante, car de S_1^* , $S_2^* \in \rho - \sigma \subseteq \rho$, on déduit en appliquant (2)

$$(S_1^* - S) \cap (S_2^* - S) = (S_1^* \cap S_2^*) - S = \begin{cases} S_1^* \\ S_2^* - S \\ 0 \end{cases}$$

Nous dirons que les segmentations σ et σ^* de 1-2 et 1-3 sont les segmentations induites par ρ dans S et $P - S$, respectivement.

Une segmentation concordante ρ est un ensemble fini partiellement ordonné par $\subset$, et par conséquent elle admet des segments minimaux.

1-4. Un segment minimal de ρ est soit un 1-segment, soit un 2-segment.

Si $S(a_i\ a_j)$ est minimal dans ρ et $\omega[S(a_i\ a_j)] \geq 3$, il existe $a_k \in S(a_i\ a_j)$, avec $i < k < j$. Mais alors, d'après (1) , $S_\rho(a_k) \neq S(a_i\ a_j)$ et d'après 1-1 , $S_\rho(a_k) \subseteq S(a_i\ a_j)$, de sorte que $S_\rho(a_k) \subset S(a_i\ a_j)$, ce qui est contradictoire.

Considérons maintenant les ensembles $\{P_k\}$ et $\{S'_k\}$, $1 \leq k \leq n$, de sous-suites de P , construites par récurrence comme suit :

(a') $P_1 = P$

(b') S'_1 est un segment de P_1 avec $\omega(S'_1) = 1,2$

(a) $P_k = P_{k-1} - S'_{k-1}$

(b) S'_k est un segment de P_k avec $\omega(S'_k) = 1,2$,

et d'autre part, soit :

(c) $\rho = \{S_k\}$, l'ensemble des segments S_k de P de mêmes extrémités que S'_k .

1-5. ρ est une segmentation concordante de P , et réciproquement, pour chaque segmentation concordante ρ de P , on peut construire deux ensembles $\{P_k\}$ et $\{S'_k\}$ de sous-suites de P , satisfaisant à (a) , (b) , (c) .

On a $P_1 \supset P_2 \supset \ldots \supset P_k \supset \ldots$, de sorte que si $a_i \in P$, il existe k

(1) $S^* - S$ est la sous-suite (de P) des éléments de S^* qui n'appartiennent pas à S ; cette définition subsiste quand $S \not\subset S^*$.

avec $a_i \in P_k$ et $a_i \notin P_{k+1}$; mais puisque d'après (a) , $P_{k+1} = P_k - S'_k$, on a $a_i \in S'_k$, donc d'après (c) , a_i est extrémité de S_k . Par ailleurs, si a_i est extrémité de S_k et S_h , à la fois, et si par exemple $k < h$, on a d'après (b) et (c) , d'une part $a_i \notin P_k - S'_k = P_{k+1}$, d'autre part $a_i \in S'_h \subseteq P_h$, donc, puisque $k+1 \leq h$, $a_i \in P_{k+1}$, ce qui est contradictoire. D'après (1) , ρ est bien une segmentation de P . Enfin si $k < h$, $S_k = S(a_{i_0}\, a_{j_0})$, $S_h = S(a_i\, a_j)$ et si (2) n'est pas valable pour S_k et S_h , une extrémité de S_h , soit a_i , est telle que $i_0 < i < j_0$; mais $a_i \in S'_h \subseteq P_h \subset P_k$, c'est-à-dire qu'on a pour le segment S'_k de P_k , $\omega(S'_k) \geq 3$, contrairement à (b) .

Si maintenant on suppose la réciproque valable pour toute n'-suite avec $n' < n$, soit P une n-suite admettant une segmentation concordante ρ . Si S est un segment minimal de ρ , on a d'après 1-4 , $\omega(S) = 1,2$, et $P - S$ est une n'-suite avec $n' < n$. D'autre part, d'après 1-3 , la segmentation σ^* induite par ρ dans $P - S$ est concordante. D'après l'hypothèse, on peut donc construire les ensembles $\{P_1 , \dots , P_\ell\}$ et $\{S'_1 , \dots , S'_\ell\}$ de sous-suites de $P - S$ satisfaisant, avec σ^* , à (a) , (b) , (c) . Les ensembles de sous-suites $\{P , P_1 , \dots , P_\ell\}$ et $\{S , S'_1 , \dots , S'_\ell\}$ ainsi que la segmentation ρ , sont alors dans le même cas, relativement à P .

