MÉMOIRES DE LA S. M. F.

SUZANNE DIXMIER

Sur les p-groupes dont la longueur de Frattini est donnée

Mémoires de la S. M. F., tome 18 (1969)

<http://www.numdam.org/item?id=MSMF_1969__18__3_0>

Bull. Soc. math. France,
Mémoire 18, 1969, 55 p.

SUR LES p-GROUPES DONT LA LONGUEUR DE FRATTINI EST DONNÉE

par Suzanne DIXMIER (*)

-:-:-

TABLE DES MATIÈRES

(*) Thèse Sciences math., Paris 1969

CHAPITRE IV

Exposants des quotients des suites centrales ascendante et descendante .

CHAPITRE V

Retour à l'étude des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Qu'il me soit permis d'exprimer à Monsieur Michel LAZARD ma très grande gratitude pour ses conseils et pour l'aide constante qu'il a bien voulu m'accorder.

Ma reconnaissance va également à Monsieur Pierre SAMUEL qui m'a fait l'honneur de présider mon jury.

Je remercie aussi Monsieur MALLIAVIN qui a bien voulu me donner un second sujet de thèse.

CHAPITRE I

Suite p-dérivée d'un groupe. Groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

§1. Les groupes abéliens dont l'exposant divise un nombre premier p, fixé, forment une variété (que nous noterons $\mathcal{V}$), c'est-à-dire une classe de groupes contenant les sous-groupes, les images par des homomorphismes et les produits directs de groupes de la classe [10, p.33]. Il existe un moyen naturellement lié à $\mathcal{V}$ d'associer à chaque groupe G un sous-groupe $G_{p,1}$. Définissons $G_{p,1}$ comme l'intersection de tous les sous-groupes normaux N de G tels que G/N appartienne à $\mathcal{V}$.

Ce groupe $G_{p,1}$ est le plus petit sous-groupe normal de G qui soit le noyau d'un homomorphisme de G dont l'image appartienne à $\mathcal{V}$. En effet, si N_i (où i parcourt un ensemble I) est l'ensemble des sous-groupes normaux de G tels que G/N_i appartienne à $\mathcal{V}$, alors $\bigcap_{i\in I} N_i$ est un sous-groupe normal de G et $G/\bigcap_{i\in I} N_i$ est isomorphe de façon naturelle à un sous-groupe de $\prod_{i\in I} G/N_i$. On en déduit que $G/\bigcap_{i\in I} N_i$ est isomorphe à un sous-groupe d'un groupe appartenant à $\mathcal{V}$ et appartient lui-même à $\mathcal{V}$.

Nous noterons pG le sous-groupe de G engendré par les p-ièmes puissances des éléments de G et G' le groupe dérivé de G. Alors :

$$G_{p,1} = \langle pG, G' \rangle ,$$

sous-groupe de G engendré par pG et G'.

Le procédé peut se poursuivre. Nous définirons ainsi :

$$G_{p,0} = G ,$$
$$G_{p,1} = \langle pG, G' \rangle ,$$
$$G_{p,n+1} = (G_{p,n})_{p,1} \quad \text{où } n \text{ est entier et } n \geq 1 ,$$

et nous obtiendrons une chaîne de sous-groupes complètement invariants de G, qu'on appelle suite p-dérivée de G [10, p.184].

Si cette chaîne atteint l'élément neutre 1 de G au bout d'un nombre fini de termes, c'est-à-dire si $G_{p,N} = \{1\}$ pour un entier N, alors le groupe G a un exposant qui divise p^N et son n-ième groupe dérivé est réduit à l'élément neutre. Notons que si G est engendré par un nombre fini d'éléments, ceci entraîne que G est un p-groupe fini.

Si le groupe G est un p-groupe fini, le groupe $G_{p,1}$ est le sous-groupe de Frattini de G. Plus généralement, le groupe $G_{p,n+1}$ est le sous-groupe de Frattini de $G_{p,n}$ et la suite p-dérivée est la suite des sous-groupes de Frattini successifs de G ; elle atteint $\{1\}$ au bout d'un nombre fini de

termes. Nous appellerons dans ce cas longueur de Frattini de G le plus petit entier $f(G)$ tel que :

$$G_{p,f(G)} = \{1\}.$$

Les remarques suivantes seront utilisées dans la suite :

a) si H est un sous-groupe de G, alors :

$$H' \subset G' \quad \text{et} \quad pH \subset pG .$$

D'où :

$$H_{p,1} \subset G_{p,1} .$$

Plus généralement, en utilisant une récurrence, on obtient :

$$H_{p,n} \subset G_{p,n} .$$

b) si G et H sont deux groupes finis, alors :

$$(G\times H)' = G'\times H' \quad \text{et} \quad p(G\times H) = pG\times pH .$$

D'où :

$$(G\times H)_{p,1} = G_{p,1}\times H_{p,1} .$$

Plus généralement, en utilisant une récurrence, on obtient :

$$(G\times H)_{p,n} = G_{p,n}\times H_{p,n} .$$

c) si φ est un homomorphisme de G, alors :

$$\varphi(G') = (\varphi(G))' \quad \text{et} \quad \varphi(pG) = p\,\varphi(G) .$$

D'où :

$$\varphi(G_{p,1}) = (\varphi(G))_{p,1} .$$

Plus généralement, en utilisant une récurrence, on obtient :

$$(1) \quad \varphi(G_{p,n}) = \{\varphi(G)\}_{p,n} .$$

Donc les termes de la suite p-dérivée de G ont pour image les termes de la suite p-dérivée de $\varphi(G)$.

Une conséquence de cette remarque est que $(\varphi(G))_{p,n}/(\varphi(G))_{p,n+1} = \varphi(G_{p,n})/\varphi(G_{p,n+1})$ est isomorphe à un quotient du groupe $G_{p,n}/G_{p,n+1}$.

Utilisant les notations précédentes, nous pouvons tirer des remarques (a), (b), (c) les résultats qui suivent et qui concernent les longueurs des suites p-dérivées, dans le cas où celles-ci sont finies.

$$(a') \quad f(H) \leq f(G) .$$

$$(b') \quad f(G\times H) = \max(f(G),f(H)) .$$

$$(c') \quad f(\varphi(G)) \leq f(G) .$$

§2. Dans toute la suite, nous noterons $\mathcal{L}(r)$ un groupe libre à r générateurs, où r est un entier et $r \geq 1$. Appelons $a_1, a_2, \ldots, a_r$ un système libre générateur de $\mathcal{L}(r)$ et donnons-nous un groupe G à r géné-

rateurs $g_1, g_2, \dots, g_r$. Il existe un homomorphisme surjectif θ de $\mathcal{L}(r)$ sur G , défini par :

$$\theta(a_i) = g_i \qquad (i = 1, 2, \dots, r) .$$

D'après (1) :

$$G_{p,n} = \theta(\mathcal{L}(r)_{p,n}) \qquad n \text{ entier} ; \quad n \geq 0 .$$

Supposons que G soit un p-groupe fini dont la longueur de Frattini soit $f(G) \geq 0$.

Alors :

$$G_{p,f(G)} = \{1\} \quad \text{et} \quad \theta(\mathcal{L}(r)_{p,f(G)}) = \{1\}.$$

Nous en déduisons que :

$$\mathcal{L}(r)_{p,f(G)} \subset \operatorname{Ker} \theta .$$

Le groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,f(G)}$ est un groupe fini puisqu'il possède un nombre fini de générateurs, que sa suite dérivée a un nombre fini de termes et que son exposant est fini. Nous pouvons énoncer le :

Théorème 1 : Tout p-groupe fini à r générateurs et de longueur de Frattini $f(G)$ est isomorphe à un quotient du p-groupe fini :

$$\mathcal{L}(r)/\mathcal{L}(r)_{p,f(G)} .$$

L'étude de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ où n est un entier, $n \geq 0$, donnera donc des renseignements sur les p-groupes à r générateurs dont la longueur de Frattini est au plus n . On déduit, en particulier, des résultats concernant l'ordre de G et la suite centrale descendante de G . Appelons :

$c(r,n,p)$ la classe de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$,

$g(r,n,i,p)$ le nombre de générateurs du i-ème quotient de la suite centrale descendante de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$,

$e(r,n,i,p)$ l'exposant du i-ème quotient de la suite centrale descendante de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Nous pouvons énoncer la :

Proposition 1 : Soit G un p-groupe fini à r générateurs dont la longueur de Frattini est $f(G) = n$; soit c la classe de G , soient d_i le nombre de générateurs et e_i l'exposant du i-ème quotient de la suite centrale descendante de G . Alors :

l'ordre de G divise l'ordre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$;

$c \leq c(r,n,p)$;

$d_i \leq g(r,n,i,p)$;

e_i divise $e(r,n,i,p)$.

En fait, chaque quotient de la suite centrale descendante de G est isomorphe à un quotient du quotient de même indice de la suite centrale descendante de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Si $s \geq n$, il existe un homomorphisme de $\mathcal{L}(s)/\mathcal{L}(s)_{p,n}$ sur $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$. Ceci prouve que $c(r,n,p)$ est une fonction croissante de r , ainsi que $g(r,n,i,p)$ et $e(r,n,i,p)$.

On remarque aussi que le groupe G/pG est isomorphe à un quotient de $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})/p(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$.

Et encore : si g est un élément de G et si a est un élément de $\mathcal{L}(r)$ tel que $\theta(a) = g$, alors le nombre d'éléments de la classe de conjugaison de g dans G est au plus égal au nombre d'éléments de la classe de conjugaison de l'image $\bar{a}$ de a dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ dans ce groupe lui-même. En effet, si un élément $\bar{x}$ de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ centralise $\bar{a}$, son image dans G centralise g et l'indice du centralisateur de g dans G divise l'indice du centralisateur de $\bar{a}$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

CHAPITRE II

Quelques propriétés des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Les notations sont les notations du paragraphe 1 ; nous supposerons toujours $r \geq 2$.

§1. Ordre du groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Les quotients $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$ (n entier ; $n \geq 0$) sont des p-groupes abéliens élémentaires ; en particulier le groupe $\mathcal{L}(r)_{p,1}$ est d'indice fini p^r dans $\mathcal{L}(r)$.

Un sous-groupe d'un groupe libre est libre ; quand il est d'indice fini, le nombre de ses générateurs est donné par le théorème de Schreier [10, p.155].

Si $\mathcal{U}$ est un sous-groupe d'indice fini N d'un groupe libre à r générateurs, le groupe $\mathcal{U}$ est un groupe libre à $N(r-1)+1$ générateurs.

Le groupe $\mathcal{L}(r)_{p,1}$ est donc un groupe libre à $(r-1)p^r+1$ générateurs.

Notation : soit $\varphi(r, n+1, p)$ le nombre de générateurs du p-groupe abélien élémentaire $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$.

Nous venons de voir que : $\varphi(r,1,p) = r$

et : $\varphi(r,2,p) = (r-1)p^r+1$.

Etablissons une relation de récurrence entre $\varphi(r,n,p)$ et $\varphi(r, n+1, p)$ où $n \geq 1$.

Supposons que le groupe $\mathcal{L}(r)_{p,n-1}$ soit un groupe libre à $\varphi(r,n,p)$ générateurs ; alors $\mathcal{L}(r)_{p,n}$ est un groupe dont l'indice dans le précédent est fini et égal à :

$$p^{\varphi(r,n,p)} .$$

Appliquons le théorème de Schreier. Le groupe $\mathcal{L}(r)_{p,n}$ est un groupe libre et le nombre de ses générateurs est :

$$\varphi(r, n+1, p) = [\varphi(r,n,p)-1]p^{\varphi(r,n,p)}+1 .$$

D'où la relation de récurrence cherchée.

Nous pouvons exprimer l'ordre du groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$; il suffit de remarquer que :

$$|\mathcal{L}(r)/\mathcal{L}(r)_{p,n}| = \prod_{i=1}^{n} |\mathcal{L}(r)_{p,i-1}/\mathcal{L}(r)_{p,i}| .$$

Nous utilisons ici la notation habituelle : l'ordre d'un groupe fini G est $|G|$.

D'où la :

Proposition 2 : Le groupe $\mathcal{L}(r)_{p,n}$ est un groupe libre dont le nombre de générateurs $\varphi(r, n+1, p)$ est donné par la récurrence :

$$\varphi(r, 1, p) = r \quad ; \quad \varphi(r, n+1, p) = [\varphi(r,n,p)-1]p^{\varphi(r,n,p)}+1 , \quad n \geq 1$$

et
$$|\mathcal{L}(r)/\mathcal{L}(r)_{p,n}| = p^{\sum_{i=1}^{n}\varphi(r,i,p)} .$$

La croissance de $\varphi(r,n,p)$ avec l'indice n est très rapide. Par exemple :

$$\varphi(2,1,2) = 2 \quad ; \quad \varphi(2,2,2) = 2^2+1 = 5 \quad ;$$
$$\varphi(2,3,2) = 2^7+1 = 129 \quad ; \quad \varphi(2,4,2) = 2^{136}+1 > 10^{40} .$$

Remarquons que $\mathcal{L}(r)_{p,n+1}$ est un sous-groupe caractéristique de $\mathcal{L}(r)_{p,n}$ distinct de $\mathcal{L}(r)_{p,n}$ $(n = 0,1,\ldots)$. D'après le théorème de Levi [10, p.160] on a :

$$\bigcap_{n=0}^{\infty} \mathcal{L}(r)_{p,n} = \{1\} .$$

§2. Structure du quotient de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ par son groupe dérivé.

Posons dans ce paragraphe et pour simplifier $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ où n est un entier au moins égal à 1 .

Le groupe $\mathcal{G}/\mathcal{G}'$ est un p-groupe abélien à r générateurs dont la longueur de Frattini est au plus n . D'après le théorème 1 , tout p-groupe abélien à r générateurs au plus et dont la longueur de Frattini est au plus n est un quotient de $\mathcal{G}/\mathcal{G}'$.

Si nous désignons par Z_{p^n} le groupe cyclique d'ordre p^n , et si H est le produit direct de r groupes isomorphes à Z_{p^n}, alors tout p-groupe abélien à r générateurs au plus et dont la longueur de Frattini est au plus n est isomorphe à un quotient de H .
Donc $\mathcal{G}/\mathcal{G}' \simeq H$, et nous pouvons énoncer la :
Proposition 3 : Le groupe $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})/(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})'$ est le produit direct de r groupes cycliques d'ordre p^n .

Le groupe engendré par les puissances p^n-ièmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est réduit à $\{1\}$. Donc l'exposant de $\mathcal{G}$ est au plus p^n. Nous venons de voir que tout élément de $\mathcal{G}$ dont l'image dans $\mathcal{G}/\mathcal{G}'$ appartient à un système générateur libre de ce groupe est d'exposant au moins p^n . Nous en déduisons que l'exposant de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est exactement p^n. Si l'image dans $\mathcal{G}/\mathcal{G}'$ d'un élément appartient à un système générateur libre de $\mathcal{G}/\mathcal{G}'$, alors cet élément est d'ordre p^n . En particulier, l'image dans $\mathcal{G}$ de tout élément d'un système libre de générateurs de $\mathcal{L}(r)$ est d'ordre p^n .

§3. Ordre des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Dans ce paragraphe, nous étudierons l'ordre d'un élément de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ en fonction de sa position dans la suite décroissante des sous-groupes de Frattini successifs $\mathcal{L}(r)_{p,n-i}/\mathcal{L}(r)_{p,n}$ du groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ lui-même.

Le cas $n = 2$ conduit au :

Lemme 1 : Le groupe $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$ se compose des éléments x de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ tels que $x^p = 1$.

Posons pour simplifier $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$. Nous avons vu dans le paragraphe 2 que $\mathcal{G}/\mathcal{G}'$ est isomorphe au produit direct de r groupes cycliques d'ordre p^2.
L'image dans $\mathcal{G}/\mathcal{G}'$ d'un élément x de $\mathcal{G}$ d'ordre p est un élément d'ordre p de $\mathcal{G}/\mathcal{G}'$ ou l'élément neutre. Cette image est donc la puissance p-ième d'un élément de $\mathcal{G}/\mathcal{G}'$. Ceci prouve que x appartient à $\langle p\mathcal{G}, \mathcal{G}'\rangle = \mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$.

Réciproquement, tout élément de $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$ est d'ordre p ou est l'élément neutre, puisque le groupe $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$ est un p-groupe abélien élémentaire.
Une conséquence immédiate du lemme 1 est que :
$\mathcal{G} - \{\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}\}$ se compose des éléments de $\mathcal{G}$ dont l'ordre est p^2.

Etudions maintenant le cas général :

Théorème 2 : L'ensemble des solutions de $x^{p^i} = 1$ (i entier, n entier, $1 \leq n$, $0 \leq i \leq n$) dans le groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est le groupe $\mathcal{L}(r)_{p,n-i}/\mathcal{L}(r)_{p,n}$.

Faisons une récurrence sur n. Le théorème est vrai pour 1 ; supposons-le vrai jusqu'à l'entier n ; nous supposons donc en particulier que les solutions de $x^p = 1$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ sont les éléments de $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$.

Cherchons les solutions de $x^p = 1$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$. Leur image dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est un sous-ensemble de l'ensemble des solutions de $x^p = 1$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, donc un sous-ensemble de $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$. Les solutions de $x^p = 1$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$ appartiennent à $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$.

Or $\mathcal{L}(r)_{p,n-1}$ est un groupe libre à un nombre fini $\varphi(r,n,p)$ de générateurs et $\mathcal{L}(r)_{p,n+1} = (\mathcal{L}(r)_{p,n-1})_{p,2}$. D'après le lemme 1, l'ensemble des

solutions de $x^p = 1$ dans $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ est donc $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$ et l'ensemble des solutions que $x^p = 1$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$ est le sous-groupe $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$.

Faisons maintenant une récurrence sur i. Le théorème 2 est vrai pour $i = 1$; soit $2 \leq i \leq n+1$ et soit g un élément d'ordre p^i dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$. Il existe de tels éléments : par exemple, si a est un générateur de $\mathcal{L}(r)$, l'image de $a^{p^{n+1-i}}$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$ est d'ordre p^i puisque l'image de a est d'ordre p^{n+1} comme nous l'avons vu dans le paragraphe 2. Par hypothèse de récurrence :

$$g^p \in \mathcal{L}(r)_{p,n+1-(i-1)}/\mathcal{L}(r)_{p,n+1} = \mathcal{L}(r)_{p,n+2-i}/\mathcal{L}(r)_{p,n+1},$$

et $g \notin \mathcal{L}(r)_{p,n+2-i}/\mathcal{L}(r)_{p,n+1}$. Il en résulte que l'image de g dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+2-i}$ est un élément de l'ensemble des solutions dans ce groupe de $x^p = 1$; cette image appartient à $\mathcal{L}(r)_{p,n+1-i}/\mathcal{L}(r)_{p,n+2-i}$. D'où :

$$g \in \mathcal{L}(r)_{p,n+1-i}/\mathcal{L}(r)_{p,n+1}.$$

Réciproquement, si $g \in \mathcal{L}(r)_{p,n+1-i}/\mathcal{L}(r)_{p,n+1}$, sa puissance p-ième appartient à $\mathcal{L}(r)_{p,n+1-(i-1)}/\mathcal{L}(r)_{p,n+1}$ et donc est solution de $x^{p^{i-1}} = 1$, donc g est solution de $x^p = 1$.

