Séminaire Dubreil.
Algèbre et théorie
des nombres

Michel Lazard

Le mémoire de Hall et Higman sur la p-longueur des groupes p-résolubles

Séminaire Dubreil. Algèbre et théorie des nombres, tome 13, n° 2 (1959-1960), exp. n° 20, p. 1-10

<http://www.numdam.org/item?id=SD_1959-1960__13_2_A9_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
13e année, 1959/60, n° 20

LE MÉMOIRE DE HALL ET HIGMAN SUR LA p-LONGUEUR DES GROUPES p-RÉSOLUBLES [1]

par Michel LAZARD

Cet exposé ne prétend nullement être un résumé du mémoire de HALL et HIGMAN. Beaucoup d'énoncés ne seront même pas reproduits, et nous ne pourrons donner que des aperçus des démonstrations. Notre seul but est de donner une première idée des méthodes et des résultats contenus dans l'article en question, et de souligner son importance.

1. Notations et définitions.

Dans tout cet exposé, "groupe" signifiera "groupe fini".

L'ordre d'un groupe G (resp. d'un élément $x \in G$) sera noté $\mathrm{Ord}\, G$ (resp. $\mathrm{Ord}\, x$).

La notation " $N \lhd G$ " signifiera que N est un sous-groupe distingué du groupe G.

Nous désignerons par Π un ensemble de nombres premiers, par Π' l'ensemble complémentaire. Quand Π se réduira à un seul nombre premier p, nous écrirons p et p' au lieu de $\{p\}$ et $\{p\}'$. Si n est un entier naturel, la notation " $n \mid \Pi$ " signifiera que tous les facteurs premiers de n appartiennent à Π.

Un groupe G sera dit un Π-groupe si $\mathrm{Ord}\, G \mid \Pi$ (ce qui équivaut à $\forall\, x \in G$, $\mathrm{Ord}\, x \mid \Pi$).

Une suite de composition dans un groupe G est une suite croissante de sous-groupes, allant de l'élément neutre jusqu'à G, où chaque sous-groupe est distingué dans le suivant.

Une Π-suite dans un groupe G est une suite de composition dont tous les quotients sont des Π-groupes ou des Π'-groupes.

Un groupe G sera dit Π-résoluble s'il possède une Π-suite.

Un groupe est p-résoluble pour tout nombre premier p si et seulement s'il est résoluble (considérer une suite de Jordan-Hölder).

La Π-longueur d'un groupe Π-résoluble G est l'entier $\ell_\Pi(G)$, égal au nombre minimum de Π-groupes qui apparaissent comme quotients dans une Π-suite de G.

2. Π-suites descendantes et ascendantes d'un groupe Π-résoluble.

Pour tout G, définissons des sous-groupes $\Phi(G, \Pi)$ et $\Psi(G, \Pi)$.

$\Phi(G, \Pi)$ est le plus petit sous-groupe distingué de G tel que $G/\Phi(G, \Pi)$ soit un Π-groupe. On établit son existence en le définissant comme le sous-groupe engendré par les puissances n-ièmes de tous les éléments de G, où $n|\Pi$ et n est "assez grand" (c'est-à-dire divisible par le plus grand diviseur n_0 de Ord G tel que $n_0|\Pi$). Il résulte de cette seconde définition que, pour tout homomorphisme $f : G \to H$, on a

$$f(\Phi(G, \Pi)) \subset \Phi(H, \Pi)$$

$\Psi(G, \Pi)$ est le plus grand sous-groupe distingué de G qui soit un Π-groupe. On établit son existence en remarquant que le produit de 2 Π-sous-groupes distingués de G est encore un Π-sous-groupe distingué. Pour tout épimorphisme $f : G \to H$, on a

$$f(\Psi(G, \Pi)) \subset \Psi(H, \Pi) \quad .$$

Puisqu'on s'intéresse au nombre de Π-groupes quotients dans les Π-suites de G, on pourra supposer que les quotients extrêmes sont des Π'-groupes (éventuellement réduits à l'élément neutre).