2. Identités. Supposons maintenant que les éléments a_i de P soient pris dans un groupe G et notons $\overline{P} = a_1\, a_2 \dots a_n$ le produit des éléments de P , dans l'ordre de P ; si R est une sous-suite de P , notons également $\overline{R}$, le produit de ses éléments dans l'ordre de P ; notons enfin S' , la sous-suite des extrémités du segment S de P . Le segment S sera dit unitaire si

$$(3) \quad \overline{S'} = 1 ,$$

et ρ sera une segmentation unitaire si ses segments sont unitaires.

2-1. Si P admet une segmentation concordante et unitaire, $\overline{P} = 1$.

Si 2-1 est vraie pour toute n'-suite avec $n' < n$, soit S un segment minimal de la segmentation concordante et unitaire ρ de la n-suite P . D'après 1-4 , $\omega(S) = 1,2$, de sorte que chaque élément de S étant extrémité, $\overline{S} = \overline{S'} = 1$. D'autre part, $P - S$, qui est une n'-suite avec $n' < n$, admet d'après 1-3 , une segmentation concordante σ^* induite par ρ , dont les segments ont mêmes extrémités que certains segments de ρ ; il s'en suit que σ^* est également unitaire, donc d'après l'hypothèse $\overline{P - S} = 1$. Si l'on pose $S = S(a_i\, a_j)$, on a par conséquent

$$\bar{P} = a_1 a_2 \cdots a_n = a_1 \cdots a_{i-1} \bar{S} a_{j+1} \cdots a_n = a_1 \cdots a_{j-1} a_{j+1} \cdots a_n =$$
$$= \overline{P - S} = 1 .$$

Par ailleurs 2-1 est triviale pour $n = 1$.

2-2. Pour qu'une segmentation concordante ρ de P soit unitaire, il faut et il suffit que pour chaque $S \in \rho$

$$(3') \qquad \bar{S} = 1$$

Si ρ est concordante et unitaire et $S \in \rho$, la segmentation σ induite par ρ dans S est, d'après 1-2 , concordante, et puisque $\sigma \subseteq \rho$, également unitaire ; d'après 2-1 , on a par conséquent $\bar{S} = 1$.

Réciproquement, ρ étant concordante et $S = S(a_i\ a_j) \in \rho$, considérons $S_\rho(a_{i+1})$; d'après (1) et 1-1 , $S_\rho(a_{i+1}) \subset S$, donc $S_\rho(a_{i+1}) = S(a_{i+1} a_{i_1})$, avec $i < i_1 < j$. Considérons alors la suite des segments $S(a_{i_k+1}\ a_{i_{k+1}})$, définie par

$$S_\rho(a_{i_k+1}) = S(a_{i_k+1}\ a_{i_{k+1}}) ;$$

d'après (1) et 1-1 on a $i < i_1 < i_2 < \ldots < i_k < \ldots < j$, et puisqu'elle est finie, $i_h = j-1$, pour un certain h . Si maintenant (3') est valable pour tout segment appartenant à ρ , $\bar{S}(a_{i_{k+1}}\ a_{i_{k+1}}) = 1$, $k = 1, 2, \ldots, h-1$, de sorte que

$$1 = \bar{S} = a_i\ \bar{S}(a_{i+1}\ a_{i_1}) \cdots \bar{S}(a_{i_{h-1}+1} a_{j-1}) a_j = a_i\ a_j = \bar{S}' ,$$

c'est-à-dire que ρ est unitaire.

Nous dirons qu'une relation $\bar{P} = a_1 a_2 \cdots a_n = 1$, $a_i \in G$, est une identité si P admet une segmentation concordante et unitaire.

2-3. Si $\bar{P} = 1$ est une identité, ρ une segmentation concordante et unitaire de P et $S \in \rho$, $\bar{S} = 1$ et $\overline{P - S} = 1$ sont également des identités.

Les segmentations concordantes induites par ρ dans S et $P - S$, étant contenues dans ρ , sont de même que ρ , unitaires, et d'après 2-1 , $\bar{S} = 1$ et $\overline{P - S} = 1$

Considérons maintenant les propositions suivantes ;

(α). $\bar{P} = 1$ est une identité

(β). $\bar{P} = 1$ est telle que P contienne un segment unitaire S , avec $\omega(S) = 1,2$.