Une conséquence du théorème 2 est que l'ordre d'un élément g de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est p^i où i est le plus petit entier tel que g appartienne à $\mathcal{L}(r)_{p,n-i}/\mathcal{L}(r)_{p,n}$.

Les solutions de $x^{p^i} = 1$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, où i est un entier fixé, forment un groupe. Nous remarquons que ceci entraîne que les solutions de $x^{p^i} = 1$ dans tout sous-groupe de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ forment elles-même un groupe.

Nous verrons plus loin, par contre, que les puissances p-ièmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ ne forment pas un groupe lorsque $n > 1$.

Enfin l'application $\varphi : x \longmapsto x^p$ envoie
$\{\mathcal{L}(r)_{p,j}/\mathcal{L}(r)_{p,n}\} - \{\mathcal{L}(r)_{p,j+1}/\mathcal{L}(r)_{p,n}\}$ dans
$\{\mathcal{L}(r)_{p,j+1}/\mathcal{L}(r)_{p,n}\} - \{\mathcal{L}(r)_{p,j+2}/\mathcal{L}(r)_{p,n}\}$ lorsque $0 \leq j \leq n-2$.

§4. Automorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Appelons $(a_1, a_2, \ldots, a_r)$ un système générateur du groupe libre $\mathcal{L}(r)$ où $r \geq 2$.

Un endomorphisme f de $\mathcal{L}(r)$ est défini par la suite $f(a_1), f(a_2), \ldots, f(a_r)$, et réciproquement, si $b_1, b_2, \ldots, b_r$ sont des

éléments distincts ou confondus de $\mathcal{L}(r)$, il existe un endomorphisme f de $\mathcal{L}(r)$ tel que $f(a_i) = b_i$, où $i = 1, 2, \ldots, r$. Chacun des groupes $\mathcal{L}(r)_{p,n}$ est stable pour tout endomorphisme f de $\mathcal{L}(r)$.
Il existe donc un homomorphisme naturel θ_n du monoïde des endomorphismes de $\mathcal{L}(r)$ dans celui des endomorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, où p est un nombre premier fixé. Cet homomorphisme est surjectif. Or, pour qu'un endomorphisme d'un p-groupe fini G soit un automorphisme, il est nécessaire et suffisant que l'endomorphisme induit sur le quotient de G par son sous-groupe de Frattini $G_{p,1}$ soit surjectif : en effet $G_{p,1}$ est l'intersection des sous-groupes maximaux de G, et l'image de G est contenue dans un sous-groupe maximal de G si et seulement si l'image de $G/G_{p,1}$ est contenue dans un sous-groupe maximal de $G/G_{p,1}$, autrement dit, si l'endomorphisme de $G/G_{p,1}$ n'est pas surjectif.
Appliquons ce résultat à $\theta_n(f)$ où f est un endomorphisme de $\mathcal{L}(r)$. Pour que $\theta_n(f)$ soit un automorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, il est nécessaire et suffisant que $\theta_1(f)$ soit un automorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,1}$.

Soit $\mathcal{E}$ l'ensemble des endomorphismes de $\mathcal{L}(r)$ dont l'image par θ_1 soit un automorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,1}$. Alors :

$$\theta_n(\mathcal{E}) = \mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$$

groupe des automorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Si m et n sont deux entiers au moins égaux à 1 tels que $m > n$, il existe un homomorphisme naturel de $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,m})$ sur $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$. En effet, tout endomorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,m}$ stabilise $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,m}$.

Il existe donc un homomorphisme naturel $\gamma_{m,n}$ du monoïde des endomorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,m}$ dans celui de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.
De plus, il est clair que :

$$\theta_n = \gamma_{m,n} \circ \theta_m$$

donc $\gamma_{m,n}$ est surjectif. Enfin, un endomorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,m}$ et son image par $\gamma_{m,n}$ induisent le même endomorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,1}$.
Si nous nous limitons aux automorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,m}$, nous voyons donc que $\gamma_{m,n}$ est un homomorphisme surjectif de $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,m})$ sur $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$. Enfin, si s est un entier tel que $s \geq m \geq n$:

$$\gamma_{s,n} = \gamma_{m,n} \circ \gamma_{s,m} \qquad \text{et} \qquad \gamma_{n,n} = \mathrm{id}.$$

Essayons d'obtenir quelques renseignements sur $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ où $n \geq 1$. D'après les remarques précédentes :

$$\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,1}) \simeq \mathrm{GL}(r,p),$$

où $\mathrm{GL}(r,p)$ est le groupe des applications linéaires d'un espace vectoriel

de dimension r sur le corps à p éléments, et il existe, pour tout entier $n \geq 1$, un homomorphisme surjectif $\gamma_{n,1}$ de $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ sur $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,1})$.

Appelons $\mathrm{Ker}\,\gamma_{n,1}$ le noyau de $\gamma_{n,1}$. Alors :

$$\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})/\mathrm{Ker}\,\gamma_{n,1} \simeq \mathrm{GL}(r,p) .$$

Le sous-groupe normal $\mathrm{Ker}\,\gamma_{n,1}$ est composé des automorphismes induisant l'identité sur $\mathcal{L}(r)/\mathcal{L}(r)_{p,1}$. Ces automorphismes sont l'image par θ_n d'éléments f de $\mathcal{E}$ tels que :

$$f(a_i) = a_i u_i \quad \text{où} \quad u_i \in \mathcal{L}(r)_{p,1} \quad \text{et} \quad i = 1, 2, \ldots, r .$$

Donc $(\theta_n \circ f)(a_i) = \theta_n(a_i)\theta_n(u_i)$ et l'élément $\theta_n(u_i)$ est un élément arbitraire de $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$. Nous obtenons ainsi la forme générale d'un élément de $\mathrm{Ker}\,\gamma_{n,1}$ et nous connaissons l'ordre de ce groupe :

$$|\mathrm{Ker}\,\gamma_{n,1}| = |\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}|^r .$$

D'où le :

Théorème 3 : Le groupe $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ contient un sous-groupe normal $\mathrm{Ker}\,\gamma_{n,1}$, tel que le quotient soit isomorphe à $\mathrm{GL}(r,p)$. Le groupe $\mathrm{Ker}\,\gamma_{n,1}$ lui-même est un p-groupe dont l'ordre est $|\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}|^r$. Tout élément de $\mathrm{Ker}\,\gamma_{n,1}$ est obtenu en choisissant pour image de chaque élément d'un système générateur minimal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ un élément arbitraire de sa classe modulo $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$.

Le noyau de $\gamma_{m,n}$, où $m > n \geq 1$, est composé des automorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,m}$ où $\theta_m(u_i)$ est un élément de $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,m}$, les notations étant celles utilisées plus haut et $i = 1, 2, \ldots, r$.

Soit maintenant G un p-groupe fini à r générateurs, c'est-à-dire que $G/G_{p,1}$ est un p-groupe abélien élémentaire, d'ordre p^r, et de longueur de Frattini n. Si $g_1, g_2, \ldots, g_r$ est un système générateur de G, il existe un homomorphisme surjectif naturel ν de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ sur G défini par :

$$(\nu \circ \theta_n)(a_i) = g_i \qquad (i = 1, 2, \ldots, r) .$$

Le noyau de ν est un sous-groupe normal $\mathcal{H}$ de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$. Soit Γ le sous-groupe de $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ qui stabilise $\mathcal{H}$. Il existe un homomorphisme naturel, qui est surjectif, de Γ sur Aut G. Le noyau Δ de cet homomorphisme se compose des éléments de Γ qui induisent l'identité sur le quotient de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ par $\mathcal{H}$. Mais $\mathcal{H}$ est un sous-groupe de $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$ puisque G possède exactement r générateurs. Donc tout élément de Δ induit l'identité sur $\mathcal{L}(r)/\mathcal{L}(r)_{p,1}$, donc appartient à $\mathrm{Ker}\,\gamma_{n,1}$. On en déduit que Δ est un p-groupe. Puisque $\mathrm{Aut}\,G \simeq \Gamma/\Delta$, alors Aut G possède un sous-groupe normal, le sous-groupe des

éléments qui induisent l'identité sur $G/G_{p,1}$ image de Ker $\gamma_{n,1} \cap \Gamma$, qui est un p-groupe, et le quotient de Aut G par ce p-groupe est isomorphe à un sous-groupe de GL(r,p). On retrouve par une méthode différente un résultat bien connu de la théorie des p-groupes finis.

Nous utiliserons dans la suite le corollaire suivant, conséquence immédiate du théorème 3 :

Corollaire 1 : Quel que soit l'élément x de $\{\mathcal{L}(r)/\mathcal{L}(r)_{p,n}\} - \{\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}\}$ et quel que soit l'indice i $(1 \leq i \leq r)$, il existe un automorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ qui applique x sur l'élément $\theta_n(a_i)$ où $a_1, \ldots, a_r$ est un système générateur de $\mathcal{L}(r)$.

§5. Quelques propriétés des sous-groupes caractéristiques.

Dans ce paragraphe, nous poserons $\theta_n(a_i) = \bar{a}_i$ si $\{a_1, a_2, \ldots, a_r\}$ est un système générateur de $\mathcal{L}(r)$ et si θ_n a la même signification que dans le paragraphe 4.

Proposition 4 : Le groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ possède un seul sous-groupe caractéristique maximal qui est $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$ (on suppose $n \geq 1$).

Il est clair que $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$ est un sous-groupe caractéristique de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$. Ce sous-groupe est même complètement invariant, c'est-à-dire qu'il est stable pour tout endomorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Soit M un sous-groupe caractéristique de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ non contenu dans $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$. Alors M contient un élément x de $\{\mathcal{L}(r)/\mathcal{L}(r)_{p,n}\} - \{\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}\}$. D'après le corollaire 1, il existe r automorphismes $\alpha_1, \alpha_2, \ldots, \alpha_r$ de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ tels que $\alpha_1(x) = \bar{a}_1$, $\alpha_2(x) = \bar{a}_2$, $\ldots$, $\alpha_r(x) = \bar{a}_r$.

Puisque x appartient au sous-groupe caractéristique M, les éléments $\alpha_i(x) = \bar{a}_i$ où $i = 1, 2, \ldots, r$ appartiennent aussi à M. Le sous-groupe M contient un système générateur de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$; il est donc lui-même le groupe entier et la proposition 4 est démontrée.

Supposons que $\mathcal{H}$ soit un sous-groupe caractéristique de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n} = \mathcal{G}$. Tout automorphisme de $\mathcal{G}$ stabilise $\mathcal{H}$; les résultats du paragraphe précédent montrent que le groupe des automorphismes de $\mathcal{G}/\mathcal{H}$ est isomorphe au groupe des automorphismes induits sur $\mathcal{G}/\mathcal{H}$ par les automorphismes de $\mathcal{G}$ lui-même ; donc Aut($\mathcal{G}/\mathcal{H}$) est isomorphe au quotient de Aut $\mathcal{G}$ par le groupe des automorphismes de $\mathcal{G}$ qui induisent l'identité sur $\mathcal{G}/\mathcal{H}$. Puisque tout automorphisme de $\mathcal{G}/\mathcal{H}$ provient de façon naturelle d'un automorphisme de $\mathcal{G}$ qui conserve $\mathcal{H}$,

c'est que tout sous-groupe caractéristique de $\mathcal{G} / \mathcal{H}$ est l'image d'un groupe caractéristique de $\mathcal{G}$ qui contient $\mathcal{H}$ et réciproquement. D'où la :

Proposition 5 : Si $\mathcal{H}$ est un sous-groupe caractéristique de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n} = \mathcal{G}$, il y a identité entre l'ensemble des sous-groupes caractéristiques de $\mathcal{G}$ qui contiennent $\mathcal{H}$ et l'ensemble des images réciproques des sous-groupes caractéristiques du groupe $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})/\mathcal{H}$.

Appliquons la proposition 5 au cas où $\mathcal{H} = \mathcal{G}'$. Nous avons vu au paragraphe 2 que $\mathcal{G} / \mathcal{G}'$ est isomorphe au produit direct de r groupes cycliques d'ordre p^n. Appelons ψ l'application de $\mathcal{G} / \mathcal{G}'$ dans lui-même définie par :

$$\psi : x \longmapsto x^p .$$

Les seuls sous-groupes caractéristiques de $\mathcal{G} / \mathcal{G}'$ sont les groupes :

$$\mathcal{G} / \mathcal{G}' \supset \psi(\mathcal{G} / \mathcal{G}') \supset \ldots \supset \psi^i(\mathcal{G} / \mathcal{G}') \supset \ldots \supset \psi^n(\mathcal{G} / \mathcal{G}') = \{1\} .$$

L'image réciproque du groupe $\psi^i(\mathcal{G} / \mathcal{G}')$ est le sous-groupe de $\mathcal{G}$ engendré par $\mathcal{G}'$ et les puissances p^i-èmes des éléments de $\mathcal{G}$ $(i = 1,2,\ldots,n)$. D'où la :

Proposition 6 : Les sous-groupes caractéristiques de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ qui contiennent le groupe dérivé $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})'$ sont les groupes $H_0 = \mathcal{L}(r)/\mathcal{L}(r)_{p,n} \supset H_1 \ldots \supset H_n = (\mathcal{L}(r)/\mathcal{L}(r)_{p,n})'$ où H_i est engendré par $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})'$ et les puissances p^i-èmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ $(i = 0, 1, \ldots, n)$.

La proposition 4 indique en particulier que tous les sous-groupes de la suite centrale descendante et ceux de la suite centrale ascendante distincts de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ appartiennent à $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$. Nous améliorerons ce résultat dans la suite.

Afin de continuer l'étude des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, nous allons étudier avec plus de détails le cas $n = 2$.

CHAPITRE III

Étude des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ où $r \geq 2$

§1. Premières propriétés.

Pour plus de commodité, nous noterons dans tout ce paragraphe :

$\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ et $\mathcal{K} = \mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$.

Le groupe $\mathcal{G}$ est métabélien. En effet $\mathcal{G}/\mathcal{K}$ est un p-groupe abélien élémentaire. Donc $\mathcal{G}'$ est un sous-groupe de $\mathcal{K}$. Le groupe $\mathcal{K}$ lui-même est un p-groupe abélien élémentaire. Donc $\mathcal{G}' = \mathcal{G}_2$ est un p-groupe abélien élémentaire.

Nous utiliserons les notations suivantes :

si $x_1, x_2, \ldots, x_n$ sont des éléments de $\mathcal{G}$, nous poserons :

$[x_2,x_1] = x_2x_1x_2^{-1}x_1^{-1}$ et $[x_n,x_{n-1}, \ldots, x_1] = [x_n,[x_{n-1}, \ldots, x_1]]$.

De plus, si n est un entier au moins égal à 0 et si x et y sont des éléments de $\mathcal{G}$, nous définirons par récurrence :

$[0x,y] = y$; $[1x,y] = [x,y]$; $[nx,y] = [x,(n-1)x,y]$ si $n > 1$.

Nous identifierons un élément a_i où $i = 1, 2, \ldots, r$ d'un système générateur $\{a_1, a_2, \ldots, a_r\}$ de $\mathcal{L}(r)$ avec son image $\theta_2(a_i)$ dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,2} = \mathcal{G}$

Nous appellerons commutateur élémentaire de poids n, où n est un entier au moins égal à 2, un élément de $\mathcal{L}(r)$ de la forme :

$[x_n,x_{n-1}, \ldots, x_1]$ où $x_i \in \{a_1, a_2, \ldots, a_r\}$.

Enfin si x et y sont deux éléments du groupe $\mathcal{G}$, nous poserons : $x_y = xyx^{-1}$.

Le groupe $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2} = \mathcal{K}$ est un sous-groupe caractéristique de $\mathcal{G}$. Tout élément g de $\mathcal{G}$ définit un automorphisme intérieur : $x \longmapsto gxg^{-1}$ de $\mathcal{G}$. Cet automorphisme intérieur induit un automorphisme de $\mathcal{K}$. Si nous utilisons pour $\mathcal{K}$ la notation additive, ce groupe $\mathcal{K}$ devient un espace vectoriel sur le corps à p élément GF(p) et g induit une application linéaire $\bar{g}$ de l'espace vectoriel $\mathcal{K}$ sur lui-même. Nous avons entre les deux notations la relation suivante : quels que soient l'élément x de $\mathcal{K}$ et l'élément g de $\mathcal{G}$ on a :

$$(2)\quad [g,x] = (gxg^{-1})x^{-1} = \bar{g}(x)-x = (\bar{g}-1)x$$

Lemme 2 : L'anneau des endomorphismes de $\mathcal{K}$ engendré par $\mathcal{G}$ est commutatif

En effet, le centralisateur de $\mathcal{K}$ dans $\mathcal{G}$ contient $\mathcal{K}$ qui est abélien et le quotient de $\mathcal{G}$ par ce centralisateur est un p-groupe abélien élémentaire qui est isomorphe au groupe des automorphismes de $\mathcal{K}$ engendrés

par les automorphismes intérieurs de $\mathcal{G}$. Quels que soient a , b dans $\mathcal{G}$ et x dans $\mathcal{K}$, on a :

$$\bar{a}\,\bar{b}\,x = \bar{b}\,\bar{a}\,x \ .$$

Lemme 3 : Si a et b appartiennent à $\mathcal{G}$ et si x appartient à $\mathcal{K}$, alors :

$$(3)\quad [a,b,x] = [b,a,x] \ .$$

Il suffit d'utiliser la relation (2) et le lemme 2 :

$$[a,b,x] = (\bar{a}-1)(\bar{b}-1)x = (\bar{b}-1)(\bar{a}-1)x = [b,a,x] \ .$$

Du lemme 3 on déduit que, si $b_1, b_2, \dots, b_n$ sont des éléments de $\mathcal{G}$ et si x appartient à $\mathcal{K}$, l'élément $[b_1, b_2, \dots, b_n, x]$ est indépendant de l'ordre dans lequel sont écrits les éléments $b_1, b_2, \dots, b_n$.
D'où le :

Corollaire 2 : Tout commutateur élémentaire de poids $n \geq 2$ a pour image dans $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ un élément de la forme :

$$[n_1 a_1 , \dots , n_r a_r , a_i , a_j]$$

où $n_1, \dots, n_r$ sont des entiers positifs ou nuls tels que $\sum_{i=1}^{r} n_i = n-2$ et $a_i, a_j \in \{a_1, \dots, a_r\}$.