Soit $A_0 = G \rhd A_1 \rhd A_2 \cdots \rhd A_n = 1$ une Π-suite du groupe Π-résoluble G. Si A_i/A_{i+1} est un Π-groupe (resp. un Π'-groupe) nous formerons une Π-suite qui décroît plus rapidement que (A_i) en posant $B_j = A_j$ pour $j \leqslant i$,

$$B_{i+1} = \Phi(A_i, \Pi) \subset A_{i+1} \quad (\text{resp. } B_{i+1} = \Phi(A_i, \Pi') \subset A_{i+1}),$$

$$B_j = B_{i+1} \cap A_j \qquad \text{pour} \qquad j > i \quad .$$

D'autre part, l'extension d'un Π-groupe par un Π-groupe est encore un Π-groupe. Il en résulte l'existence d'une Π-suite descendant plus vite que toutes les autres ; on l'obtient en posant $A_{i+1} = \Phi(A_i, \Pi)$ (resp. $A_{i+1} = \Phi(A_i, \Pi')$) pour i impair (resp. pair). L'entier $\ell_\Pi(G)$ est donc atteint pour une suite dont tous les sous-groupes sont distingués (et même complètement invariants) dans G.

Nous utiliserons au contraire la Π-suite ascendante, qui croît plus vite que toutes les Π-suites dont les sous-groupes sont distingués.

C'est la suite

$$(*) \qquad (1) = P_0 \lhd N_0 \lhd P_1 \dots P_i \lhd N_i \lhd P_{i+1} \lhd \dots \quad ;$$

que l'on obtient en posant $N_i/P_i = \Psi(G/P_i , \Pi')$ et $P_{i+1}/N_i = \Psi(G/N_i , \Pi)$, pour $i \geqslant 0$; $\ell_\Pi(G)$ est le plus petit entier i tel que $N_i = G$.

Nous conserverons les notations P_i, N_i dans cet exposé.

3. Introduction d'une représentation linéaire des groupes p-résolubles.

LEMME 1. - *Le sous-groupe P_1 contient son centralisateur modulo N_0.*

Autrement dit, P_1/N_0 contient son centralisateur dans G/N_0. Nous passerons donc au quotient, ce qui permet de supposer que $N_0 = (1)$. Soit Z le centralisateur de P_1. Si $P_1 \not\subset Z$, P_1 est un sous-groupe distingué de $P_1 Z$, distinct de $P_1 Z$. Choisissons un sous-groupe M, minimal pour les propriétés suivantes : $M \lhd G$, $P_1 \subsetneq M \subset P_1 Z$.

Puisque G est Π-résoluble, M/P_1 est un Π-groupe ou un Π'-groupe (d'après le thèorème de Jordan-Hölder appliqué aux suites de compositions dont tous les sous-groupes sont distingués). M/P_1 ne peut pas être un Π-groupe (car $P_1 = \Psi(G , \Pi)$), donc est un Π'-groupe. Donc (cf. [2], théorème 25, p. 132) il existe un sous-groupe X, tel que $XP_1 = M$, $X \cap P_1 = (1)$. Comme $X \subset P_1 Z$ et que Z centralise P_1, tout élément de X opère sur P_1, par automorphisme intérieur, comme un élément de P_1. Or P_1 est un Π-groupe, et $X \simeq M/P_1$ un Π'-groupe. Donc X centralise P_1, $M = X \times P_1$ (produit direct), X est caractéristique dans M, donc distingué dans G, contrairement aux hypothèses $X \neq (1)$, $\Psi(G , \Pi') = N_0 = (1)$.

Nous supposerons désormais que Π se réduit à un nombre premier p, et nous étudierons les groupes p-résolubles.

Rappelons d'abord quelques propriétés des p-groupes. Si G est un p-groupe, et si on définit son sous-groupe de Frattini F comme l'intersection des sous-groupes maximaux de G, alors on a les résultats suivants : F est engendré par les commutateurs (x , y) et les p-ièmes puissances x^p des éléments de G ; G/F est donc un p-groupe abélien élémentaire ; sa dimension, en tant qu'espace vectoriel sur le corps premier $\underset{\sim}{Z}_p$ est le nombre minimum de générateurs de G. Les automorphismes intérieurs de G induisent l'identité sur G/F, et tout automorphisme de G qui induit l'identité sur G/F a pour ordre une puissance de p.