(γ). $\bar{P} = 1$ est soit telle que $\omega(P) = 1,2$, soit telle que P contienne un segment $S \neq P$, avec $\bar{S} = 1$.

On a, en tenant compte de 1-4 , (α) $\rightarrow$ (β) $\rightarrow$ (γ) .

Soit A un sous-ensemble de G , et notons (α_A) , (β_A) , (γ_A) ,

obtenues de (α) , (β) , (γ) , en affirmant qu'elles sont valables, pour toute relation $\overline{P} = 1$, avec $a_i \in A \cup A^{-1}$.

2-4. On a les équivalences $(\alpha_A) \rightleftarrows (\beta_A) \rightleftarrows (\gamma_A)$.

$(\gamma_A) \rightarrow (\beta_A)$. Si (γ) est valable pour $\overline{P} = 1$ et $\omega(P) \geq 3$, l'ensemble des segments $S \neq P$, avec $\overline{S} = 1$, n'est pas vide, donc il contient un segment minimal S_0 , avec $\overline{S}_0 = 1$; en appliquant (γ) à $\overline{S}_0 = 1$, on déduit $\omega(S_0) = 1,2$ et $\overline{S}'_0 = \overline{S}_0 = 0$

$(\beta_A) \rightarrow (\gamma_A)$. Si $\overline{P} = 1$, supposons qu'on ait construit, comme à 1-5 , les ensembles $\{P_1 , \ldots , P_k\}$ et $\{S'_1 , \ldots , S'_k\}$ de sous-suites de P , satisfaisant à (a) et (b) et de plus que

$$(4) \quad \overline{P}_1 = \ldots = \overline{P}_k = \overline{S}'_1 = \ldots = \overline{S}'_k = 1 .$$

Prenons $P_{k+1} = P_k - S'_k$; on a, d'après (4) , $\overline{P}_{k+1} = \overline{P_k - S_k} = 1$, et par conséquent, en appliquant (β) à $\overline{P}_{k+1} = 1$, on peut également obtenir un segment S'_{k+1} de P_{k+1} avec $\omega(S'_{k+1}) = 1,2$ et $\overline{S}'_{k+1} = 1$. On déduit que (4) est valable pour tout k . Mais alors $\rho = \{S_k\}$, définie par (c) , qui d'après 1-5 , est une segmentation concordante est également telle que $\overline{S}'_k = 1$, c'est-à-dire unitaire.

Notons $[A]$ le sous-groupe engendré dans G , par le sous-ensemble A , c'est-à-dire l'ensemble des $\overline{P} = a_1 a_2 \ldots a_n$, avec $a_i \in A \cup A^{-1}$. Si $A \cap A^{-1} = 0$, et si (β_A) est valable, on dit que $[A]$ est <u>librement engendré</u> par A , ou encore que A est un <u>système libre</u>, et on écrit $[A] = [[A]]$. G est un <u>groupe libre</u>, s'il contient un sous-ensemble A tel que $G = [[A]]$, et A est appelée une <u>base libre</u> de G .

L'intérêt des équivalences 2-4 , réside dans le fait que, dans ces définitions, on peut remplacer (β) , soit par (α) , logiquement plus fort, soit par (γ) , plus faible, de sorte que, dans les démonstrations, on est conduit à utiliser (α) pour les groupes libres figurant dans l'hypothèse et (γ) pour ceux figurant dans la conclusion. De plus (α) caractérise complètement les relations survenant entre les générateurs d'un groupe libre - autrement dit elle constitue une solution du "problème des mots" dans ce cas particulier ; ceci résulte de 2-1 et 2-4 . Il n'en est pas de même pour (β) ; il existe en effet des relations $\overline{P} = 1$ avec $a_i \in A \cup A^{-1}$, ayant la propriété (β) et qui ne soient pas valables dans $[[A]]$ si $x \in A$, $x \, x \, x^{-1} = 1$, par exemple.

Retenons la définition :

(L_α). A est un système libre, si $A \cap A^{-1} = 0$ et si les seules relations $\overline{P} = 1$, avec $a_i \in A \cup A^{-1}$ sont les identités.

3. Relations irréductibles. $P = \{a_1, a_2, \dots, a_n\}$ avec $a_i \in G$ sera dite suite irréductible si $\overline{S} \neq 1$, pour chaque segment $S \subset P$; on dira dans ces mêmes conditions que $\overline{P}$ est un produit irréductible et $\overline{P} = 1$ une relation irréductible. En utilisant (γ), on déduit de 2-4 :

(L_γ). A est un système libre, si $A \cap A^{-1} = 0$, et s'il n'existe pas de relation irréductible $\overline{P} = 1$, avec $a_i \in A \cup A^{-1}$ et $\omega(P) \geq 3$.