Cherchons maintenant quelques relations plus précises satisfaites par les commutateurs et utilisant la condition : l'exposant de $\mathcal{K}$ est le nombre premier p ; remarquons que les relations précédemment obtenues au lemme 3 et au corollaire 2 restent valables si plus généralement le groupe $\mathcal{K}$ est un sous-groupe normal abélien d'un groupe $\mathcal{G}$ à r générateurs $a_1, a_2, \dots, a_r$ et si $\mathcal{K}$ contient $\mathcal{G}'$. Les calculs se font alors dans l'anneau des endomorphismes de $\mathcal{K}$.

Nous utiliserons la notation : $\binom{s}{t} = \dfrac{s(s-1)\dots(s-t+1)}{t!}$
où s et t sont deux entiers tels que $s \geq t \geq 1$; nous poserons $\binom{s}{0} = 1$ si s entier positif au moins égal à 0 , $\binom{s}{t} = 0$ dans tous les autres cas.

Lemme 4 : Si s est un entier positif ou nul, si x est un élément de $\mathcal{G}$ et si u est un élément de $\mathcal{K}$, alors :

$$(4)\qquad x^s u = \prod_{t=0}^{s} [tx,u]^{\binom{s}{t}} \quad , \quad t \text{ entier} \ .$$

Utilisons la notation additive :

$$x^s u = x^s u x^{-s} = \bar{x}^s u = \{(\bar{x}-1)+1\}^s u = \left\{ \sum_{t=0}^{s} \binom{s}{t} (\bar{x}-1)^t \right\} u$$

si nous remarquons que :

$$(\bar{x}-1)^t u = [tx,u]$$

et si nous revenons à la notation multiplicative, nous obtenons la formule (4).

Ce résultat est encore valable si $\mathcal{K}$ est un sous-groupe abélien normal d'un groupe $\mathcal{G}$ et si $\mathcal{K}$ contient $\mathcal{G}'$.

Lemme 5 : Si t et p sont deux entiers tels que $0 \leq t \leq p-1$, alors :

$$(5) \quad \sum_{s=0}^{p-1} \binom{s}{t} = \binom{p}{t+1} .$$

En particulier, si p est un nombre premier et si $0 \leq t \leq p-2$, alors $\sum_{s=0}^{p-1} \binom{s}{t}$ est un multiple de p .

En effet, si X est une indéterminée :

$$1 + (X+1) + \ldots + (X+1)^{p-1} = \frac{(X+1)^p - 1}{X}$$

La relation (5) s'obtient en égalant les coefficients de X^t dans chacun des deux membres. Si p est premier et $0 \leq t \leq p-2$, on sait que $\binom{p}{t+1}$ est un multiple de p .

Corollaire 3 : Si x et y sont deux éléments de $\mathcal{G}$, alors :

$$\prod_{s=0}^{p-1} {}^{x^s}[x,y] = [px,y] .$$

Posons en effet $u = [x,y]$ et utilisons les lemmes 4 et 5 et le fait que $u^p = 1$. Nous obtenons :

$$\prod_{s=0}^{p-1} {}^{x^s}[x,y] = \prod_{s=0}^{p-1} \prod_{t=0}^{s} [tx,u]^{\binom{s}{t}} = \prod_{s=0}^{p-1} \prod_{t=0}^{p-1} [tx,u]^{\binom{s}{t}} = \prod_{t=0}^{p-1} [tx,u]^{\sum_{s=0}^{p-1} \binom{s}{t}}$$

$$= \prod_{t=0}^{p-1} [tx,u]^{\binom{p}{t+1}} = [(p-1)x,u] = [(p-1)x,x,y] = [px,y] .$$

Lemme 6 : Si x et y sont deux éléments d'un groupe et si n est un entier au moins égal à 1, alors :

$$(6) \quad [x^n,y] = {}^{x^{n-1}}[x,y] \ldots {}^{x}[x,y][x,y] .$$

Il suffit de faire une récurrence sur l'entier n et d'utiliser la formule bien connue : si a, b, c sont des éléments d'un groupe, alors :

$$(7) \quad [ab,c] = {}^{a}[b,c][a,c] .$$

On obtient :

$$[x^n,y] = {}^{x}[x^{n-1},y][x,y] = {}^{x}\left({}^{x^{n-2}}[x,y] \ldots {}^{x}[x,y][x,y]\right)[x,y]$$

$$= {}^{x^{n-1}}[x,y] \ldots {}^{x}[x,y][x,y] .$$

En combinant le lemme 6, le corollaire 3 et le fait que la p-ième puissance de tout élément de $\mathcal{G}$ appartient à $\mathcal{K}$, nous obtenons le :

Corollaire 4 : Si x et y sont deux éléments de $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ alors :

$$[px,y] = \prod_{s=0}^{p-1} x^s [x,y] = [x^p,y] .$$

En particulier, si y est un élément de $\mathcal{K} = \mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$, on a :

$$[px,y] = [x^p,y] = 1 .$$

Si a, b, c sont des éléments d'un groupe, il est bien connu que :

(8) $[a, bc] = [a,b]^b[a,c]$.

Supposons que a et c appartiennent à $\mathcal{G}$ et que b appartienne à $\mathcal{K}$. Alors :

(9) $[a, bc] = [a,b]^b[a,c] = [a,b][a,c]$.

En particulier, supposons que $c = b^{-1}$:

$$1 = [a, b\, b^{-1}] = [a, b][a, b^{-1}] .$$

Nous voyons donc que si a appartient à $\mathcal{G}$ et si b appartient à $\mathcal{K}$:

(10) $[a,b]^{-1} = [a,b^{-1}]$.

Démontrons maintenant un lemme que nous utiliserons fréquemment dans la suite.

Lemme 7 : Si x et y sont deux éléments de $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$, alors :

$$[(p-1)x,(p-1)y,x,y] = 1 .$$

Utilisons les résultats précédents :

$$\begin{aligned}[(p-1)x,(p-1)y,x,y] &= [(p-1)y,(p-1)x,x,y] = [(p-1)y,px,y] \\ &= [(p-1)y,x^p,y] = [(p-1)y,y,x^p]^{-1} = [py,x^p]^{-1} \\ &= [y^p,x^p]^{-1} = 1 .\end{aligned}$$

Nous pouvons maintenant majorer la classe $c(r,2,p)$ de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$

Proposition 7 : La classe du groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ est au plus égale à :

$$r(p-1)+1 .$$

Un commutateur élémentaire a pour image dans $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ un élément de la forme :

$$z = [n_1 a_1, \ldots, n_r a_r, a_i, a_j] ,$$

où $n_1, \ldots, n_r$ sont des entiers positifs ou nuls. Posons $n = 2 + \sum_{i=1}^{r} n_i$.

si $n \geq r(p-1)+3$, l'un au moins des nombres $n_1, \ldots, n_r$ est supérieur ou égal à p et le corollaire 4 entraîne $z = 1$.

Si $n = r(p-1)+2$ et si aucun des entiers $n_1, \ldots, n_r$ n'est supé-

rieur ou égal à p, alors $n_1 = \dots = n_r = p-1$. Dans ce cas $n_i = n_j = p-1$ et le lemme 7 montre que $z = 1$.

Donc $\mathcal{G}_{r(p-1)+2} = 1$.

L'étude qui va suivre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ montrera que la classe de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ est exactement égale à $r(p-1)+1$.

Nous étudierons pour commencer le cas plus simple $r = 2$. Nous utiliserons ensuite les résultats obtenus pour $r = 2$ dans l'étude du cas général $r \geq 2$.

§2. Étude des groupes $\mathcal{L}(2)/\mathcal{L}(2)_{p,2}$.

Soient a_1 et a_2 les générateurs de $\mathcal{L}(2)$ que nous identifierons avec leur image canonique dans $\mathcal{L}(2)/\mathcal{L}(2)_{p,2}$. Nous poserons dans tout ce paragraphe $\mathcal{G} = \mathcal{L}(2)/\mathcal{L}(2)_{p,2}$ et $\mathcal{K} = \mathcal{L}(2)_{p,1}/\mathcal{L}(2)_{p,2}$.

La classe c de $\mathcal{G}$ est au plus égale à $2(p-1)+1 = 2p-1$, ainsi que l'indique la proposition 7 appliquée au cas $r = 2$. Les paragraphes II-1 et II-2 nous fournissent l'ordre de $\mathcal{G}$ et celui de $\mathcal{G}'$. Ainsi :

$$|\mathcal{G}| = p^{2+p^2+1} = p^{p^2+3} \quad \text{et} \quad |\mathcal{G}/\mathcal{G}'| = p^4.$$

D'où :

$$|\mathcal{G}'| = |\mathcal{G}| : p^4 = p^{p^2+3-4} = p^{p^2-1}.$$

Le groupe $\mathcal{G}' = \mathcal{G}_2$ est un p-groupe abélien élémentaire d'ordre p^{p^2-1} ; c'est donc un p-groupe abélien élémentaire à p^2-1 générateurs.

Si c est la classe de $\mathcal{G}$, la suite centrale descendante de $\mathcal{G}$:

$$\mathcal{G} = \mathcal{G}_1 \supset \mathcal{G}_2 \supset \dots \supset \mathcal{G}_c \supsetneq \mathcal{G}_{c+1} = \{1\},$$

permet de définir une suite de p-groupes abéliens élémentaires :

$$H_2 = \mathcal{G}_2/\mathcal{G}_3, \dots, H_i = \mathcal{G}_i/\mathcal{G}_{i+1}, \dots, H_c = \mathcal{G}_c/\mathcal{G}_{c+1} = \mathcal{G}_c$$

et le groupe $\mathcal{G}_2$ est isomorphe au produit direct des $c-1$ groupes précédents.

$$\mathcal{G} \simeq H_2 \times \dots \times H_c.$$

Si $c < 2p-1$, nous poserons $H_i = \mathcal{G}_i/\mathcal{G}_{i+1}$ si $c < i \leq 2p-1$. Alors $\mathcal{G}_i = \mathcal{G}_{i+1} = \{1\}$ et H_i est réduit à l'élément neutre. Dans ces conditions :

$$(11) \qquad \mathcal{G} \simeq H_2 \times \dots \times H_{2p-1}$$

certains facteurs (les derniers) pouvant être réduits à un élément.

Nous savons [3, pp. 151-152] que $\mathcal{G}_n$, quel que soit l'entier n au

moins égal à 1, est engendré modulo $\mathcal{G}_{n+1}$ par les images de tous les commutateurs élémentaires de poids n ; le corollaire 2 et la relation (9) indiquent que $\mathcal{G}_n$ est engendré modulo $\mathcal{G}_{n+1}$ par les éléments de la forme $[n_1a_1, n_2a_2, a_1, a_2]$ où n_1 et n_2 sont des entiers positifs ou nuls tels que $n_1+n_2 = n-2$; le corollaire 4 indique de plus que, si $\max(n_1,n_2) \geq p$, alors $(n_1a_1, n_2a_2, a_1, a_2) = 1$.

Le nombre de commutateurs élémentaires de la forme $[n_1a_1, n_2a_2, a_1, a_2]$ où $n_1+n_2 = n-2$ est égal au nombre de représentations de $n-2$ comme somme de deux entiers n_1, n_2 positifs ou nuls, l'ordre étant à considérer ; le nombre de ces représentations est $n-2+1 = n-1$; on peut en effet choisir $n_1 = 0, 1, \ldots, n-2$ et le choix de n_2 s'en déduit.

Si $p \leq n-2 \leq 2p-3$, c'est-à-dire si $p+2 \leq n \leq 2p-1$, le corollaire 4 indique que certains de ces commutateurs élémentaires ont pour image 1 dans $\mathcal{G}$. Leur nombre est le nombre de représentations de $n-2$ comme somme de deux entiers n_1, n_2 positifs ou nuls dont l'un est au moins égal à p , et l'ordre étant à considérer ; donc leur nombre est égal au double du nombre de représentations de $n-2-p$ comme somme de deux entiers positifs ou nuls, l'ordre étant à considérer, c'est-à-dire $2(n-2-p+1) = 2(n-p-1)$.

Le nombre de générateurs non triviaux de $\mathcal{G}_n/\mathcal{G}_{n+1}$ obtenus est au plus :

$$(n-1) - 2(n-p-1) = 2p-n+1 .$$

Le nombre de générateurs d'un groupe de la suite :

$$(12) \quad H_2, H_3, \ldots, H_p, H_{p+1}, H_{p+2}, \ldots, H_{2p-1}$$

est au plus égal au nombre de même rang dans la suite :

$$(13) \quad 1, 2, \ldots, p-1, p, p-1, \ldots, 2 .$$

Or la somme des termes de la deuxième suite est :

$$S = 1+2+\ldots+p-1 + p + p-1 +\ldots+2 = 2\sum_{i=1}^{p} i - (p+1) = 2\,\frac{p(p+1)}{2} - (p+1) = p^2-1.$$

De l'égalité (11) nous tirons :

$$p^{p^2-1} = |\mathcal{G}| = |H_2| \cdot |H_3| \ldots |H_{2p-1}| \leq p^s = p^{p^2-1} .$$

Nous en déduisons que S est la somme du nombre des générateurs des groupes de la suite (12), donc que la suite (13) est la suite des nombres de générateurs de la suite des groupes (12) ; en particulier $\mathcal{G}_{2p-1}$ est un p-groupe abélien élémentaire à deux générateurs et la classe de $\mathcal{G}$ est $c = 2p-1$. D'où la :

<u>Proposition 8</u> : <u>La classe de</u> $\mathcal{G} = \mathcal{L}(2)/\mathcal{L}(2)_{p,2}$ <u>est</u> $c(2,2,p) = 2p-1$.
<u>Le groupe</u> $\mathcal{G}_n/\mathcal{G}_{n+1}$ <u>est un p-groupe abélien élémentaire dont le nombre</u>

de générateurs est $n-1$ si $2 \leq n \leq p+1$ et $2p-(n-1)$ si $p+2 \leq n \leq 2p-1$, c'est-à-dire que la suite des nombres de générateurs de

$$\mathcal{G}_2/\mathcal{G}_3 ; \ldots , \mathcal{G}_{2p-1}/\mathcal{G}_{2p} = \mathcal{G}_{2p-1} \text{ est :}$$

1, 2, ... , p-1, p, p-1, ... 2 .

Quels renseignements pouvons-nous obtenir sur la suite centrale ascendante de $\mathcal{G}$? Nous savons que ses termes successifs $\{1\} = Z_0(\mathcal{G}) \subset Z_1(\mathcal{G}) \subset \ldots \subset Z_{2p-2}(\mathcal{G})$ sont tous contenus dans $\mathcal{K}$ qui est le seul sous-groupe caractéristique maximal de $\mathcal{G}$, comme l'a montré la proposition 4 .

Appelons $\sum$ l'ensemble des éléments de la base de $\mathcal{G}_2$ déterminée au début de ce paragraphe ; c'est l'ensemble des éléments de la forme $[n_1a_1, n_2a_2, a_1, a_2]$, où $0 \leq n_1 \leq p-1$; $0 \leq n_2 \leq p-1$ et où n_1 et n_2 ne sont pas tous les deux égaux à p-1.

Si nous adjoignons à $\sum$ les deux éléments a_1^p et a_2^p, nous obtenons une base de $\mathcal{K}$. Nous utiliserons les notations du paragraphe 1 .

Lemme 8 : L'homomorphisme $\bar{a}_1-1$ (resp $\bar{a}_2-1$) de $\mathcal{K}$ est une application de l'ensemble $\sum \cup \{1\}$ dans lui-même. Si deux éléments de cet ensemble ont une même image différente de 1 , c'est qu'ils sont égaux.

En effet : $(\bar{a}_1-1)([n_1a_1, n_2a_2, a_1, a_2]) = [(n_1+1)a_1, n_2a_2, a_1, a_2]$

$(\bar{a}_2-1)([n_1a_1, n_2a_2, a_1, a_2]) = [n_1a_1, (n_2+1)a_2, a_1, a_2]$;

Ces images sont toutes les deux égales à 1 si et seulement si l'on se trouve dans l'un des deux cas suivants :

$n_1 = p-1$ et $n_2 = p-2$

ou $n_1 = p-2$ et $n_1 = p-1$,

c'est-à-dire dans le cas où l'élément de $\sum$ est l'un des deux générateurs de $\mathcal{G}_{2p-1}$.

Remarquons que l'image par $\bar{a}_1-1$ ou $\bar{a}_2-1$ d'un élément de poids n de $\sum$ est 1 ou un élément de poids n+1.

Enfin : $(\bar{a}_1-1)(a_1^p) = 1 = (\bar{a}_2-1)(a_2^p)$

(14) $(\bar{a}_1-1)(a_2^p) = [a_1, a_2^p] = [a_2^p, a_1]^{-1} = [pa_2, a_1]^{-1} = [(p-1)a_2, a_1, a_2]$.

(15) $(\bar{a}_2-1)(a_1^p) = [a_2, a_1^p] = [a_1^p, a_2]^{-1} = [pa_1, a_2]^{-1} = [(p-1)a_1, a_1, a_2]^{-1}$.

L'image de a_2^p par $\bar{a}_1-1$ est un élément de $\sum$ qui n'appartient pas à $(\bar{a}_1-1)\sum$, celle de a_1^p par $\bar{a}_2-1$ est l'inverse d'un élément de $\sum$ qui

n'appartient pas à $(\bar{a}_2-1)\sum$.

Un élément y de $\mathfrak{K}$ peut s'écrire d'une façon unique sous la forme :

$$(16)\quad y = a_1^{pr_1}\, a_2^{pr_2} \prod [n_1a_1,\ n_2a_2,\ a_1,\ a_2]^{u(n_1,\ n_2)}$$

où $0 \le r_i \le p-1$ $(i = 1,2)$ et où le produit est étendu à tous les éléments de $\sum$ et $u(n_1, n_2)$ est un entier tel que $0 \le u(n_1, n_2) \le p-1$.

Déterminons le centre de $\mathcal{G}$. Il se compose des éléments y du type précédent tels que :

$$(\bar{a}_1-1)(y) = 1 = (\bar{a}_2-1)(y) .$$

Le lemme 8 et les relations (14) et (15) indiquent que $r_1 = r_2 = 0$ et que $u(n_1, n_2) = 0$ pour tout élément de $\sum$ qui n'est pas de poids $2p-1$.

Donc $Z_1(\mathcal{G}) = \mathcal{G}_{2p-1}$.

Montrons que les premiers termes de la suite centrale ascendante coïncident avec les derniers termes de la suite centrale descendante. Ceci est vrai pour $Z_1(\mathcal{G})$ et $\mathcal{G}_{2p-1}$. Faisons une récurrence.