On utilisera dans ce qui suit, soit (L_α), soit (L_γ), suivant l'opportunité.

3-1. Pour tout $\overline{P}$, avec $a_i \in G$, il existe une sous-suite P_m de P, irréductible, avec $\overline{P} = \overline{P}_m$

Si P n'est pas irréductible, il existe $S_1 \subset P$ avec $\overline{S}_1 = 1$, de sorte que $\overline{P} = \overline{P - S_1}$. Si l'on note $P_2 = P - S_1$, on a donc $\overline{P} = \overline{P}_2$. Plus généralement on construit par récurrence une chaîne stricte de sous-suites de P :

$$P \supset P_2 \supset \dots \supset P_m \supset \dots, \quad \text{avec } \overline{P} = \overline{P}_2 = \dots = \overline{P}_m = \dots$$

qui est finie, puisque P est fini, de sorte que pour un certain m, P_m est nécessairement irréductible.

3-2. Si $G = [[A]]$, tout $1 \neq a \in G$ admet une représentation unique comme produit irréductible d'éléments de $A \cup A^{-1}$.

D'après 3-1 il existe une représentation irréductible de a. Si maintenant $1 \neq a = \prod_n a_i = \prod_m b_j$, avec $a_i, b_j \in A \cup A^{-1}$ et $\prod a_i$, $\prod b_j$, irréductibles,

$$\overline{P} = \prod b_{m-j+1}^{-1} a_i = 1$$

est une identité et par conséquent P admet une segmentation ρ, concordante et unitaire. Si $S \in \rho$, on a $\overline{S} = 1$ et puisque $\prod a_i \neq 1$, $\prod b_j \neq 1$ sont irréductibles, l'extrémité à gauche de S est dans $\{b_{m-j+1}^{-1}\}$ et l'extrémité à droite dans $\{a_i\}$; enfin, en vertu de (1) et (2), $m = n$ et $S = S(b_i^{-1} a_i)$. Mais alors, puisque S est unitaire $b_i = a_i$.

Si $a = \overline{P}$ est la représentation irréductible de $1 \neq a \in G = [[A]]$, on appellera longueur $\lambda(a)$ de a, le nombre $\omega(P)$. On posera $\lambda(1) = 0$; on a évidemment $\lambda(a) = \lambda(a^{-1})$.

Si $\lambda(a) = 2m+1$, l'élément a_{m+1} de P sera dit centre de a ; si $\lambda(a) = 2m$, a_m sera le centre à gauche de a, et a_{m+1} le centre à droite.

La relation $a \sim b \rightleftarrows a = b^\varepsilon$, $\varepsilon = \pm 1$, entre les éléments de G est une équivalence. Considérons dans $P = \{a_1, a_2, \dots, a_n\}$ avec $a_i \in G$,

l'ensemble des classes relatives à cette équivalence. Si $x \in G$, P sera dit x-simple si la classe des a_i avec $a_i \sim x$, se réduit à un seul élément de P .

Si $G = [[A]]$, $\overline{P} = a_1\, a_2 \dots a_n$, $a_i \in G$ et si $a_i = \overline{\prod_j} a_{ij}$, $a_{ij} \in A \cup A^{-1}$ est la représentation irréductible de a_i , nous noterons :

$$P_A = \overline{\prod_i}\ \overline{\prod_j}\ a_{ij} \quad ;$$

on appellera longueur maximum $\ell(P)$ de P , le nombre max. $\{\lambda(a_i)\}$.

Si P_A admet une segmentation concordante et unitaire ρ , le segment minimum appartenant à ρ et contenant les centres de a_i , sera dit couverture centrale $C_\rho(a_i)$ de a_i ; il existe, en effet, des segments minimaux satisfaisant à cette condition, et si S_1 et S_2 sont dans ce cas, on a $S_1 \not\subset S_2$, $S_2 \not\subset S_1$ et puisqu'ils ont en commun les centres de a_i , $S_1 \cap S_2 = 0$; mais alors d'après (2) , $S_1 = S_2$.

Supposons maintenant que $\overline{P} = 1$ avec $a_i \in G = [[A]]$, soit une relation irréductible et $\omega(P) \geq 3$. D'après (L_α) , $\overline{P}_A = 1$ est une identité ; soit ρ la segmentation concordante et unitaire qu'admet dans ce cas P_A .

3-3. On a $a_i \sim a_k$, $C_\rho(a_i) = C_\rho(a_k) \longrightarrow i = k$.

Supposons $i < k$, $a_i \sim a_k$, $C_\rho(a_i) = C_\rho(a_k) = C_\rho$; deux cas sont à distinguer :

1) $\lambda(a_i) = \lambda(a_k) = 2m+1$. Le centre $a_{i,m+1}$ de a_i appartient à C_ρ , donc d'après 1-1 , $S_\rho(a_{i,m+1}) \subseteq C_\rho$, et puisque C_ρ est minimum dans ρ à contenir $a_{i,m+1}$, $S_\rho(a_{i,m+1}) = C_\rho$; de façon analogue $S_\rho(a_{k,m+1}) = C_\rho$. On en conclut que $C_\rho = S(a_{i,m+1}\, a_{k,m+1})$.

Si maintenant $a_i = a_k$, on a, d'une part $a_{i,m+1} = a_{k,m+1}$, d'autre part puisque C_ρ est unitaire $a_{i,m+1} = a_{k,m+1}^{-1}$; ceci contredit $A \cap A^{-1} = 0$.

Si $a_i = a_k^{-1}$, on a d'après 2-2 , $\overline{C}_\rho = 1$, donc

$$\overline{S}(a_i\, a_k) = a_{i_1} \dots a_{i_m}\, \overline{C}_\rho\, a_{k,m+2} \dots a_{k,2m+1} = a_{i_1} \dots a_{i_m}\, a_{i_m}^{-1} \dots a_{i_1}^{-1} = 1$$

$$\overline{S}(a_{i+1}\, a_{k-1}) = a_i^{-1}\, \overline{S}(a_i\, a_k)\, a_k^{-1} = a_i^{-1}\, a_i = 1$$

ce qui est incompatible avec l'hypothèse : $\overline{P} = 1$ irréductible et $\omega(P) \geq 3$.

2) $\lambda(a_i) = \lambda(a_k) = 2m$. Considérons le segment $S(a_{i,m+1}\, a_{km})$, qui n'est pas supposé appartenir à ρ . On a

(5) $\quad a \in S(a_{i,m+1}\, a_{km}) \longrightarrow S_\rho(a) \subseteq S(a_{i,m+1}\, a_{km})$.

En effet, dans le cas contraire et si $a \in S(a_{i,m+1}\ a_{km})$, $S_\rho(a)$ contient soit les centres de a_i , soit les centres de a_k , sans contenir ceux de l'autre, ce qui est incompatible avec l'hypothèse $C_\rho(a_i) = C_\rho(a_k)$

Notons $S_\rho(a_{i,m+1}) = S(a_{i,m+1}\ a_{i_1,j_1}) = S_1$; l'irréductibilité de $\prod_j a_{ij}$, (1) , (2) et (5) entraînent $i < i_1$. Pour les mêmes raisons, la suite de segments consécutifs, définie par

$$S_\rho(a_{i_h,j_h+1}) = S(a_{i_h,j_h+1}\ a_{i_{h+1},j_{h+1}}) = S_h$$

est telle que $i < i_1 < \ldots < i_h < \ldots \leq k$, et puisqu'elle est finie, $i_t = k$, pour un certain t . Considérons $S_{t-1} = S(a_{i_{t-1},j_{t-1}}\ a_{k,j_t})$; (5) entraîne $j_t \leq m$.

Si $j_t < m$, $a_{k,j_t+1} \in S(a_{i,m+1}\ a_{km})$, donc en tenant compte de (1) , (2) et (5) , $S_\rho(a_{k,j_t+1}) \subset S(a_{k_1}\ a_{k,2m})$; mais d'après 2-2 , $\bar{S}_\rho(a_{k,j_t+1}) = 1$, ce qui contredit l'hypothèse de l'irréductibilité de $\prod_j a_{kj}$.