Supposons que $Z_i(\mathcal{G}) = \mathcal{G}_{2p-i}$ où $1 \le i \le p-2$. Posons $n = 2p-i$; nous supposons donc $p+1 < n \le 2p-1$. Un élément y de la forme (16) appartient à $Z_{i+1}(\mathcal{G})$ si et seulement si son image par $\bar{a}_1-1$ et son image par $\bar{a}_2-1$ appartiennent toutes les deux à $Z_i(\mathcal{G}) = \mathcal{G}_{2p-i} = \mathcal{G}_n$; chaque facteur présent dans l'expression de y avec un exposant non nul appartient à $\sum$ et son poids est au moins égal à $n-1$; ces éléments sont les générateurs de $\mathcal{G}_{n-1} = \mathcal{G}_{2p-i-1}$ modulo $\mathcal{G}_n$; réciproquement tous ces éléments appartiennent à $Z_{i+1}(\mathcal{G})$. Donc :

$$Z_{i+1}(\mathcal{G}) = \mathcal{G}_{2p-i-1} .$$

Examinons le cas où $p \le i \le 2p-2$. Nous venons de voir que $Z_{p-1}(\mathcal{G}) = \mathcal{G}_{p+1}$. Un élément y de la forme (16) appartient à $Z_p(\mathcal{G})$ si et seulement si ne figurent avec un exposant non nul que des facteurs de poids au moins égal à p, ou a_1^p , ou a_2^p . Donc $Z_p(\mathcal{G}) = \mathcal{G}_p.\langle a_1^p, a_2^p\rangle$.

D'une façon analogue, une récurrence montre que, si $p \le i \le 2p-2$, alors

$$Z_i(\mathcal{G}) = \mathcal{G}_{2p-i}\langle a_1^p, a_2^p\rangle .$$

D'où la :

Proposition 9 : La chaîne centrale ascendante de $\mathcal{G} = \mathcal{L}(2)/\mathcal{L}(2)_{p,2}$ est la suivante :

si $1 \leq i \leq p-1$, alors $Z_i(\mathcal{G}) = \mathcal{G}_{2p-i}$;

si $p \leq i \leq 2p-2$, alors $Z_i(\mathcal{G}) = \mathcal{G}_{2p-i} \cdot \langle a_1^p, a_2^p \rangle$.

Nous voyons en particulier que $Z_{2p-2} = \mathcal{K} = \mathcal{L}(2)_{p,1}/\mathcal{L}(2)_{p,2}$.

§3. Suite centrale descendante des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ si $r \geq 2$.

Soient $a_1, a_2, \ldots, a_r$ les générateurs de $\mathcal{L}(r)$ que nous identifierons avec leur image canonique dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$. Nous poserons dans tout ce paragraphe :

$$\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2} \quad \text{et} \quad \mathcal{K} = \mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2} .$$

a- La classe $c = c(r,2,p)$ de $\mathcal{G}$ est au plus égale à $r(p-1)+1$, ainsi que l'indique la proposition 7. Les paragraphes II-1 et II-2 nous fournissent l'ordre de $\mathcal{G}$ et celui de $\mathcal{G}'$. Ainsi :

$$|\mathcal{G}| = p^r \cdot p^{(r-1)p^r+1} = p^{(r-1)p^r+r+1} \quad \text{et} \quad |\mathcal{G} / \mathcal{G}'| = p^{2r} .$$

D'où :

$$|\mathcal{G}'| = |\mathcal{G}| : p^{2r} = p^{(r-1)(p^r-1)} .$$

Le groupe $\mathcal{G}' = \mathcal{G}_2$ est un p-groupe abélien élémentaire d'ordre $p^{(r-1)(p^r-1)}$; c'est donc un p-groupe abélien élémentaire à $(r-1)(p^r-1)$ générateurs. La suite centrale descendante de $\mathcal{G}$:

$$\mathcal{G} = \mathcal{G}_1 \supset \mathcal{G}_2 \supset \ldots \supset \mathcal{G}_c \supsetneq \mathcal{G}_{c+1} = 1$$

est telle que chaque quotient $\mathcal{G}_i/\mathcal{G}_{i+1}$ $(1 \leq i \leq c)$ est abélien. Posons $H_i = \mathcal{G}_i/\mathcal{G}_{i+1}$ $(1 \leq i \leq c)$. Formons le produit direct :

$$G = H_1 \times H_2 \times \ldots \times H_c$$

suivant la méthode utilisée pour associer un anneau de Lie gradué au groupe nilpotent $\mathcal{G}$ [9 ; I, 2] ; nous nous intéresserons seulement à la structure de groupe abélien sur $H = H_2 \times \ldots \times H_c$. Chacun des facteurs $H_2, \ldots, H_c$ de H est un p-groupe abélien élémentaire dont le nombre de générateurs est $g(r,2,n,p)$ avec les notations introduites I-2 . Nous savons que

$$\mathcal{G}_2 \simeq H_2 \times \ldots \times H_c .$$

Donc :

$$\sum_{n=2}^{c} g(r,2,n,p) = (r-1)(p^r-1)$$

Si $c < r(p-1)+1$, nous introduisons $H_{c+1} = \ldots = H_{r(p-1)+1} = \{1\}$ et enfin $H_{r(p-1)+2} = \{1\}$.

En posant $g(r,2,n,p) = 0$ si $c < n \leq r(p-1)+2$, nous obtiendrons les relations

$$(17) \qquad H = H_2 \times \dots \times H_{r(p-1)+2} \simeq \mathcal{G}_2 \cdot$$

$$(18) \qquad \sum_{n=2}^{r(p-1)+2} g(r,2,n,p) = (r-1)(p^r-1) \cdot$$

Appelons $N(r,n,p)$ le nombre d'éléments de $\mathcal{L}(r)$ de la forme :

(B_n) : $[n_1a_1, \dots, n_ra_r, a_i, a_j]$

où $0 \leq n_i \leq p-1$ (n_i entier, $1 \leq i < j \leq r$, tels que : $\sum_{i=1}^{r} n_i = n-2$; n entier, $2 \leq n \leq r(p-1)+2$) .

Formons le p-groupe abélien élémentaire $K_n(r)$ à $N(r,n,p)$ générateurs, que nous identifierons aux éléments (B_n) de $\mathcal{L}(r)$.
Il existe un homomorphisme $f_n(r)$ de $K_n(r)$ sur $H_n(r)$, l'image de $[n_1a_1, \dots, n_ra_r, a_i, a_j]$ étant son image naturelle dans $\mathcal{G}_n / \mathcal{G}_{n+1}$.
Si nous posons :

$$K(r) = K_2(r) \times \dots \times K_{r(p-1)+2}(r) ,$$

il existe un homomorphisme naturel $f(r)$ de $K(r)$ sur H , qui est l'homomorphisme tel que $f_{|K_n}(r) = f_n(r)$ $(n + 2, \dots, r(p-1)+2)$.

Le nombre des éléments (B_n) où $2 \leq n \leq r(p-1)+2$ est $p^r.\binom{r}{2}$ puisque chaque coefficient n_i $(1 \leq i \leq r)$ est susceptible de prendre n'importe quelle valeur entre 0 et p-1, et qu'il existe $\binom{r}{2}$ choix possibles pour les couples (i, j). Donc le nombre de générateurs du p-groupe abélien élémentaire $K(r)$ est $p^r.\binom{r}{2}$.

Supposons que nous ayons trouvé $\rho(r,n,p)$ éléments linéairement indépendants de $K_n(r)$ et qui appartiennent au noyau de $f_n(r)$. Alors :

$$g(r,2,n,p) \leq N(r,n,p) - \rho(r,n,p) .$$

Si de plus :

$$\sum_{n=2}^{r(p-1)+2} \{N(r,n,p) - \rho(r,n,p)\} = (r-1)(p^r-1) ,$$

nous aurons prouvé que le nombre de générateurs $g(r,2,n,p)$ de $H_n(r) = \mathcal{G}_n / \mathcal{G}_{n+1}$ est exactement $N(r,n,p)$; et si enfin $g(r,2,n,p)+1, p) > 1$, nous aurons prouvé que la classe de $\mathcal{G}$ est $r(p-1)+1$.

Nous ferons une récurrence sur le nombre de générateurs r de $\mathcal{G}$.
Si $r = 2$, nous avons vu au paragraphe 2 que nous pouvions choisir :

$$\rho(2,n,p) = 0 \qquad \text{si } 2 \leq n \leq 2p-1$$

et $\rho(2,2p,p) = 1$, car l'élément $[(p-1)a_1, (p-1)a_2, a_1, a_2]$

a pour image 1 dans $H_{2p}(2)$. Alors :

$$\sum_{n=2}^{2p} [N(2,n,p) - \rho(2,n,p)] = p^2-1$$

et $g(2,2p-1,p) = 2 > 1$

Supposons donc que l'étude de $\mathcal{L}(r-1)/\mathcal{L}(r-1)_{p,2}$ (où $r \geq 3$) nous ait permis de trouver $(r-1)(p-1)+1$ nombres entiers positifs ou nuls $g(r-1,n,p)$ où $n = 2,\ldots,(r-1)(p-1)+2$, ayant la signification indiquée plus haut et tels que

$$\sum_{n=2}^{(r-1)(p-1)+2} \rho(r-1,n,p) = \{ \sum_{n=2}^{(r-1)(p-1)+2} N(r-1,n,p)\} - (r-2)(p^{r-1}-1)$$

$$(R) \qquad = \binom{r-1}{2} p^{r-1} - (r-2)(p^{r-1}-1) = \binom{r-2}{2} p^{r-1}+r-2 .$$

Supposons en outre que les $g(r-1,n,p)$ relations entre images de produits de commutateurs élémentaires de $\mathcal{L}(r-1)$ aient été obtenues en utilisant seulement le corollaire 2 p. 18 , le corollaire 4 p.20 et le lemme 7 p. 20.

Si $\mathcal{L}(r)$ est un groupe libre ayant pour système générateur $\{a_1, a_2, \ldots, a_r\}$, le sous-groupe engendré par $\{a_2, \ldots, a_r\}$ est un groupe libre à $r-1$ générateurs. Les éléments (B_n) de $\mathcal{L}(r)$ pour lesquels $n_1 = 0$ et $i \neq 1$, appartiennent à $\langle a_2, \ldots, a_r \rangle$; le groupe $K_n(r-1)$ peut ainsi naturellement être plongé dans $K_n(r)$. Les $g(r-1,n,p)$ éléments linéairement indépendants de $K_n(r-1)$ qui ont pour image par $f_n(r-1)$ l'élément neutre de $H_n(r-1)$, considérés comme éléments de $K_n(r)$ ont pour image par $f_n(r)$ l'élément neutre de $H_n(r)$.

Cherchons des éléments de $K_n(r)$, n'appartenant pas $K_n(r-1)$ dont l'image par $f_n(r)$ soit 1 . Nous utiliserons pour cela le corollaire 4, le lemme 7 et la relation de Ph. Hall qui est la suivante :

Si x, y et z sont des éléments d'un groupe G :

$$[{}^z x,y,z].[{}^y z,x,y].[{}^x y,z,x] = 1 .$$

D'où

$$[x,y,z][z,x,y][y,z,x] \equiv 1 \mod G_4 .$$

Cette relation est d'une grande importance dans la méthode qui permet d'associer un anneau de Lie gradué à certaines suites de sous-groupes d'un groupe [8, Ch 1]. Ici elle devient :

$$(19) \quad [x,y,z][z,x,y][y,z,x] = 1$$

car $[{}^z x,y,z] = [\,[z,x]x,y,z] = {}^{[z,x]}[x;y;z].[\,[z,x],y,z]$

$$= [x,y,z]$$

La relation (19) nous permettra d'écrire des relations :

$$(C_n)\quad (f_n(r))\ \{[\ldots,n_ia_i,\ldots,n_ja_j,\ldots,(n_k+1)a_k,\ldots,a_i,a_j].[\ldots,n_ia_i,\ldots,(n_j+1)a_j,\ldots,n_ka_k,\ldots,a_i,a_k]^{-1}$$
$$[\ldots,(n_i+1)a_i,\ldots,n_ja_j,\ldots,n_ka_k,\ldots,a_j,a_k]\} = 1$$

où les points représentent des termes de la forme n_ta_t, d'indices distincts, où $a_t \in \{a_1,\ldots,a_r\} - \{a_i, a_j, a_k\}$, où n_i, n_j, n_k, n_t sont des entiers compris entre 0 et p-1 , où $\sum_{s=1}^{r} n_s = n-3$ et $i < j < k$.

Si l'un au moins des entiers n_i, n_j, n_k est égal à p-1 , le corollaire 4 montre que l'un au moins des facteurs de (C_n) a une image par $f_n(r)$ égale à 1 .

A chacun des éléments de $K_n(r)$ de la forme :

(B'_n) $[(n_1+1)a_1,\ldots,n_ja_j,\ldots,n_ka_k,\ldots,a_j,a_k]$ où $\sum_{s=1}^{r} n_s = n-3$;

$0 \leq n_1 \leq p-2$ et $1 < j < k \leq r$, nous pouvons associer l'élément :

$$X(n_1,\ldots,n_r,j,k) = [n_1a_1,\ldots,n_ja_j,\ldots,(n_k+1)a_k,\ldots,a_1,a_j][n_1a_1,\ldots,(n_j+1)a_j,\ldots,n_ka_k,\ldots,a_1,a_k]^{-1}.\ [(n_1+1)a_1,\ldots,n_ja_j,\ldots,n_ka_k,a_j,a_k]$$

La relation de Ph. Hall indique que :

$$\{f_n(r)\}\ X(n_1,\ldots,n_r,j,k) = 1 .$$

Le nombre total d'éléments $X(n_1,\ldots,n_r,j,k)$ lorsque $1 + \sum_{s=1}^{r} n_s$ varie de 1 à r(p-1) est clairement :

$$\binom{r-1}{2}\, p^{r-1}(p-1) .$$

A chacun des éléments de $K_n(r)$ de la forme :

(B''_n) $[(p-1)a_1,\ldots,n_ja_j,\ldots,n_ka_k,\ldots,a_1,a_j]$ où $\sum_{s=2}^{r} n_s = n-2-(p-1)$ et où il existe un entier k supérieur strictement à j pour lequel $n_k \neq 0$; nous associons l'élément :

$$Y(n_2,\ldots,n_r,j) = [(p-1)a_1,\ldots,n_ja_j,\ldots,n_ka_k,a_1,a_j][(p-1)a_1,\ldots,(n_j+1)a_j,\ldots,(n_k-1)a_k,a_1,a_k]^{-1}$$

où k est le plus grand entier tel que $n_k \neq 0$ dans l'élément $[(p-1)a_1,\ldots,n_ja_j,\ldots,n_ka_k,\ldots,a_1,a_j]$ choisi de la forme (B''_n) .
D'après la relation de Ph. Hall $\{f_n(r)\}\ \{Y(n_2,\ldots,n_r,j)\} = 1$.

Si j est fixé, tel que $2 \leq j \leq r$, le nombre total des éléments du type (B''_n) où n varie de 2 à r(p-1)+2 est : $p^{r-1} - p^{j-1}$.

Enfin si :

(B'''_n) $Z(n_2,\ldots,n_{j-1},j) = [(p-1)a_1,\ldots,n_ia_i,\ldots,(p-1)a_j,a_1,a_j]$ où

$\sum_{s=2}^{j-1} n_s = n-2-2(p-1)$ et $j \neq 1$, le lemme 7 indique que

$$(f_n(r))\ \{Z(n_2,\dots,n_{j-1},j)\} = 1 .$$

Si j est fixé, tel que $2 \leq j \leq r$, le nombre total des éléments du type (B_n''') où n varie de 2 à $r(p-1)+2$ est : p^{j-2}.

Si j est fixé, le nombre total d'éléments $Y(n_2,\dots,n_r,j)$ et $Z(n_2,\dots,n_{j-1},j)$ est : $p^{r-1} - p^{j-1} + p^{j-2}$.

Faisons varier j de 2 à r. Nous avons obtenu au total s_r éléments, appartenant chacun à l'un des $K_n(r)$ et tels que leur image par l'homomorphisme $f_n(r)$ correspondant soit l'élément neutre ; et

$$s_r = \sum_{j=2}^{r} (p^{r-1} - p^{j-1} + p^{j-2}) = (r-1)p^{r-1} - \sum_{j=1}^{r-1} p^j + \sum_{j=0}^{r-2} p^j .$$

$$= (r-1)p^{r-1} - p^{r-1} + 1 = (r-2)p^{r-1} + 1 .$$

Pour un n fixé, les éléments faisant intervenir seulement $a_2,\dots,a_r$, trouvés au préalable, les éléments $X(n_1,\dots,n_r,j,k)$, $Y(n_2,\dots,n_r,j)$ et $Z(n_2,\dots,n_{j-1},j)$ sont linéairement indépendants dans $K_n(r)$ puisque les premiers sont linéairement indépendants et que les éléments des trois derniers types possèdent chacun un facteur qui leur est propre (facteurs du type (B_n') ou (B_n''), ou (B_n''')). Appelons $\rho(r,n,p)$ le nombre des éléments de ces quatre types pour n fixé. Alors :

$$\sum_{n=2}^{r(p-1)+2} \rho(r,n,p) = \sum_{n=2}^{(r-1)(p-1)+2} \rho(r-1,n,p) + \binom{r-1}{2} p^{r-1}(p-1)+(r-2)p^{r-1} + 1$$

$$= \binom{r-2}{2} p^{r-1} + r-2 + \binom{r-1}{2} p^{r-1}(p-1)+(r-2)p^{r-1} + 1$$

$$= \binom{r-1}{2} p^r + r-1 .$$

La fonction $\rho(r,n,p)$ de l'entier n (compris entre 2 et $r(p-1)+2$) que nous venons de déterminer, satisfait à la relation obtenue à partir de la relation (R) en y remplaçant r par $r+1$.

Le noyau de $f_n(r)$ est engendré par les $\rho(r,n,p)$ éléments des quatre types indiqués plus haut et correspondant au poids n fixé. Le noyau de la restriction de $f_n(r)$ à $K_n(r-1)$ est de même dimension que le noyau de $f_n(r-1)$. Ceci indique que l'intersection de $\mathcal{G}_n$ avec $\langle a_2, \dots, a_r\rangle$ est exactement le n-ième terme $\langle a_2,\dots,a_r\rangle_n$ de la suite centrale descendante de $\langle a_2,\dots,a_r\rangle$.

Déterminons explicitement un système libre de générateurs de $\mathcal{G}_2$ qui soit formé d'images dans $\mathcal{G}$ de commutateurs élémentaires de $\mathcal{L}(r)$, et tels que les images des commutateurs de poids n dans $\mathcal{L}(r)$ dans ce

système, forment un système libre de générateurs de $\mathcal{G}_n / \mathcal{G}_{n+1} \simeq H_n(r)$.

La récurrence précédente permet de remarquer qu'on obtient des éléments indépendants des deux types suivants :

(I) $[(p-1)a_s,\ldots,n_j a_j,a_s,a_j]$ où $1 \leq s < j \leq r$ et $n_j \not\equiv p-1$

(II) $[n_s a_s,\ldots,n_r a_r,a_s,a_j]$ où $1 \leq s < j \leq r$ et $n_s \not\equiv p-1$

Les éléments (B'_n), (B''_n), (B'''_n) et les éléments de type (I), (II), pour $s = 1$, forment, avec l'ensemble des éléments de type (B_n) où a_1 n'intervient pas, un ensemble de systèmes générateurs pour les quotients successifs $\mathcal{G}_n / \mathcal{G}_{n+1}$ $(n \geq 2)$. Les éléments de type (B'_n), (B''_n), (B'''_n) s'expriment en fonction des autres éléments de ces systèmes ; on peut les exclure des systèmes générateurs. Supposons que les éléments de type (I) et (II) où $s > 1$ forment un ensemble de systèmes générateurs des quotients $H_n(r-1)$. Nous voyons que les éléments de type (I) ou (II) forment un ensemble de systèmes générateurs des quotients $\mathcal{G}_n / \mathcal{G}_{n+1}$ $(n \geq 2)$.