On a par conséquent $j_t = m$, et puisque d'après 2-2 , $\bar{s}_h = 1$, $h = 1 , 2 , \ldots , t-1$,

$$\bar{S}(a_{i,m+1}\ a_{km}) = \bar{S}_1\ \bar{S}_2 \ldots \bar{S}_{t-1} = 1$$

Si $a_i = a_k$, $a_{ij} = a_{kj}$, donc

$$\bar{S}(a_i\ a_{k-1}) = a_{i_1} \ldots a_{im}\ \bar{S}(a_{i,m+1}\ a_{km})\ a_{km}^{-1} \ldots a_{k_1}^{-1} = a_{i_1} \ldots a_{im} a_{im}^{-1} \ldots a_{i_1}^{-1} = 1$$

ce qui contredit l'hypothèse $\bar{P} = 1$ irréductible et $\omega(P) \geq 3$.

Si $a_i = a_k^{-1}$, $a_{k,2m-j+1} = a_{ij}^{-1}$, donc

$$\bar{S}(a_i\ a_k) = a_{i_1} \ldots a_{i_m}\ \bar{S}(a_{i,m+1}\ a_{km})\ a_{k,m+1} \ldots a_{k,2m} = a_{i_1} \ldots a_{i_m} a_{i_m}^{-1} \ldots a_{i_1}^{-1} = 1$$

$$\bar{S}(a_{i+1}\ a_{k-1}) = a_i^{-1}\ \bar{S}(a_i\ a_k)\ a_k^{-1} = a_i^{-1}\ a_i = 1$$

ce qui est également incompatible avec cette hypothèse.

3-4. <u>Quel que soit</u> $a_\iota \in P$ <u>avec</u> $\lambda(a_\iota) = \ell(P)$, <u>il existe un segment</u> S <u>de</u> P , a_ι<u>-simple avec</u> $\lambda(\bar{S}) < \lambda(a_\iota)$

Considérons l'ensemble ρ^* (de segments appartenant à ρ) des couvertures centrales correspondant aux éléments $a \in P$, avec $a \sim a_\iota$. Soit $C_\rho(a_\varkappa)$, $a_\varkappa \sim a_\iota$ un segment minimal de ρ^* et posons $C_\rho(a_\varkappa) = S(a_{i,j+1}\ a_{kh})$;

on a $\bar{S}(a_{i,j+1}\ a_{kh}) = 1$, $a_{i,j+1}\ a_{kh} = 1$.

a) $a_\nu \sim a_\varkappa$, $i < \nu < k \longrightarrow \nu = \varkappa$.

Si $i < \nu < k$, les centres de a_ν appartiennent à $C_\rho(a_\varkappa)$, donc $C_\rho(a_\nu) \subseteq C_\rho(a_\varkappa)$ et puisque $C_\rho(a_\varkappa)$ est minimale dans ρ^* , $C_\rho(a_\nu) = C_\rho(a_\varkappa)$; si de plus $a_\nu \sim a_\varkappa$, d'après 3-3 , $\nu = \varkappa$.

Quatre cas sont à distinguer :

1) Un centre de a_i et un centre de $a_k \notin S(a_{i,j+1}\ a_{kh})$.

Dans ce cas $a_\varkappa \in S(a_{i+1}\ a_{k-1})$ et d'après a) , $S(a_{i+1}\ a_{k-1})$ est a_i-simple.

D'autre part $2[\lambda(a_i) - j] \leq \lambda(a_i) \leq \lambda(a_\iota)$, $2h \leq \lambda(a_k) \leq \lambda(a_\iota)$ de sorte que

$$\lambda(a_i) - j + h \leq \lambda(a_i)$$

et

$$\lambda[\bar{S}(a_{i+1}\ a_{k-1})] = \lambda[a_{i,\lambda(a_i)}^{-1} \cdots a_{i,j+1}^{-1}\ \bar{S}(a_{i,j+1}\ a_{kh})\ a_{kh}^{-1} \cdots a_{k_1}^{-1}]$$

$$= \lambda[a_{i,\lambda(a_i)}^{-1} \cdots a_{i,j+2}^{-1}\ a_{k,h-1}^{-1} \cdots a_{k_1}^{-1}] = \lambda(a_i) - (j+1) + h - 1 < \lambda(a_\iota)$$

On prend $S = S(a_{i+1}\ a_{k-1})$.

2) Les centres de $a_i \in S(a_{i,j+1}\ a_{kh})$ et un centre de $a_k \notin S(a_{i,j+1}\ a_{kh})$.