Le nombre d'éléments du type (I) est :

$$\sum_{s=1}^{r-1} \left\{ \sum_{j=s+1}^{r} p^{j-s-1}(p-1) \right\} = \sum_{s=1}^{r-1} \left\{ \sum_{j=s+1}^{r} p^{j-s} - \sum_{j=s+1}^{r} p^{j-s-1} \right\}$$

$$= \sum_{s=1}^{r-1} (p^{r-s}-1) = \left(\sum_{i=0}^{r-1} p^i \right) - r .$$

Le nombre d'éléments du type (II) est :

$$\sum_{s=1}^{r} (r-s)p^{r-s}(p-1) = \sum_{s=1}^{r} (r-s)(p^{r-s+1} - p^{r-s}) = \sum_{s=1}^{r} (r-s+1)p^{r-s+1} - \sum_{s=1}^{r} p^{r-s+1}$$

$$- \sum_{s=1}^{r} (r-s)p^{r-s} = \sum_{j=1}^{r} j\, p^j - \sum_{j=0}^{r-1} j\, p^j - \sum_{i=1}^{r} p^i = r\, p^r - \sum_{i=1}^{r} p^i .$$

Le nombre total d'éléments des types (I) et (II) est :

$$\left(\sum_{i=0}^{r-1} p^i \right) - r + r\, p^r - \sum_{i=1}^{r} p^i = 1 - r + r\, p^r - p^r = (r-1)(p^r-1) ,$$

qui est la dimension de $\mathcal{G}_2$ considéré comme espace vectoriel sur le corps à p éléments.

Donc l'ensemble des éléments de $\mathcal{G}_2$ images de commutateurs élémentaires de $\mathcal{L}(r)$ des types (I) et (II) forme un système libre (S_r) de générateurs de $\mathcal{G}_2$ et les images des éléments de poids n de ce système générateur forment un système libre de générateurs de $\mathcal{G}_n / \mathcal{G}_{n+1}$.

Choisissons en particulier $n = r(p-1)+1$. Les éléments de (S_r) qui engendrent $\mathcal{G}_{r(p-1)+1}$ sont, suivant les deux types :

l'élément : $[(p-1)a_1,\ldots,(p-1)a_{r-1}, (p-2)a_r,a_1,a_r]$

les $r-1$ éléments : $[(p-2)a_1,(p-1)a_2,\ldots,(p-1)a_r,a_1,a_j]$ où $2 \leq j \leq r$.

Au total, nous obtenons r générateurs. Donc $\mathcal{G}_{r(p-1)+1}$ est un p-groupe abélien élémentaire à r générateurs. Nous pouvons énoncer le :

Théorème 4 : La classe de $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ est $r(p-1)+1$ $(r \geq 2)$. Le groupe $\mathcal{G}_{r(p-1)+1}$ est un p-groupe abélien élémentaire à r générateurs. On obtient un système libre générateur de $\mathcal{G}_n/\mathcal{G}_{n+1}$ où $2 \leq n \leq r(p-1)+1$ en prenant les éléments :

(I) $[(p-1)a_s,\ldots,n_ja_j,a_s,a_j]$ où $1 \leq s < j \leq r$; $n_j \neq p-1$ et $\sum_{i=s+1}^{r} n_i = n-2-(p-1)$,

(II) $[n_sa_s,\ldots,n_ra_r,a_s,a_j]$ où $1 \leq s < j \leq r$; $n_s \neq p-1$ et $\sum_{i=s}^{r} n_i = n-2$

où $a_1,\ldots,a_r$ sont les images dans $\mathcal{G}$ par l'application canonique d'un système générateur de $\mathcal{L}(r)$.

b - Le théorème 4 fournit explicitement un système générateur libre de $\mathcal{G}_n/\mathcal{G}_{n+1}$ où $2 \leq n \leq r(p-1)+1$, considéré comme espace vectoriel sur le corps à p éléments. Nous pouvons, en comptant le nombre d'éléments dans un tel système, déterminer la dimension de $\mathcal{G}_n/\mathcal{G}_{n+1}$.

Notations : Nous utiliserons les conventions suivantes :

$\omega(n,s)$ est le nombre de représentations de l'entier n comme somme de s entiers positifs ou nuls, l'ordre des termes étant pris en considération. $\overline{\omega}(n,s,p)$ est le nombre de représentations de l'entier n comme somme de s entiers $n_1,n_2,\ldots,n_s$, l'ordre des termes étant pris en considération et $0 \leq n_i \leq p-1$ où p est un entier au moins égal à 2 fixé.

Le nombre d'éléments de type (I), de poids n fixé et où $s = 1$ est :

$$(20)\quad \alpha(r,n,p) = \sum_{j=2}^{r} \{\overline{\omega}(n-2-(p-1),j-1,p)-\overline{\omega}(n-2-2(p-1),j-2,p)\}$$
$$= \sum_{j=2}^{r} \{\overline{\omega}(n-1-p,j-1,p)-\overline{\omega}(n-2p,j-2,p)\} .$$

Le nombre d'éléments du type (II), de poids n fixé et où $s = 1$ est :

$$(21)\quad \beta(r,n,p) = \{\overline{\omega}(n-2,r,p)-\overline{\omega}(n-2-(p-1),r-1,p)\}(r-1)$$
$$= (r-1)\{\overline{\omega}(n-2,r,p)-\overline{\omega}(n-1-p,r-1,p)\}$$

$g(r,n,p)$ est donné par la récurrence :

$$(22)\quad g(r,n,p) = g(r-1,n,p) + \alpha(r,n,p) + \beta(r,n,p) \quad (n \geq 2) .$$

Nous pouvons achever complètement le calcul dans le cas $p = 2$. Alors $\overline{\omega}(n,s,2)$ est le nombre de représentations de n comme somme de s entiers $n_1, n_2, \ldots, n_s$ égaux chacun à 0 ou 1 et l'ordre des termes étant pris en considération. Dans ce cas :

$$\overline{\omega}(n,s,2) = \binom{s}{n}$$

nombre de parties à n éléments de l'ensemble à s éléments formé par les indices. Exprimons $\alpha(r,n,2)$ et $\beta(r,n,2)$ en utilisant les formules (20) et (21) et le lemme 5 :

$$\alpha(r,n,2) = \sum_{j=2}^{r} \{\overline{\omega}(n-3,j-1,2) - \overline{\omega}(n-4,j-2,2)\} = \sum_{j=2}^{r} \left\{\binom{j-1}{n-3} - \binom{j-2}{n-4}\right\} ;$$

si $n = 2$, alors $\alpha(r,n,2) = 0$,

si $n > 2$, alors $\alpha(r,n,2) = \sum_{j=2}^{r} \binom{j-2}{n-3} = \sum_{j=0}^{r-2} \binom{j}{n-3} = \binom{r-1}{n-2}$

et

$$\beta(r,n,2) = (r-1)\{\overline{\omega}(n-2,r,2) - \overline{\omega}(n-3,r-1,2)\} = (r-1)\left\{\binom{r}{n-2} - \binom{r-1}{n-3}\right\} = (r-1)\binom{r-1}{n-2}$$

La formule de récurrence (22) s'écrit :

si $n = 2$ $\quad g(r,2,2) = g(r-1,2,2) + r-1$

si $n \geq 3$ $\quad g(r,n,2) = g(r-1,n,2) + r\binom{r-1}{n-2} = g(r-1,n,2) + (n-1)\binom{r}{n-1}$

Ecrivons chacune de ces formules pour les entiers décroissants de r à 3 et additionnons membre à membre. Nous obtenons :

$$g(r,2,2) = g(2,2,2) + \sum_{i=3}^{r} (i-1) = 1 + \sum_{i=2}^{r-1} i = \frac{r(r-1)}{2} = \binom{r}{2}$$

si $n \geq 3$ $\quad g(r,n,2) = g(2,n,2) + (n-1)\sum_{j=3}^{r} \binom{j}{n-1} = g(2,n,2)$

$$+ (n-1)\sum_{j=0}^{r} \binom{j}{n-1} - (n-1)\left[\binom{1}{n-1} + \binom{2}{n-1}\right]$$

$$= g(2,n,2) + (n-1)\left[\binom{r+1}{n} - \binom{1}{n-1} - \binom{2}{n-1}\right]$$

si $n = 3$ $\quad g(r,3,2) = 2 + 2\left[\binom{r+1}{3} - 1\right] = 2\binom{r+1}{3}$

si $n > 3$ $\quad g(r,n,2) = 0 + (n-1)\binom{r+1}{n} = (n-1)\binom{r+1}{n}$.

D'où la :

<u>Proposition 10</u> : <u>Si</u> $p = 2$, <u>le nombre de générateurs de</u> $\mathcal{G}_n / \mathcal{G}_{n+1}$ <u>où</u> $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{2,2}$ <u>et</u> $r \geq 2$, <u>est donné par</u> :
$g(r,2,2) = \binom{r}{2}$; <u>si</u> $n \geq 3$, <u>alors</u> $g(r,n,2) = (n-1)\binom{r+1}{n}$.

Dans le cas général, nous donnerons une formule de récurrence permettant de calculer $\overline{\omega}(r,n,p)$. Supposons que $n = sp + \ell$ où s est le quotient de la division de n par p et ℓ le reste de cette division. Si

$n = n_1 + n_2 + \dots + n_r$

est une représentation de n comme somme de r entiers au moins égaux à 0, nous associerons à cette représentation un r-uple d'entiers $(n'_1,\dots,n'_r)$ tels que $0 \le n'_i \le p-1$ $(i = 1,2,\dots,r)$, de la façon suivante : nous poserons :

$n'_i = n_i - [\frac{n_i}{p}]\, p = n_i - v_i\, p$ où $v_i = [\frac{n_i}{p}]$ partie entière de $\frac{n_i}{p}$

est le quotient de la division de n_i par p ; c'est-à-dire que nous appellerons n'_i le reste de cette division $(i = 1,2,\dots,r)$.

Appelons $\sum_{i=1}^{r} v_i$ la hauteur de la représentation .

Alors $n'_1 + \dots + n'_r = n - \left(\sum_{i=1}^{r} v_i\right) p$ et nous obtenons ainsi une représentation de $n - \left(\sum_{i=1}^{r} v_i\right) p$ dont les termes sont compris entre 0 et $p-1$ que nous appellerons représentation réduite de la précédente.

Classons les $\omega(n,r)$ représentations de n comme somme de r entiers positifs ou nuls, l'ordre étant pris en considération, deux représentations étant dans la même classe si $u = \sum_{i=1}^{r} v_i$ est le même pour les deux représentations et si les n'_i de même indice sont égaux. Dans une telle classe, le nombre d'éléments est $\omega(u,r)$.

Groupons les classes pour lesquelles u est constant. Le nombre de représentations de n ayant même hauteur est égal au produit de $\omega(u,r)$ par le nombre de représentations réduites associées, donc à $\omega(u,r)\overline{\omega}(n-pu,r,p)$. Enfin faisons varier u de 0 à s . Nous obtenons la formule :

$$(23)\quad \omega(n,r) = \sum_{u=0}^{[\frac{n}{p}]} \omega(u,r).\overline{\omega}(n-up,r,p) \ .$$

Il est facile de montrer que :

$$(24)\quad \omega(n,r) = \binom{r+n-1}{n} = \binom{r-1+n}{r-1} \ .$$

Il suffit de faire une récurrence sur r ; la formule est vraie pour $r = 1$; supposons la vraie jusqu'à r :

$$\omega(n,r+1) = \sum_{i=0}^{n} \omega(n-i,r) = \sum_{i=0}^{n} \omega(i,r) = \sum_{i=0}^{n} \binom{r-1+i}{r-1} = \sum_{i=0}^{r-1+n} \binom{i}{r-1} = \binom{r+n}{r} \ ,$$

à l'aide du lemme 5. Enfin si $[\frac{n}{p}] = 0$, on a $\overline{\omega}(n,r,p) = \omega(n,r,p)$.

La formule (23), qui est une formule de récurrence sur $[\frac{n}{p}]$ permet d'écrire

$$(25)\quad \begin{cases} \overline{\omega}(n,r,p) = \omega(n,r) - \sum_{u=1}^{[\frac{n}{p}]} \omega(u,r)\ \overline{\omega}(n-up,r,p) \\ \overline{\omega}(n - [\frac{n}{p}]p,r,p) = \omega(n - [\frac{n}{p}]p,r) \ . \end{cases}$$

Supposons $p > 2$.

Les premiers termes et les derniers termes de la suite centrale descendante ont un nombre de générateurs que nous pouvons maintenant expliciter.

Supposons $2 \leq n \leq p$. Alors, il n'y a pas de générateurs du type (I) à ajouter et :

$$\alpha(r,n,p) = 0 \ .$$

Calculons le nombre de générateurs du type (II) à ajouter :

$$\beta(r,n,p) = (r-1)\{\overline{\omega}(n-2,r,p) - \overline{\omega}(n-1-p,r-1,p)\} = \overline{\omega}(n-2,r,p).(r-1)$$
$$= (r-1)\omega(n-2,r) = (r-1)\binom{r+n-3}{n-2} \ .$$

La formule de récurrence (22) s'écrit :

$$g(r,n,p) = g(r-1,n,p) + (r-1)\binom{r+n-3}{n-2} \ .$$

Enfin $g(2,n,p) = n-1$.

Nous obtenons donc :

$$g(r,n,p) = \sum_{i=2}^{r} (i-1)\binom{i+n-3}{n-2} = \sum_{i=2}^{r} (n-1)\binom{i+n-3}{n-1} = (n-1)\sum_{i=0}^{r+n-3}\binom{i}{n-1} =$$
$$(n-1)\binom{r+n-2}{n} \ .$$

Si $n = p+1$, nous obtenons :

$$\alpha(r,p+1,p) = \sum_{j=2}^{r} \overline{\omega}(0,j-1,p) = r-1$$

$$\beta(r,p+1,p) = (r-1)\{\overline{\omega}(p-1,r,p) - \overline{\omega}(0,r-1,p)\} = (r-1)\binom{r+p-2}{r-1} - (r-1)$$

et la formule de récurrence (22) s'écrit :

$$g(r,p+1,p) = g(r-1,p+1,p) + (r-1)\binom{r+p-2}{r-1}$$

et $g(2,p+1,p) = p$.

La récurrence est la même, en posant $n = p+1$. D'où la :

<u>Proposition 11</u> : <u>Si</u> $r \geq 2$, $p \geq 2$ <u>et</u> $2 \leq n \leq p+1$, <u>alors</u>

$$g(r,n,p) = (n-1)\binom{r+n-2}{n} = (n-1)\binom{r+n-2}{r-2} \ .$$

Pour étudier les derniers termes de la suite centrale descendante, posons :

$$t = r(p-1)+2-n \ , \quad \text{c'est-à-dire :} \quad n = r(p-1)+2-t \ .$$

Alors :

$$\alpha(r,n,p) = \sum_{j=2}^{r} \{\overline{\omega}((r-1)(p-1)-t,j-1,p) - \overline{\omega}((r-2)(p-1)-t,j-2,p)\}$$

$$\beta(r,n,p) = (r-1)\{\overline{\omega}(r(p-1)-t,r,p) - \overline{\omega}((r-1)(p-1)-t,r-1,p)\}$$
$$= (r-1)\{\overline{\omega}(t,r,p) - \overline{\omega}(t,r-1,p)\} .$$

Supposons $1 \leq t \leq p-2$. Interviennent dans $\alpha(r,n,p)$ les j tels que $(r-1)(p-1)-t \leq (j-1)(p-1)$, c'est-à-dire $r-j \leq \frac{t}{p-1}$, donc $j = r$:

$$\alpha(r,n,p) = \overline{\omega}(r-1)(p-1)-t,r-1,p) - \overline{\omega}((r-2)(p-1)-t,r-2,p)$$
$$= \overline{\omega}(t,r-1,p) - \overline{\omega}(t,r-2,p) = \binom{r+t-2}{t} - \binom{r+t-3}{t} = \binom{r+t-3}{t-1}$$
$$\beta(r,n,p) = (r-1)\left[\binom{r+t-1}{t} - \binom{r+t-2}{t}\right] = (r-1)\binom{r+t-2}{t-1} .$$

D'où la formule de récurrence :

$$g(r,n,p) = g(r-1,n,p) + \binom{r+t-3}{t-1} + (r-1)\binom{r+t-2}{t-1}$$
$$= g(r-1,n,p) + \binom{r+t-3}{t-1}(1+r+t-2) .$$

Mais $g(r-1,n,p) = 0$. D'où

$$(26) \quad g(r,n,p) = (r+t-1)\binom{r+t-3}{t-1} .$$

Supposons $t = p-1$. Interviennent dans $\alpha(r,n,p), j = r$ et $j = r-1$.

$$\alpha(r,n,p) = \overline{\omega}((r-1)(p-1)-t,r-1,p) + \overline{\omega}((r-1)(p-1)-t,r-2,p)$$
$$= \overline{\omega}((r-2)(p-1)-t,r-2,p) - \overline{\omega}((r-2)(p-1)-t,r-3,p)$$
$$= \overline{\omega}(p-1,r-1,p)+1 - \overline{\omega}(p-1,r-2,p)-1 = \binom{r+(p-1)-3}{p-2}$$
$$\beta(r,n,p) = (r-1)\binom{r+t-2}{t-1} ,$$

et $g(r-1,n,p) = 0$.

La formule (26) est encore valable.

Supposons enfin $t = p$; deux valeurs de j sont à conserver : $j = r$ et $j = r-1$.

$$\alpha(r,n,p) = \overline{\omega}(p,r-1,p) - \overline{\omega}(p,r-2,p) + \overline{\omega}(1,r-2,p) - \overline{\omega}(1,r-3,p)$$
$$= \omega(p,r-1) - \omega(1,r-1)\overline{\omega}(0,r-1) - \omega(p,r-2) + \omega(1,r-2)\overline{\omega}(0,r-2)$$
$$+ r-2-(r-3)$$
$$= \omega(p,r-1) - \omega(p,r-2) = \binom{r+t-3}{t-1} \quad \text{où } t = p .$$
$$\beta(r,n,p) = (r-1)[\overline{\omega}(p,r,p) - \overline{\omega}(p,r-1,p)]$$
$$= (r-1)[\omega(p,r) - \omega(1,r) - \omega(p,r-1) + \omega(1,r-1)]$$
$$= (r-1)\left[\binom{r+p-1}{p} - r - \binom{r+p-2}{p} + r-1\right] = (r-1)\binom{r+p-2}{p-1} - (r-1) .$$

Remarquons que $g(r-1,n,p) = r-1$ dans ce cas. La formule (26) est encore valable. D'où la :

Proposition 12 : Si $r \geq 2$, $p \geq 2$ et $1 \leq t \leq p$, si nous posons $n = r(p-1)+2-t$, alors

$$g(r,n,p) = (r+t-1)\binom{r+t-3}{t-1} = (r+t-1)\binom{r+t-3}{r-2}$$

§4. Suite centrale ascendante des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ si $r \geq 2$.