On a $a_\varkappa \in S(a_i\ a_{k-1})$. Par ailleurs, $C_\rho(a_i) \subseteq C_\rho(a_\varkappa)$ donc puisque $C_\rho(a_\varkappa)$ est minimal dans ρ^* , $C_\rho(a_i) = C_\rho(a_\varkappa)$; si $a_i \sim a_\varkappa$, d'après 3-3 , $i = \varkappa$. En tenant compte de également a) , on conclut que $S(a_i\ a_{k-1})$ est a_i-simple.

D'autre part $2j < \lambda(a_i) \leq \lambda(a_\iota)$, $2h \leq \lambda(a_\iota)$ de sorte que

$$j + h < \lambda(a_\iota)$$

et

$$\lambda[\bar{S}(a_i\ a_{k-1})] = \lambda(a_{i_1} \cdots a_{ij}\ a_{kh}^{-1} \cdots a_{k_1}^{-1}) \leq j + h < \lambda(a_\iota)$$

On prend $S = S(a_i\ a_{k-1})$

3) Un centre de $a_i \notin S(a_{i,j+1}\ a_{kh})$ et les centres de $a_k \in S(a_{i,j+1}\ a_{kh})$.

Ce cas est symétrique à 2) et on peut prendre $S = S(a_{i+1}\ a_k)$

4) Les centres de a_i et les centres de $a_k \in S(a_{i,j+1}\ a_{kh})$.

On montre comme à 2) et 3) que $S(a_i\ a_k)$ est a_i-simple. D'autre part $2j < \lambda(a_\iota)$, $2[\lambda(a_k) - h] < \lambda(a_k) \leq \lambda(a_\iota)$ de sorte que

$$j + \lambda(a_k) - h < \lambda(a_\iota)$$

et

$$\lambda[\bar{S}(a_i\, a_k)] = \lambda(a_{i_1} \cdots a_{ij}\, a_{k,h+1} \cdots a_{k,\lambda(a_k)}) \leq j + \lambda(a_k) - h < \lambda(a_i)$$

On prend $S = S(a_i\, a_k)$.

4. Théorème de Nielsen-Schreier. Soit $G = [[A]]$, $X \subseteq G$. On dira que X est un ensemble de Nielsen, si $X \cap X^{-1} = 0$ et si :

(N). Quel que soit le sous-ensemble fini $Y \subseteq X$, il existe $b \in Y$ avec $\lambda(b) = \ell(Y)$, tel que pour toute suite irréductible, b-simple, S , d'éléments de $Y \cup Y^{-1}$, $\lambda(\bar{S}) \geq \lambda(b)$.

D'après (L_γ) et 3-4 , on a le critère de liberté :

4-1. Un ensemble de Nielsen est un système libre.

Soit maintenant H un sous-groupe de $G = [[A]]$ et L $(a < b)$ une relation de bon ordre dans H , satisfaisant à :

$$(6) \qquad \lambda(a) < \lambda(b) \longrightarrow a < b \ .$$

Si $L(a)$ est l'ensemble des $x \in H$, avec $x < a$, a sera dit L-indécomposable si $a \notin [L(a)]$. Notons H_L , l'ensemble des éléments de H , L-indécomposables .

4-2. On a $H = [[H_L]]$; H est un groupe libre .

Il est évident que $H = [H_L]$ et $H_L \cap H_L^{-1} = 0$

Soit d'autre part $Y \subseteq H_L$ un sous ensemble fini et b l'élément maximum de Y dans le bon ordre L ; d'après (6) , $\lambda(b) = \ell(Y)$. Une suite b-simple d'éléments de $Y \cup Y^{-1}$ est de la forme

$S = \left\{ b_1^{\varepsilon_1} , \ldots , b_m^{\varepsilon_m} , b^{\varepsilon} , b_{m+1}^{\varepsilon_{m+1}} , \ldots , b_{m+n}^{\varepsilon_{m+n}} \right\}$, $b_i \in Y$, où $b_i \neq b$, donc $b_i < b$, et ε_i , $\varepsilon = \pm 1$. Si de plus $\lambda(\bar{S}) < \lambda(b)$, donc d'après (6) , $\bar{S} < b$, on déduit

$$b = (b_m^{-\varepsilon_m} \cdots b_1^{-\varepsilon_1}\, \bar{S}\, b_{m+n}^{-\varepsilon_{m+n}} \cdots b_{m+1}^{-\varepsilon_{m+1}})^{\varepsilon} \in [L(b)] ,$$

ce qui contredit $b \in Y \subseteq H_L$. On a par conséquent $\lambda(\bar{S}) \geq \lambda(b)$, pour tout S , b-simple, c'est-à-dire que H_L est un ensemble de Nielsen, et d'après 4-1 , $[H_L] = [[H_L]]$.

Nous appelons H_L , une base libre de Lévi , et notons $\mathcal{H}_L$, l'ensemble des H_L attachés à chaque bon ordre L satisfaisant à (6) .

Si $X \subseteq G$, notons $X(\lambda)$, l'ensemble des $x \in X$, avec $\lambda(x) \leq \lambda$.

Dans le cas d'un sous-groupe H de G , soit $\{\lambda_1 , \lambda_2 , \ldots , \lambda_k , \ldots\}$ l'ensemble des nombres $\lambda(a)$, avec $1 \neq a \in H$, et supposons $\lambda_1 < \lambda_2 < \ldots < \lambda_k < \ldots$ Considérons les systèmes libres

$$H_{\lambda_1} \subseteq H_{\lambda_2} \subseteq \ldots \subseteq H_{\lambda_k} \subseteq \ldots$$

définis par récurrence comme suit :

(a). H_{λ_1} est un système libre maximal tel que $H_{\lambda_1} \subseteq H(\lambda_1)$

(b). H_{λ_k} est un système libre maximal tel que $H_{\lambda_{k-1}} \subseteq H_{\lambda_k} \subseteq H(\lambda_k)$

Puisque la propriété d'un ensemble d'être un système libre est de caractère fini, l'existence des systèmes libres maximaux dont il est question dans (a) et (b) est assurée par le théorème de Zorn. Notons :

(c). $H_M = \bigcup H_{\lambda_k}$; suivant la même propriété, H_M est un système libre.

4-3. On a $H = [[H_M]]$.

Il suffit de montrer que $H \subseteq [H_M]$. Supposons que $H(\lambda_{k-1}) \subseteq [H_{\lambda_{k-1}}]$ et montrons que

$$(7) \quad H(\lambda_k) \subseteq [H_{\lambda_k}] .$$

Soit $x \in H(\lambda_k)$; si $\lambda(x) \leq \lambda_{k-1}$, on a $x \in H(\lambda_{k-1}) \subseteq [H_{\lambda_{k-1}}] \subseteq [H_{\lambda_k}]$, d'après l'hypothèse.

Si $\lambda(x) = \lambda_k$, d'après (6), $\{H_{\lambda_k}, x\}$ n'est pas libre. Soit $\bar{P} = 1$, avec $a_i \in \{H_{\lambda_k}, x\} \cup \{H_{\lambda_k}, x\}^{-1}$ une relation irréductible et telle que $\omega(P) \geq 3$. Puisque H_{λ_k} est un système libre il existe $a_i \in P$, avec $a_i = x^{\varepsilon}$, $\varepsilon = \pm 1$ et puisque $\lambda(a_i) = \lambda(x) = \lambda_k = \ell(P)$, on a d'après 3-4 une égalité de la forme

$$b_1^{\varepsilon_1} \ldots b_m^{\varepsilon_m} x^{\varepsilon} b_{m+1}^{\varepsilon_{m+1}} \ldots b_{m+n}^{\varepsilon_{m+n}} = \bar{S} \quad ; \quad \varepsilon_i , \varepsilon = \pm 1$$

où, puisque S est x-simple, $x \neq b_i \in H_{\lambda_k}$ et $\lambda(\bar{S}) < \lambda_k$, donc $\lambda(\bar{S}) \leq \lambda_{k-1}$

Mais alors $\bar{S} \in H(\lambda_{k-1}) \subseteq [H_{\lambda_{k-1}}] \subseteq [H_{\lambda_k}]$, de sorte que

$$x \in [H_{\lambda_k}] .$$

De façon analogue ($\lambda(\bar{S}) < \lambda_1$, donc $\lambda(\bar{S}) = 0$ et $\bar{S} = 1$) on montre que $H(\lambda_1) \subseteq [H_{\lambda_1}]$; (7) est donc valable pour tout k. On en déduit

$$H = \bigcup H(\lambda_k) \subseteq \bigcup [H_{\lambda_k}] = [\bigcup H_{\lambda_k}] = [H_M] .$$

On notera $\mathcal{H}_M$, l'ensemble des bases H_M.

Remarquons que la seul notion utilisée dans la construction de H_M est celle de système libre, à l'exclusion de toute autre notion auxiliaire, comme par exemple la L-indécomposabilité dans le cas de H_L.