Nous poserons encore $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ et

$\mathcal{K} = \mathcal{L}(r)_{p,1} / \mathcal{L}(r)_{p,2}$. Le groupe $\mathcal{G}$ contient un sous-groupe isomorphe à $\mathcal{L}(r-1) / \mathcal{L}(r-1)_{p,2}$. En effet, appelons H_i le sous-groupe de $\mathcal{G}$ engendré par $\{a_1,\ldots,a_r\} - \{a_i\}$, où i est un entier fixé choisi dans $\{1,2,\ldots,r\}$. Nous avons vu, dans l'étude générale des endomorphismes de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, qu'à toute application de $\{a_1,a_2,\ldots,a_r\}$ dans $\mathcal{G}$ correspond de façon unique un endomorphisme de $\mathcal{G}$. Soit ξ_i l'endomorphisme de $\mathcal{G}$ défini par :

$$\xi_i(a_j) = a_j \quad \text{si } j \neq i \quad ; \quad \xi_i(a_i) = 1 \ ,$$

et soit η_i l'injection canonique de H_i dans $\mathcal{G}$. Alors ξ_i restreint à H_i est l'identité id_{Hi} et

$$\xi_i \circ \eta_i = id_{H_i} \quad ; \quad \text{enfin} \quad \xi_i(\mathcal{G}) = H_i \ .$$

Appelons K_i le noyau de ξ_i . Alors $\mathcal{G} = K_i . H_i$ et $K_i \cap H_i = \{1\}$. En effet, si x appartient à $K_i \cap H_i$, alors $\xi_i(x) = 1$ puisque x appartient à K_i et $\xi_i(x) = x$ puisque x appartient à H_i ; donc $K_i \cap H_i = \{1\}$. De plus si g est un élément de $\mathcal{G}$, alors $\xi_i(g)$ appartient à H_i et $g.\xi_i(g)^{-1}$ appartient au noyau K_i de ξ_i, donc $g = k\,h$ où k appartient à K_i et $h = \xi_i(g)$ appartient à H_i .

Le groupe $\mathcal{G}$ est le produit semi-direct du sous-groupe normal K_i par le sous-groupe H_i et tout élément de $\mathcal{G}$ s'écrit d'une façon unique comme produit d'un élément de K_i par un élément de H_i .

Le groupe $K_i \cap \mathcal{K}$ contient a_i^p ainsi que tous les commutateurs élémentaires faisant intervenir explicitement a_i . La base de $\mathcal{K}$ que nous avons déterminée en (3a) se compose d'éléments de $K_i \cap \mathcal{K}$, de commutateurs ne faisant pas intervenir a_i et des éléments $a_1^p,\ldots,a_{i-1}^p,a_{i+1}^p,\ldots,a_r^p$, ces derniers éléments appartenant à H_i. Nous voyons donc que $\mathcal{K} = (K_i \cap \mathcal{K}).(H_i \cap \mathcal{K})$. Puisque $K_i \cap H_i = \{1\}$, c'est que $K_i \cap \mathcal{K}$ est engendré par a_i^p et les commutateurs de la base de $\mathcal{K}$ qui contiennent explicitement a_i et que $H_i \cap \mathcal{K}$ est engendré par les éléments $a_1^p,\ldots,a_{i-1}^p,a_{i+1}^p,\ldots,a_r^p$ et les commutateurs de la base qui ne contiennent pas explicitement a_i, c'est-à-dire par les éléments de la base correspondante du sous-groupe $\mathcal{L}(r-1)_{p,1} / \mathcal{L}(r-1)_{p,2}$ associée au sous-groupe de $\mathcal{G}$ engendré par $\{a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_r\}$.

Appelons L l'intersection des sous-groupes normaux K_i lorsque i varie de 1 à r ; L est le sous-groupe de $\mathcal{K}$ engendré par les éléments de la base $\mathcal{G}_2$ déterminée en (3a) qui font intervenir explicitement tous les r éléments générateurs $a_1,a_2,\ldots,a_r$. Soit $\mathcal{B}$ l'ensemble de ces éléments ; ils sont des deux types suivants :

(I') $[(p-1)a_1,\dots,n_r a_r,a_1,a_r]$ où $n_r \not\equiv p-1$ et $n_2,\dots,n_{r-1}$ sont différents de 0 .

(II') $[n_1a_1,\dots,n_r a_r,a_1,a_j]$ où $1 < j \leq r$, $n_1 \not\equiv p-1$ et $n_k \not\equiv 0$ si $k \neq 1,j$.

Construisons une suite croissante de sous-groupes de L par le moyen suivant : $S_0(L) = \{1\}$; $S_n(L)$ est l'ensemble des éléments de L qui centralisent $\mathcal{G}/S_{n-1}(L)$ où $n \geqslant 1$.

Lemme 9 : $S_n(L)$ est le sous-groupe de L engendré par les éléments de la base $\mathcal{B}$ dont le poids est au moins égal à $r(p-1)+2-n$.

Un élément z de L s'écrit d'une façon unique sous la forme :

$$z = \prod [(p-1)a_1,\dots,n_r a_r,a_1,a_r]^{u(n_2,\dots,n_r)} \cdot \prod [n_1a_1,\dots,n_r a_r,a_1,a_j]^{v(n_1,\dots,n_r,j)}$$

où les produits sont étendus à tous les éléments du type (I') de $\mathcal{B}$ pour le premier, du type (II') de $\mathcal{B}$ pour le deuxième. Pour que z appartienne à $S_n(L)$, il est nécessaire et suffisant que $[a_i,z]$ appartienne à $S_{n-1}(L)$ pour $i = 1,2,\dots,r$. Examinons de près la forme des $[a_i,z]$ ainsi que l'ensemble $[a_i,\mathcal{B}]$.

Si x est un élément du type (I'), alors $[a_i,x] = 1$ ou $[a_i,x] \in \mathcal{B}$

Si y est un élément du type (II'), alors $[a_i,y] = 1$ ou $[a_i,y] \in \mathcal{B}$ sauf si $i = 1$ et $y = [n_1a_1,\dots,n_r a_r,a_1,a_j]$ où $n_1 = p-2$, $n_j \not\equiv p-1$ et $j \neq r$.

Alors :

$$[a_1,y] = [a_1(p-2)a_1,\dots,n_r a_r,a_1,a_j] = [(p-1)a_1,\dots,n_r a_r,a_1,a_j]$$

où $n_r \not\equiv 0$ et $1 < j < r$.

Appliquons la relation de Ph. Hall :

$$[a_1,y] = [(p-1)a_1,\dots,(n_j+1)a_j,\dots,(n_r-1)a_r,a_1,a_r] \in \mathcal{B}$$

Voyons maintenant les conditions pour que $[a_i,z]$ appartienne à $S_1(L)$. Considérons le facteur $[(p-1)a_1,\dots,n_r a_r,a_1,a_r]^{u(n_2,\dots,n_r)}$.

Si $n_r \not\equiv p-2$, ce facteur donne naissance dans $[a_r,z]$ au facteur :

$$[(p-1)a_1,\dots,(n_r+1)a_r,a_1,a_r]^{u(n_1,\dots,n_r)} \neq 1 \quad \text{et}$$

aucun autre facteur de z ne fait apparaître dans $[a_r,z]$ un élément $[(p-1)a_1,\dots,(n_r+1)a_r,a_1,a_r]$, donc $u(n_2,\dots,n_r)$ est l'exposant de cet élément dans $[a_r,z]$.

Si $n_r = p-2$ et si l'un des n_i où $2 \leq i \leq r-1$ est différent de $p-1$, par exemple n_k, alors, d'une façon analogue, on voit que l'exposant de $[(p-1)a_1,\dots,(n_k+1)a_k,\dots,(p-2)a_r,a_1,a_r]$ dans $[a_k,z]$ est $u(n_2,\dots,n_r)$.

Si $n_r = p-2$ et tous les n_i où $2 \leq i \leq r-1$ sont égaux à $p-1$, alors le facteur $[(p-1)a_1,\ldots,(p-2)a_r,a_1,a_r]$ appartient à $\mathcal{G}_{r(p-1)+1}$ qui appartient au centre de $\mathcal{G}$.

Considérons maintenant le facteur $[n_1a_1,\ldots,n_ra_r,a_1,a_j]^{v(n_1,\ldots,n_r,j)}$ supposé du type (II'). Si l'un des n_i où $2 \leq i \leq r$ est différent de $p-1$, par exemple n_k, l'exposant de $[n_1a_1,\ldots,(n_k+1)a_k,\ldots,n_ra_r,a_1,a_j]$ dans $[a_k,z]$ est $v(n_1,\ldots,n_r,j)$.

Si tous les n_i où $2 \leq i \leq r$ sont égaux à $p-1$ et si $n_1 \neq p-2$, on voit de même que l'exposant de $[(n+1)a_1,\ldots,n_ra_r,a_1,a_j]$ dans $[a_1,z]$ est $v(n_1,\ldots,n_r,j)$.

Si $n_1 = p-2$ et $n_i = p-1$ pour $2 \leq i \leq r$, alors le facteur $[(p-2)a_1,\ldots,(p-1)a_r,a_1,a_j]$ appartient à $\mathcal{G}_{r(p-1)+1}$ qui appartient au centre de $\mathcal{G}$.

Cette étude montre que, pour que z appartienne à $S_1(L)$, il est nécessaire et suffisant que tous les exposants $u(n_2,\ldots,n_r)$ et $v(n_1,\ldots,n_r,j)$ soient nuls sauf ceux qui correspondent aux éléments de poids $r(p-1)+1$. Et par récurrence, que z appartient à $S_n(L)$ si et seulement si ces exposants sont nuls pour les éléments de poids strictement inférieur à $r(p-1)+2-n$

Démontrons maintenant le :

Théorème 5 : Si $c = r(p-1)+1$, alors les termes de la suite centrale ascendante de $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ sont donnés par :

$$Z_s(\mathcal{G}) = \mathcal{G}_{c-s+1} \quad \text{si} \quad c-s+1 \geq p+1 \quad \text{c'est-à-dire si} \quad s \leq c-p$$

$$Z_s(\mathcal{G}) = \mathcal{G}_{c-s+1} \cdot \langle a_1^p,\ldots,a_r^p \rangle \quad \text{si} \quad c-p+1 \leq s \leq r(p-1) .$$

Faisons une récurrence sur le nombre r de générateurs. Le théorème se réduit à la proposition 9 si $r = 2$. Supposons le théorème vrai si le nombre de générateurs est au plus $r-1$. L'image de $Z_1(\mathcal{G})$ par ξ_i appartient à $Z_1(\xi_1(\mathcal{G})) = Z_1(H_i)$. Mais H_i est isomorphe à $\mathcal{L}(r-1)/\mathcal{L}(r-1)_{p,2}$; donc $Z_1(H_i)$ est le sous-groupe engendré par les éléments de poids $(r-1)(p-1)+1$ de la base de $(H_i)_2$ obtenue en (3a) , donc des éléments de même poids ne faisant pas intervenir a_i dans la base de $\mathcal{G}_2$ lui-même. Appelons $\mathcal{B}_i$ l'ensemble de ces éléments. Alors $Z_1(\mathcal{G}) \subset K_i \langle \mathcal{B}_i \rangle$.

Ce raisonnement est valable si $i = 1,2,\ldots,r$. Donc :

$$Z_1(\mathcal{G}) \subset \bigcap_{i=1}^{r} K_i.\langle \mathcal{B}_i \rangle = L.\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle .$$

Les éléments de $\mathcal{B}_i$ sont : un élément b_i du type (I) et $r-1$ éléments $b'_{i,j}$ du type (II) où j est l'indice du dernier élément écrit.

Nous savons que, si $k \neq i$, alors $[a_k,b_i] = 1 = [a_k,b'_{i,j}]$.

Supposons $i \neq 1,r$. Alors

$[a_i,b_i] = [(p-1)a_1,\ldots,a_i,\ldots,(p-2)a_r,a_1,a_r]$ est du type (I)

$[a_i,b'_{i,j}] = [(p-2)a_1,\ldots,a_i,\ldots,(p-1)a_r,a_1,a_j]$ est du type (II).

Supposons $i = 1$, et appliquons la relation de Ph. Hall :

$[a_1,b_1] = [a_1,(p-1)a_2,\ldots,(p-2)a_r,a_2,a_r] = [(p-1)a_2,\ldots,(p-1)a_r,a_1,a_2]^{-1}$

inverse d'un élément du type II.

$[a_1,b'_{1,j}] = [a_1,(p-2)a_2,\ldots,(p-1)a_r,a_2,a_j] = [(p-1)a_2,\ldots,(p-1)a_r,a_1,a_j]$

est du type II.

Supposons $i = r$, et appliquons éventuellement la relation de Ph. Hall:

$[a_r,b_r] = [(p-1)a_1,\ldots,(p-2)a_{r-1},a_r,a_1,a_{r-1}] =$

$[(p-1)a_1,\ldots,(p-1)a_{r-1},a_1,a_r]$ qui est du type (I)

$[a_r,b'_{r,j}] = [(p-2)a_1,\ldots,(p-1)a_{r-1},a_r,a_1,a_{r-1}]$ qui est du type (II).

Un élément de $L.\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle$ s'écrit de façon unique sous la forme :

$$g = \Big(\prod b_i^{u_i}\Big)\Big(\prod\prod b'^{v(i,j)}_{i,j}\Big) \cdot z \quad \text{où} \quad z \in L .$$

Les éléments $[a_i,b_i]$ et $[a_i,b'_{i,j}]$ n'apparaissent pas dans $[a_i,z]$; il suffit pour s'en assurer de regarder leur expression.

Donc g appartient à $Z_1(\mathcal{G})$ si et seulement si $u_i = v(i,j) = 0$ et $z \in S_1(L)$; et $Z_1(\mathcal{G}) = \mathcal{G}_{r(p-1)+1}$. On passe au quotient de $\mathcal{G}$ par $Z_1(\mathcal{G})$. On voit de même que $Z_2(\mathcal{G}) \subset (L.\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle)/Z_1(\mathcal{G})$ et ainsi de suite. Le raisonnement se poursuit jusqu'à ce qu'on ait obtenu :

$$S_{p-1}(L) = Z_{p-1}(\mathcal{G}) = \mathcal{G}_{(r-1)(p-1)+2} .$$

Appliquons ξ_i, nous voyons que $Z_p(\mathcal{G}) \subset K_i.\langle \mathcal{B}_i \rangle$ de la même façon que plus haut, donc que $Z_p(\mathcal{G}) \subset L.\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle$. Mais $\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle$ appartient au centralisateur de $\mathcal{G}/Z_{p-1}(\mathcal{G}) = \mathcal{G} / \mathcal{G}_{(r-1)(p-1)+2}$ puisqu'il appartient à $\mathcal{G}_{(r-1)(p-1)+1}$. Donc

$$Z_p(\mathcal{G}) = S_p(L).\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle = \mathcal{G}_{(r-1)(p-1)+1} .$$

Ensuite, on répète le procédé en remplaçant $\langle \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r \rangle$ par le sous-groupe engendré par les groupes que nous noterons $Z_m(H_i)$, (où $i = 1,2,\ldots,r$) et où $Z_m(H_i)$ est le m-ième terme de la suite centrale ascendante de H_i. Nous avons déterminé les groupes $Z_m(H_i)$ par l'hypothèse de récurrence. D'où le théorème 5.

§5. Automorphismes des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$.

Les notations sont celles du chapitre 2, §4 ; nous poserons encore ici $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ et $\mathcal{K} = \mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$. Appliquons le théorème 3 au cas où $n = 2$, le groupe $\mathrm{Aut}(\mathcal{G})$ contient un sous-groupe normal $\mathrm{Ker}\ \gamma_{2,1}$ qui est le sous-groupe de $\mathrm{Aut}(\mathcal{G})$ qui induit l'identité sur $\mathcal{G} / \mathcal{G}_{p,1} \simeq \mathcal{L}(r)/\mathcal{L}(r)_{p,1}$. L'ordre de ce groupe est :

$$|\ \mathrm{Ker}\ \gamma_{2,1}\ | = |\mathcal{K}|^r = p^{r[(r-1)p^r+1]} .$$

Il existe une bijection entre les éléments de $\mathrm{Ker}\ \gamma_{2,1}$ et les r-uples d'éléments de $\mathcal{K}$, si $k_1,\dots,k_r$ sont des éléments de $\mathcal{K}$, l'élément f de $\mathrm{Ker}\ \gamma_{2,1}$ qui lui est associé est défini par

$$f(a_1) = k_1 a_1, \dots, f(a_r) = k_r a_r .$$

Proposition 13 : Le sous-groupe $\mathrm{Ker}\ \gamma_{2,1}$ de $\mathrm{Aut}(\mathcal{L}(r)/\mathcal{L}(r)_{p,2})$ induit l'identité sur chacun des quotients de la suite

$\mathcal{G} \supset \mathcal{K} \supset \mathcal{G}_2 \supset \dots \supset \mathcal{G}_n \supset \dots \supset \mathcal{G}_{r(p-1)+1} \supset \{1\}$ de sous-groupes de $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$.

Par hypothèse, $\mathrm{Ker}\ \gamma_{2,1}$ induit l'identité sur $\mathcal{G} / \mathcal{K}$.
Si nous calculons modulo $\mathcal{G}_2$, alors $f((k_i a_i)^p) \equiv k_i^p a_i^p \equiv a_i^p$ modulo $\mathcal{G}_2$ donc $\mathrm{Ker}\ \gamma_{2,1}$ induit l'identité sur $\mathcal{K}/\mathcal{G}_2$.

Rappelons que, si a,b, c sont des éléments d'un groupe :

(8) $[ab,c] = {}^a[b,c].[a,c]$

(27) $[a,bc] = [a,b].{}^b[a,c]$.

Dans le cas présent, si a est un élément de $\mathcal{K}$, la formule (8) devient $[ab,c] = [a,c][b,c]$; si b est un élément de $\mathcal{K}$, la formule (27) devient $[a,bc] = [a,b][a,c]$.

Supposons que l'élément f de $\mathrm{Ker}\ \gamma_{2,1}$ soit défini par :

$f(a_i) = k_i a_i$ où $i = 1,2,\dots,r$ et k_i est un élément de $\mathcal{K}$

Alors :

$$[k_i a_i, k_j, a_j] = [k_i, k_j][k_i, a_j][a_i, k_j][a_i, a_j]$$

Supposons que : $k_i = x \prod_{s=1}^{r} (a_s^p)^{v(s)}$ et $k_j = y \prod_{s=1}^{r} (a_s^p)^{w(s)}$

où x et y appartiennent à $\mathcal{G}_2$ et v(s) et w(s) sont des entiers positifs.

Nous obtenons :

$$[k_i a_i, k_j a_j] = [k_i, a_j][a_i, k_j][a_i, a_j] \equiv \prod_{s=1}^{r} (pa_s, a_j)^{v(s)} \cdot$$

$$\prod_{s=1}^{r} (pa_s, a_i)^{-w(s)} \cdot [a_i, a_j] \mod \mathcal{G}_3$$

$$\equiv [a_i, a_j] \mod \mathcal{G}_3 .$$

Enfin : $[k_s a_s, a_i, a_j] = [k_s, a_i, a_j][a_s, a_i, a_j] = [a_s, a_i, a_j]$.

On voit alors directement que, si $n_1+n_2+\ldots+n_r+2 = n$, alors : $f([n_1 a_1, \ldots, n_r a_r, a_i, a_j]) \equiv [n_1 a_1, \ldots, n_r a_r, a_i, a_j] \mod \mathcal{G}_{n+1}$ et la proposition 13 est démontrée.

Nous pouvons tirer de cette proposition deux conséquences.

Tout d'abord $\operatorname{Ker} \gamma_{2,1}$ est un groupe d'automorphismes de $\mathcal{G}$ qui induit l'identité sur chacun des quotients de la suite de sous-groupes normaux $\mathcal{G} \supset \mathcal{K} \supset \mathcal{G}_2 \supset \ldots \supset \mathcal{G}_{r(p-1+1} \supset \{1\}$.

Cette suite est de longueur $r(p-1)+2$. Nous en déduisons [8 ; Th 2] que $\operatorname{Ker} \gamma_{2,1}$ est un groupe nilpotent (c'est d'ailleurs un p-groupe) dont la classe est au plus $r(p-1)+1$.

Ensuite, quel que soit le p-groupe G de longueur de Frattini 2 au plus à r générateurs exactement, le sous-groupe de $\operatorname{Aut}(G)$ qui induit l'identité sur $G/G_{p,1}$ est un sous-groupe de $\operatorname{Ker} \gamma_{2,1}$, et G est un quotient de $\mathcal{G}$. Donc il induit l'identité sur chaque quotient de la suite $G \supset G_{p,1} \supset G_2 \supset \ldots \supset G_n \supset \ldots \supset \{1\}$ et sa classe est au plus $r(p-1)+1$. D'où le :

Corollaire 5 : Si G est un groupe possédant exactement r générateurs et dont la longueur de Frattini est au plus 2, le sous-groupe de $\operatorname{Aut}(G)$ qui induit l'identité sur $G/G_{p,1}$ induit l'identité sur chacun des quotients de la suite $G \supset G_{p,1} \supset G_2 \supset \ldots \supset G_n \supset \ldots \supset \{1\}$; sa classe est au plus égale à $r(p-1)+1$.

Revenons à l'étude de $\mathcal{G}$. Le groupe $\operatorname{Ker} \gamma_{2,1}$ laisse fixe chaque élément du centre $Z_1(\mathcal{G})$ de $\mathcal{G}$; ce centre est un p-groupe abélien élémentaire. Il est isomorphe à $\mathcal{G} / \mathcal{K}$.

Démontrons la :

Proposition 14 : Le groupe des automorphismes de $\mathcal{G} = \mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ opère sur le centre de $\mathcal{G}$, qui est un espace vectoriel sur le corps à p-éléments, en notation additive, comme le groupe linéaire $GL(r,p)$ entier.

Nous avons déterminé dans le paragraphe 3.a , un système générateur de $Z_1(\mathcal{G})$. Remplaçons-le par le suivant :

$$\begin{cases} x_1 = [(p-1)a_1,\dots,(p-2)a_r,a_1,a_r] \\ x_i = [(p-2)a_1,\dots,(p-1)a_r,a_1,a_i]^{-1} \quad \text{où } i = 2,\dots,r \end{cases}.$$

Le groupe des automorphismes de $\mathcal{G}$ opère sur $\mathcal{G} / \mathcal{G}_{p,1}$ comme le groupe linéaire GL(r,p) entier. Nous savons donc que ce groupe est engendré par les transformations suivantes [1 , p.150] ;

$\beta_{i,j}$ telle que $\beta_{i,j}(a_i) = a_i a_j$ et $\beta_{i,j}(a_k) = a_k$ si $k \neq i$ $(i \neq j \ ; \ i,j = 1,2,\dots,r)$

δ_n telle que $\delta_n(a_i) = a_i$ si $i \neq r$ et $\delta_n a_r = a_r^n$ où $1 \leq n \leq p-1$.

Cherchons quel est l'effet de chacune des transformations $\beta_{i,j}$ et δ_n sur la base $\{x_1,x_2,\dots,x_r\}$ de $\mathcal{G}_{r(p-1)+1} = Z_1(\mathcal{G})$.

$$\delta_n(x_1) = [(p-1)a_1,\dots,(p-2)a_r^n,a_1,a_r^n] = [(p-1)a_1,\dots,(p-2)a_r^n,a_1,a_r]^n$$
$$= [(p-1)a_1,\dots,(p-2)a_r,a_1,a_r]^{nn^{p-2}} = x_1^{n^{p-1}} .$$

Mais on sait que $n^{p-1} \equiv 1 \mod p$ si n est premier à p , ce qui est le cas. Donc $\delta_n(x_1) = x_1$.

Si $i \neq r,1$:

$$\delta_n(x_i) = [(p-2)a_1,\dots,(p-1)a_r^n,a_1,a_i]^{-1} = [(p-2)a_1,\dots,(p-1)a_r,a_1,a_i]^{-n^{p-1}} = x_i .$$

Enfin :

$$\delta_n(x_r) = [(p-2)a_1,\dots,(p-1)a_r^n,a_1,a_r^n]^{-1} = [(p-2)a_1,\dots,(p-1)a_r,a_1,a_r]^{-n^p} = x_r^n .$$

En résumé :

$$\delta_n(x_i) = x_i \text{ si } i \neq r \quad \text{et} \quad \delta_n(x_r) = x_r^n .$$

D'une façon analogue, nous verrons que :

$$\beta_{i,j}(x_i) = x_i x_j \quad \text{et} \quad \beta_{i,j}(x_k) = x_k \quad \text{si } k \neq i \ (i \neq j \ ; \ i,j = 1,2,\dots,r) ,$$

et la proposition 14 est démontrée.

L'application de $\mathcal{G} / \mathcal{K}$ sur $Z_1(\mathcal{G})$ définie par :

$$a_i \longmapsto x_i \quad (i = 1,2,\dots,r)$$

donne naissance, si nous utilisons la notation additive, à un isomorphisme des $(\mathrm{Aut}(\mathcal{G}))$-modules $\mathcal{G} / \mathcal{K}$ et $Z_1(\mathcal{G})$.

De la proposition 14 nous déduisons le :

Corollaire 6 : Le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ est le seul sous-groupe caractéristique minimal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$.

En effet tout sous-groupe caractéristique de $\mathcal{G}$ est normal dans $\mathcal{G}$ donc a avec $Z_1(\mathcal{G})$ une intersection non triviale [12 ; p.144] . Puisqu'il est caractéristique, il contient $Z_1(\mathcal{G})$ entier.

CHAPITRE IV

Exposants des quotients des suites centrales

Nous établirons dans ce paragraphe quelques résultats généraux dont certains seront utiles dans la suite et qui sont donnés pour la plupart dans [3]

Si G est un groupe, non nécessairement fini, non nécessairement nilpotent, il est cependant intéressant de former la chaîne descendante des sous-groupes :

$G = G_1 \supset G_2 \supset \ldots \supset G_n \supset \ldots$ où la notation est la notation habituelle, c'est-à-dire que $G_{i+1} = [G, G_i]$, $(i \geq 1)$. Ces sous-groupes sont caractéristiques dans G ; nous pouvons former les quotients G_i/G_{i+2}. Les automorphismes intérieurs de G induisent sur chaque quotient un groupe d'automorphismes qui est isomorphe à G/C_{i+1} si nous appelons C_{i+1} le centralisateur dans G du quotient G_i/G_{i+2} .

Il est aussi possible de former une chaîne ascendante de sous-groupes $Z_0(G) = \{1\} \subset Z_1(G) \subset \ldots \subset Z_n(G) \subset \ldots$ où la notation est la notation habituelle, c'est-à-dire que $Z_{i+1}(G)$ est le groupe des éléments de G qui induisent par automorphismes intérieurs l'identité sur le quotient $G/Z_i(G)$, $(i = 0, 1, \ldots)$.

§1. Démontrons le :

Théorème 6 : Si l'un des groupes G/C_{i+1} ou G_{i+1}/G_{i+2} est d'exposant fini, l'autre est aussi d'exposant fini et les deux exposants sont égaux $(i \geq 0)$.

On sait en effet [4 ; p.150] que G_i est engendré par les éléments de la forme $[x_1,\ldots,x_i]$ où x_j appartient à G $(j = 1,\ldots,i)$ et que le groupe G_{i+1}/G_{i+2} est abélien donc qu'il est d'exposant fini si et seulement si chaque élément d'un système générateur est d'exposant fini et qu'il existe un p.p.c.m. pour tous ces exposants.

De plus, on connait la relation :

(28) $[x_{i+1},x_i,\ldots,x_1]^m \equiv [x_{i+1},[x_i,\ldots,x_1]^m] \equiv [x_{i+1}^m,[x_i,\ldots,x_1]] \bmod G_{i+2}$

pour tout entier positif m .

S'il existe un entier e positif tel que, quels que soient les éléments $x_1,\ldots,x_{i+1}$ de G , l'une des trois relations suivantes est vraie :

(29) $[x_{i+1},x_i,\ldots,x_1]^e \equiv 1 \bmod G_{i+2}$,

(30) $[x_{i+1},[x_i,\ldots,x_1]^e] \equiv 1 \bmod G_{i+2}$,

(31) $[x_{i+1}^e,[x_i,\ldots,x_1]] \equiv 1 \bmod G_{i+2}$,

la relation (28) indique que chacune des deux autres relations est vraie aussi.

La relation (29) exprime que G_{i+1}/G_{i+2} est d'exposant fini et que cet exposant divise e.
La relation (30) exprime que le quotient de G_i par son intersection avec le centralisateur de G/G_{i+2} est d'exposant fini et que cet exposant divise e.
La relation (31) exprime que le quotient G/C_{i+1} est d'exposant fini et que cet exposant divise e. Si l'un de ces trois exposants est fini, les deux autres le sont aussi et sont des diviseurs du troisième. Nous obtenons le théorème 6 et même un résultat énoncé par N.Blackburn [2 ; Th 1.5] dans le cas des p-groupes finis :

Si pour un entier r, le groupe G_r/G_{r+1} est d'exposant fini e_r, alors quel que soit l'entier $i > r$; le groupe G_i/G_{i+1} est aussi d'exposant fini e_i, et e_{i+1} divise e_i.

En effet le centralisateur de G/G_{i+2} contient G_{i+1} et le quotient de G_i par l'intersection de G_i avec le centralisateur de G/G_{i+2} est un quotient de G_i/G_{i+1} et son exposant est donc un diviseur du quotient G_i/G_{i+1}.

Corollaire 7 : Si G est un groupe fini nilpotent de classe 2, alors G_2 et $G/Z_1(G)$ ont le même exposant.

Il suffit d'appliquer le théorème 6 au cas où $i = 1$ après avoir remarqué que $G_3 = \{1\}$ entraîne $G_2/G_3 = G_2$ et $C_2 = Z_1(G)$.

Si G est un groupe nilpotent, on sait que $Z_i(G)$ centralise G_i [5 ; Th 2.5.1], donc centralise G_i/G_{i+2} et C_{i+1} contient $Z_i(G)$; l'exposant de G/C_{i+1} est un diviseur de l'exposant de $G/Z_i(G)$ si ce dernier est fini ; donc si $G/Z_i(G)$ a un exposant fini, l'exposant de G_{i+1}/G_{i+2} est un diviseur de cet exposant ($i \geq 1$).

Dans le cas général, $Z_1(G)$ est contenu dans le centralisateur de G/G_3 et l'exposant de G_2/G_3 est un diviseur de l'exposant de $G/Z_1(G)$ si ce dernier exposant est fini.

§2. On peut obtenir des résultats analogues concernant la chaîne centrale ascendante d'un groupe G.

Les automorphismes intérieurs de G induisent sur chaque quotient $Z_{i+1}(G)/Z_{i-1}(G)$ (où $i \geq 1$) un groupe d'automorphismes qui est isomorphe à G/D_i, si D_i est le centralisateur dans G du quotient $Z_{i+1}(G)/Z_{i-1}(G)$.

Démontrons le :

Théorème 7 : Si l'un des trois groupes G/D_i ou $Z_{i+1}(G)/Z_i(G)$ ou $([Z_{i+1}(G),G].Z_{i-1}(G))/Z_{i-1}(G)$ est d'exposant fini, alors chacun des deux autres est aussi d'exposant fini et les trois exposants sont égaux.

Si x,y appartiennent à $Z_{i+1}(G)$ et si g, h appartiennent à G, les relations :

$$[xy,g] = {}^x[y,g].[x,g] \equiv [y,g].[x,g] \bmod Z_{i-1}(G)$$

$$[x, gh] = [x,g].{}^g[x,h] \equiv [x,g].[x,h] \bmod Z_{i-1}(G)$$

permettant d'établir l'analogue de la relation (28) :

$$(32) \qquad [x^m,g] \equiv [x,g]^m \equiv [x,g^m] \bmod Z_{i-1}(G) .$$

Si l'une des trois congruences :

$$(33) \qquad [x^e,g] \equiv 1 \bmod Z_{i-1}(G)$$

$$(34) \qquad [x,g]^e \equiv 1 \bmod Z_{i-1}(G)$$

$$(35) \qquad [x,g^e] \equiv 1 \bmod Z_{i-1}(G)$$

est vraie pour un entier positif e quels que soient g dans G et x dans $Z_{i+1}(G)$, chacune des deux autres est vraie dans les mêmes conditions.

La relation (33) exprime que l'exposant de $Z_{i+1}(G)/Z_i(G)$ est fini et divise e.

La relation (34) exprime que $([Z_{i+1}(G),G].Z_{i-1})/Z_{i-1}$ a un exposant fini qui divise e.

La relation (35) exprime que G/D_i a un exposant fini qui divise e.

Si l'un de ces trois exposants est fini, la relation (32) exprime que les deux autres le sont aussi et divisent le premier, donc ils sont tous les trois égaux.

Corollaire 8 : Si pour un certain entier $r \geq 1$, le groupe $Z_r(G)/Z_{r-1}(G)$ est d'exposant fini ε_r, alors quel que soit $i \geq r$, le groupe $Z_i(G)/Z_{i-1}(G)$ est aussi d'exposant fini ε_i et ε_{i+1} divise ε_i

En effet $[Z_{i+1}(G),G]$ appartient à $Z_i(G)$ et le quotient $[Z_{i+1}(G),G]Z_{i-1}(G)/Z_{i-1}(G)$ est un sous-groupe de $Z_i(G)/Z_{i-1}(G)$, donc son exposant est fini et divise celui de $Z_i(G)/Z_{i-1}(G)$ si ce dernier exposant est fini.

Nous pouvons utiliser les résultats précédents pour démontrer la :

Proposition 15 : Si G est un groupe fini nilpotent, pour que les groupes de sa suite centrale ascendante et ceux de sa suite centrale descendante coïncident, il est nécessaire que les exposants des quotients des termes successifs soient tous égaux entre eux.

En effet les exposants des quotients successifs de la suite centrale ascendante décroissent avec l'indice d'après le théorème 7 ; ceux de la suite centrale descendante décroissent avec l'indice d'après le paragraphe 1. Il est donc nécessaire que tous ces exposants soient égaux.

De tels groupes non abéliens existent : par exemple, les p-sous-groupes de Sylow du groupe des permutations d'un ensemble à p^2 éléments ; dans ce cas l'exposant est p.

§3. L'étude précédente suggère l'étude des exposants dans tous les cas où se présente de façon naturelle une chaîne sous-invariante de sous-groupes. Nous pouvons essayer de généraliser ce procédé.

Soit G un groupe fini ; soient H et K deux sous-groupes de G tels que $H \supset K$. Si h est un élément de H, il existe un plus petit entier positif n(h) tel que $h^{n(h)}$ appartienne à K. Nous appellerons n(h) l'exposant de h relatif à K. Il est clair que $n(h) = 1$ si et seulement si h appartient à K. Le nombre n(h) est un diviseur de l'ordre de h.

Nous appellerons exposant de H relatif à K le plus petit commun multiple des exposants de h relatifs à K lorsque h parcourt H. Si K est normal dans H, l'exposant de H relatif à K est l'exposant de H/K.

Supposons que L soit un troisième sous-groupe de G tel que $H \supset K \supset L$. Suivant [8], nous dirons que l'automorphisme a de G stabilise (H ; K) si pour tout élément h de H on a : $a(h) \in h\,K$. Si a stabilise (H ; K) et (K ; L), nous dirons que a stabilise (H ; K ; L). Nous noterons e(H ; K) l'exposant de H relatif à K.

Montrons le :

Lemme 10 : Soient G un groupe fini et a un automorphisme de G qui stabilise la chaîne (H ; K ; L) de sous-groupes de $G(H \supset K \supset L)$. Si e(K ; L) est l'exposant de K relatif à L, alors $a^{e(K\,;\,L)}$ stabilise (H ; L).

Montrons par récurrence que si h appartient à H, il existe un élément k de K tel que, pour tout entier $i \geq 1$ on peut trouver ℓ dans L avec $a^i(h) = h\,k^i\ell$. En effet, si $i = 1$, il existe k dans K tel que $a(h) = hk$ puisque a stabilise (H ; K). Supposons le résultat vrai

pour l'entier $i \geq 1$; alors

$$a^{i+1}(h) = a(hk^i\ell) = a(h)a(k^i)a(\ell) = hk.k^i\ell' = h.k^{i+1}\ell' \quad \text{où} \quad \ell,\ell' \in L$$

Du lemme 10 nous déduisons la :

Proposition 16 : Supposons qu'un groupe A d'automorphismes du groupe fini G stabilise une suite de sous-groupes décroissants de G : $(G = G_0, G_1, \ldots, G_s = \{1\})$. Posons $e_i = e(G_i; G_{i+1})$ où $i = 0, \ldots, s-1$. Alors l'exposant de A divise le produit $e_1 \cdot e_2 \cdots e_{s-1}$.

En effet, d'après le lemme 10, si a appartient à A, alors a^{e_1} stabilise (G_0, G_2). Supposons que $a^{e_1 \cdot e_2 \cdots e_i}$ stabilise (G_0, G_{i+1}, G_{i+2}), alors le lemme 10 entraîne $a^{e_1 \cdots e_i e_{i+1}}$ stabilise (G_0, G_{i+2}).

Ainsi $a^{e_1 \cdots e_{s-1}}$ stabilise (G_0, G_s) et donc est l'identité.

Rappelons que A est nilpotent de classe au plus $\frac{s(s-1)}{2}$ [7 ; Th 1].

Corollaire 9 : Si G est un p-groupe fini, tout groupe d'automorphismes de G qui stabilise une suite décroissante de sous-groupes $(G = G_0, G_1, \ldots, G_s = \{1\})$ est lui-même un p-groupe.

En effet l'exposant de G_i relatif à G_{i+1} est une puissance de p, puisque l'ordre de chaque élément de G est une puissance de p.

CHAPITRE V

Retour à l'étude des groupes $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ si $r \geq 2$.

Utilisons les résultats des paragraphes précédents dans l'étude des groupes généraux $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ où $r \geq 2$ et $n \geq 2$.

§1. Sous-groupes abéliens normaux maximaux.

Dans le cas où $n = 2$, nous pouvons démontrer le :

Lemme 11 : Le groupe $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$ est le seul sous-groupe abélien normal maximal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$.

D'abord, $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$ est un sous-groupe abélien normal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$.

Supposons que le sous-groupe normal H de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ contienne un élément x qui n'appartienne pas à $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$. Utilisons les notations des paragraphes précédents : nous appellerons $[a_1, a_2, \ldots, a_r]$ un système générateur de $\mathcal{L}(r)$ et nous identifierons a_i $(i = 1,2,\ldots,r)$ avec son image canonique dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$. Le corollaire 1 (II ; 4) indique qu'il existe un automorphisme de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ qui applique x sur a_2 . Soit f un tel automorphisme. Alors l'image de H par f est un sous-groupe abélien normal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$. Nous pouvons donc supposer que H contient a_2, sans nuire à la généralité. Si H contient a_2 ce groupe contient tous les conjugués de a_2, dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$, puisque H est un sous-groupe normal. Il contient donc $a_1 a_2 a_1^{-1} = [a_1, a_2]a_2$. Si H est abélien, l'élément a_2 doit permuter avec chacun de ses conjugués, en particulier avec $a_1 a_2 a_1^{-1}$, donc avec $[a_1, a_2]$. Mais nous avons vu que $[a_2, a_1, a_2]$ était différent de l'élément neutre, puisque $[a_2, a_1, a_2]$ est un élément de type (II) de la base de $(\mathcal{L}(r)'/\mathcal{L}(r)_{p,2})'$ que nous avons déterminée au paragraphe III 3a. D'où une contradiction. Il est impossible qu'un sous-groupe abélien normal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ ait un élément hors de $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}$ et le lemme 11 est démontré.

Dans le cas général, nous démontrerons le :

Théorème 8 : Le groupe $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$ est le seul sous-groupe abélien normal maximal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$. $(n \geq 1)$.

Faisons une récurrence sur l'entier n . Le théorème est vrai pour $n = 2$ (et d'ailleurs aussi trivialement pour $n = 1$). Supposons le théorème vrai pour tout entier positif au plus égal à n-1 . Tout sous-groupe normal abélien H de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ a pour image dans l'homomorphisme

$\gamma_{n,n-1}$ (2.4) un sous-groupe abélien normal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n-1}$; d'après l'hypothèse de récurrence, cette image $\gamma_{n,n-1}(H)$ appartient à $\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n-1}$. Donc H lui-même appartient au groupe $\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n}$. Mais le groupe $\mathcal{L}(r)_{p,n-2}$ est un groupe libre à un nombre fini de générateurs, comme nous l'avons vu au paragraphe II.1, et $\mathcal{L}(r)_{p,n}$ est le deuxième groupe p-dérivé de $\mathcal{L}(r)_{p,n-2}$. Appliquons le lemme 11 à $\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n}$; ce groupe contient un seul sous-groupe abélien normal maximal, qui est $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$; le groupe H étant abélien, normal dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ et contenu dans $\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n}$ est abélien et normal dans ce dernier groupe ; il appartient donc à $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$, ce qui achève la démonstration.

D'après un résultat connu [12 ; 145], tout sous-groupe abélien normal maximal d'un p-groupe fini est son propre centralisateur. La représentation linéaire de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ comme groupe d'automorphismes de $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$ considéré comme un espace vectoriel de dimension $\varphi(r, p, n)$ sur le corps à p éléments, obtenue à l'aide de la restriction à $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$ des automorphismes intérieurs de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, est donc une représentation fidèle de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n-1}$.

Nous pouvons tirer d'autres conséquences du théorème 6. Par exemple le :

Corollaire 10 : Le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ appartient à $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$.

En effet le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est un sous-groupe caractéristique abélien de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$; il est donc un sous-groupe abélien normal de ce groupe, donc contenu dans $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$.

Nous pouvons améliorer un peu ce résultat. Le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ appartenant à $\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n}$ est contenu dans le centre de ce dernier groupe. Mais, avec les notations du paragraphe II.1 , on sait que

$$\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n} \simeq \mathcal{L}(\varphi(r, n-1, p))/\mathcal{L}(\varphi(r, n-1, p))_{p,2}.$$

Le théorème 5 indique que ce centre appartient au groupe dérivé de $\mathcal{L}(r)_{p,n-2}/\mathcal{L}(r)_{p,n}$ qui est lui-même un sous-groupe du groupe dérivé de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$. Le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ appartient donc à son groupe dérivé ; le groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ appartient donc à la souche de sa famille, si nous employons les définitions de l'article de Ph. Hall ([6]).

Dans cet article est introduite la notion d'isoclinisme de deux groupes. Soient G et H deux groupes ; soient Z(G) et Z(H) leurs

centres respectifs. Les deux groupes G et H sont dits isoclines si les trois conditions suivantes sont vérifiées :

(a) il existe un isomorphisme φ de $G/Z(G)$ sur $H/Z(H)$.

(b) il existe un isomorphisme ψ de G_2 sur H_2 .

(c) pour tout couple (x,y) d'éléments de G on a :
$[\overline{\varphi(x)}, \overline{\varphi(y)}] = \psi([x,y])$,

où $\overline{\varphi(x)}$ et $\overline{\psi(y)}$ sont des représentants dans H des classes $\varphi(x)$ et $\varphi(y)$ de H modulo $Z(H)$.

On obtient ainsi une répartition des groupes en "familles" , deux groupes appartenant à la même famille s'ils sont isoclines. Les groupes abéliens forment la famille qui contient le groupe réduit à un élément.

Parmi les groupes finis d'une famille, ceux qui sont du plus petit ordre possible forment la "souche" (stem) de la famille.

Il en existe quand $G/Z(G)$ et G_2 sont finis ; ce sont les groupes de la famille pour lesquels le centre appartient au groupe dérivé. En effet si G et H sont isoclines, les conditions (a), (b), (c) entraînent que $G_2 \cap Z(G)$ et $H_2 \cap Z(H)$ sont isomorphes. Si G est fini :

$$|G| = |G/Z(G)| \cdot |Z(G)/Z(G) \cap G_2| \cdot |Z(G) \cap G_2| ,$$

et G est minimum lorsque $|Z(G)/Z(G) \cap G_2|$ est le plus petit possible. On peut toujours trouver dans la famille des groupes pour lesquels ce facteur est égal à 1. Donc les groupes de la souche sont ceux pour lesquels le centre appartient au groupe dérivé. Tout autre groupe fini de la famille a pour ordre un multiple de l'ordre d'un groupe de la souche.

Etablissons maintenant la :

Proposition 17 : Les quotients des sous-groupes consécutifs de la suite centrale ascendante de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ ont tous pour exposant p. Le dernier terme distinct du groupe entier de cette suite est $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$.

Le groupe $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$ est un p-groupe abélien élémentaire ; son exposant est p . Il contient le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$; donc ce centre a l'exposant p . Appliquons le corollaire 8 (IV. 2) ; nous voyons que chaque quotient de la suite centrale ascendante a pour exposant p et la première partie de la proposition est démontrée.

Appelons c la classe de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$; alors $Z_c(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ est le groupe entier et le dernier quotient non trivial est $Z_c(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})/Z_{c-1}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$.
Ce quotient est abélien élémentaire, donc $Z_{c-1}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ contient

le sous-groupe de Frattini du groupe entier, c'est-à-dire $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$. Le groupe $Z_{c-1}(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})$ est un sous-groupe caractéristique de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ distinct du groupe entier et il contient le seul sous-groupe caractéristique maximal qui est $\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,n}$ (Proposition 4 du paragraphe II.5) ; il est donc confondu avec ce sous-groupe caractéristique maximal et la deuxième partie de la proposition est démontrée.

§2. Longueur de la suite des groupes dérivés de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Il est clair que le n-ième groupe dérivé de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est égal à $\{1\}$, par la formation même de $\mathcal{L}(r)_{p,n}$. Appelons ℓ_n la longueur de la suite dérivée de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

L'étude de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ a montré que $\ell_2 = 2$.

Supposons l'entier n au moins égal à 3, et supposons que pour tout entier m tel que $2 \leq m \leq n-1$, on ait $\ell_m = m$. Le dernier groupe dérivé de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ distinct de $\{1\}$ est un sous-groupe abélien normal de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.
Le théorème 8 nous montre qu'il est contenu dans

$$\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n} \quad ; \quad \text{d'où :}$$

$$\ell_n \geq \ell_{n-1} + 1 = n-1+1 = n .$$

Nous avons remarqué que $\ell_n \leq n$; donc $\ell_n = n$.

Quel est l'exposant du i-ème groupe dérivé $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})^{(i)}$? La démonstration que nous venons de faire indique que $(\mathcal{L}(r))^{(i)}$ appartient à $\mathcal{L}(r)_{p,i}$ mais n'appartient pas à $\mathcal{L}(r)_{p,i+1}$; ceci implique que $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})^{(i)}$ appartient à $\mathcal{L}(r)_{p,i}/\mathcal{L}(r)_{p,n}$ mais non à $\mathcal{L}(r)_{p,i+1}/\mathcal{L}(r)_{p,n}$ si $0 \leq i \leq n-1$. Le théorème 2 (I.3) montre que

$(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})^{(i)}$ a l'exposant p^{n-i}. D'où la :

Proposition 18 : La longueur de la suite des sous-groupes dérivés de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ est n ; le groupe $(\mathcal{L}(r)/\mathcal{L}(r)_{p,n})^{(i)}$ a pour exposant p^{n-i} $(0 \leq i \leq n)$.

En passant au quotient, on voit que si un p-groupe fini est de longueur de Frattini n, l'exposant de son i-ème groupe dérivé est au plus p^{n-i}.

§3. Ensemble des puissances p^j-èmes des éléments.

Si l'ensemble des puissances p^j-èmes des éléments d'un p-groupe G est lui-même un groupe, il en résulte que l'ensemble des puissances p^j-èmes des

éléments de tout quotient de G est lui-même un groupe. Si cette propriété était vraie pour un entier j tel que $1 \leq j \leq n-1$ dans le groupe $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$, elle serait vraie pour tout p-groupe à r générateurs au plus et de longueur de Frattini au plus n. Nous allons montrer qu'il n'en est rien.

Proposition 19 : Quel que soit l'entier j tel que $1 \leq j \leq n-1$, l'ensemble des p^j-èmes puissances des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ n'est pas un groupe ($n \geq 2$).

Démontrons la proposition dans le cas $n = 2$ et $j = 1$. Tout élément de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ dont la p-ième puissance est différente de 1 appartient à $\{\mathcal{L}(r)/\mathcal{L}(r)_{p,2}\} - \{\mathcal{L}(r)_{p,1}/\mathcal{L}(r)_{p,2}\}$ (lemme 1). Si x est un tel élément, et si nous utilisons les notations du paragraphe I.4, il existe un automorphisme θ_1 de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ qui applique x sur l'élément a_1 du système générateur $\{a_1, a_2, \ldots, a_r\}$ de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$; alors $x^p = \theta^{-1}(a_1^p)$. L'ensemble des puissances p-ièmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ est caractéristique. Si x^p appartenait au centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$, alors $a_1^p = \theta(x^p)$ appartiendrait aussi à ce centre. Nous avons vu au paragraphe III.4 (théorème 5) qu'il n'en était rien. L'intersection des puissances p-ièmes avec le centre $\mathcal{L}(r)/\mathcal{L}(r)_{p,2}$ est réduite à $\{1\}$. Si les puissances p-ièmes formaient un groupe, ce groupe serait caractéristique, donc normal et il aurait avec le centre une intersection non triviale [12 ; p.144] ce qui n'est pas le cas ici.

Passons au cas général. Si l'ensemble des p^j-èmes puissances des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$ formaient un groupe, l'ensemble des puissances p^j-èmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,j+1}$ formeraient un groupe. Montrons que ceci est impossible. Les éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,j+1}$ d'ordre au moins égal à p^{j+1} sont d'ordre exactement p^{j+1} et leur puissance p^{j-1}-ème appartient à $\mathcal{L}(r)_{p,j-1}/\mathcal{L}(r)_{p,j+1}$ (théorème 2). Les puissances p^j-èmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,j+1}$ forment un sous-ensemble de l'ensemble E des puissances p-ièmes des éléments de $\mathcal{L}(r)_{p,j-1}/\mathcal{L}(r)_{p,j+1}$. Nous avons vu que $\mathcal{L}(r)_{p,j-1}/\mathcal{L}(r)_{p,j+1}$ est isomorphe au groupe $\mathcal{L}(r')/\mathcal{L}(r')_{p,2}$ où $r' = \varphi(r,j,p)$ (paragraphe II.1). L'étude du cas $n = 2$, $j = 1$ vient de montrer que cet ensemble E a une intersection réduite à $\{1\}$ avec le centre de $\mathcal{L}(r)_{p,j-1}/\mathcal{L}(r)_{p,j+1}$.

Le centre de $\mathcal{L}(r)/\mathcal{L}(r)_{p,j+1}$ est contenu dans $\mathcal{L}(r)_{p,j}/\mathcal{L}(r)_{p,j+1}$

d'après le corollaire 4, donc il est contenu dans le centre de $\mathcal{L}(r)_{p,j-1}/\mathcal{L}(r)_{p,j+1}$ et il a avec l'ensemble E , donc a fortiori avec l'ensemble des puissances p^j-èmes des éléments de $\mathcal{L}(r)/\mathcal{L}(r)_{p,j+1}$ une intersection réduite à $\{1\}$. La démonstration s'achève comme dans le cas $n = 2$, $j = 1$.

§4. Pour finir, donnons une méthode permettant d'obtenir des représentations fidèles de $\mathcal{L}(r)/\mathcal{L}(r)_{p,n}$.

Soient H et K deux sous-groupes caractéristiques de $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ contenus dans $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$, tels que $H \subset K$ et que $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ n'induise pas l'identité sur K/H . De tels sous-groupes existent. Il suffit de prendre pour K et H deux termes non consécutifs de la suite centrale descendante de $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n}$ tels que $K \not\subset \mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$.

Le centralisateur de K/H dans $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ est un sous-groupe caractéristique de $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ qui n'est pas ce groupe lui-même.

Puisque $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ est isomorphe à $\mathcal{L}(r'')/\mathcal{L}(r'')_{p,2}$ où $r'' = \varphi(r,n,p)$ (paragraphe II.1), la proposition 4 indique que le centralisateur de K/H dans $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ est $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$.

Cherchons le centralisateur C de K/H dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$. Soit x un élément de C n'appartenant pas à $\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ et soit p^e l'ordre de x . Le théorème 2 indique que $e \geq 3$. Si x centralise K/H , alors $y = x^{p^{e-2}}$ centralise aussi K/H et y a pour exposant p^2 ; il appartient donc à

$$\{\mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}\} - \{\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}\} .$$

Mais aucun élément de ce dernier ensemble ne centralise K/H . Donc C ne possède aucun élément hors de $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$. Nous pouvons énoncer la :

Proposition 20 : Si H et K sont deux sous-groupes caractéristiques de $\mathcal{G} = \mathcal{L}(r)_{p,n-1}/\mathcal{L}(r)_{p,n+1}$ contenu dans $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$, tels que $H \subset K$ et que $\mathcal{G}$ ne centralise pas K/H , alors le centralisateur de K/H dans $\mathcal{L}(r)/\mathcal{L}(r)_{p,n+1}$ est $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$.

Puisque $\mathcal{L}(r)_{p,n}/\mathcal{L}(r)_{p,n+1}$ est un p-groupe abélien élémentaire, le groupe K/H peut être identifié à un espace vectoriel sur le corps à p

éléments. Les automorphismes intérieurs de $\mathfrak{L}(r)/\mathfrak{L}(r)_{p,n+1}$ induisent des applications linéaires de K/H .

La proposition 18 indique qu'on obtient ainsi une représentation fidèle de $\mathfrak{L}(r)/\mathfrak{L}(r)_{p,n}$.

Nous pouvons prendre par exemple $K = \mathfrak{G}_s$ et $H = \mathfrak{G}_{s+2}$ où :

$$2 \leq s < s+2 \leq \varphi(r,n,p)(p-1) + 1 .$$

Si $s = \varphi(r,n,p)(p-1) + 1$, le degré de la représentation est :

$$\varphi(r,n,p)^2 + \varphi(r,n,p) - 1$$

sauf si $p = 2$, $r = 2$, $n = 1$ où ce degré est 3 comme l'indiquent les propositions 10 et 12 et la proposition 8 .

BIBLIOGRAPHIE

1. E. ARTIN — Algèbre géométrique. Gauthier-Villars 1962.
2. N. BLACKBURN — On a special class of p-groups. Acta Mathematica 100 - (1958) ; 45-92.
3. S. DIXMIER — Exposants des quotients des suites centrales descendante et ascendante d'un groupe. C.R. Acad. Sc. Paris 259-(1964) ; 2751-2753 .
4. M. HALL Jr. — The theory of groups. Mac Millan (1959) .
5. Ph. HALL — A contribution to the theory of groups of prime power order. Proc. London Math.Soc. ser. 2-36-(1933) ; 29-95.
6. Ph. HALL — The classification of prime power groups. Journal für die reine und angew. Math 182-(1940) ; 130-141 .
7. Ph. HALL — Some sufficient condition for a group to be nilpotent . Illinois Journal of Math.2 (1958) ; 789-801 .
8. L. KALOUJNINE — Uber gewisse Beziehungen zwischen einer Gruppe und ihren Automorphismen. Berliner Math.Tag. (1953) ; 164-172.
9. M. LAZARD — Sur les groupes nilpotents et les anneaux de Lie. Ann. Sc. Ec. Norm.sup (3) 71-(1954) ; 101-190 .
10. E. SCHENKMAN — Group theory. Van Nostrand .
11. P. WEICHSEL — On critical p-groups. Proc. London Math. Soc.3 (14) (1964) ; 83-100 .
12. H. ZASSENHAUS — The theory of groups. Second edition. New-York (1958) .

(Texte reçu le 9 octobre 1969)

Mme Suzanne DIXMIER
64 rue Gay-Lussac
75 - PARIS 05

Joseph FLOCH, Maitre-Imprimeur à Mayenne - 20-2-1970 - n°3653