LEMME 2. - Soient G un groupe p-résoluble, et F/N_0 le sous-groupe de Frattini du p-groupe P_1/N_0. Alors P_1/F est un espace vectoriel sur $\mathbb{Z}_p$, et les automorphismes de P_1/F induits par les automorphismes intérieurs de G fournissent une représentation fidèle de G/P_1.

Le noyau de la représentation de G dans P_1/F est un sous-groupe distingué $K \supset P_1$; K/P_1 ne peut pas être un p-groupe (d'après la définition de la p-suite ascendante). Donc, si $K \neq P_1$, il existe $g \in K - P_1$, d'ordre premier à p. Comme d'autre part g induit l'identité sur P_1/F, il doit induire l'identité sur P_1/N_0 donc il appartient à P_1, d'après le lemme 1 ; il y a contradiction, et $K = P_1$.

COROLLAIRE. - $\ell_p(G/F) = \ell_p(G)$.

En effet, si G/F contenait un p'-sous-groupe distingué $H/F \neq (1)$, les éléments de H centraliseraient P_1 modulo F, donc modulo N_0, donc appartiendraient à P_1 (lemme 1), ce qui est impossible. La p-suite ascendante de G/F est donc donnée par les sous-groupes P_i/F et N_i/F, ce qui démontre l'égalité $\ell_p(G/F) = \ell_p(G)$.

On notera par ailleurs la relation :

$$\ell_p(G/P_1) = \ell_p(G) - 1 \quad .$$

4. Relations entre la p-longueur d'un groupe p-résoluble et la structure de ses p-groupes de Sylow.

Soient G un groupe p-résoluble, et S un p-sous groupe de Sylow de G. Si nous prenons l'intersection avec S d'une p-suite de G, nous obtenons une suite de composition de S dont les quotients sont précisément les p-groupes parmi les quotients de la suite dans G (remarquer qu'on obtient des sous-groupes des quotients de la suite dans G, puis considérer les ordres). Il en résulte que l'entier $\ell_p(G)$ ne peut être grand que si S est "grand" ou "compliqué". L'essentiel du travail de HALL et HIGMAN consiste en des énoncés précis qui minorent, en fonction de $\ell_p(G)$, certains invariants de structure de S. Voici ces invariants :

(1) b_p, où p^{b_p} est l'ordre de S ;

(2) c_p, la classe de S (nombre minimum de quotients dans une suite centrale de S);

(3) d_p, longueur de la série dérivée de S (nombre minimum de quotients dans une suite de compsition à quotients abéliens);

(4) e_p, où p^{e_p} est l'exposant de S, c'est-à-dire l'ordre maximum de ses éléments.

Rappelons qu'un nombre premier de Fermat est de la forme $2^n + 1$, et un nombre premier de Mersenne de la forme $2^n - 1$.

Voici maintenant quelques-uns des théorèmes de HALL et HIGMAN.

THÉORÈME. - Si G est un groupe p-résoluble, et p un nombre premier impair, alors

(1) $\quad d_p \geq \ell_p$

(2) $\quad e_p \geq \ell_p$ si p n'est pas un nombre premier de Fermat

$\quad e_p \geq [\frac{1}{2}(\ell_p + 1)]$ si p est un nombre de Fermat.

De plus, ces inégalités sont les meilleures possibles.

THÉORÈME. - Si p est impair et n'est pas un nombre de Fermat :

(1) $$c_p \geq p^{\ell_p - 1} ,$$

(2) $$b_p \geq (p^{\ell_p} - 1)/(p - 1) .$$

Si p est un nombre de Fermat supérieur à 3 :

(1) $$c_p \geq ((p - 2)^{\ell_p} - 1)/(p - 3) ;$$

(2) $$b_p \geq ((p - 2)^{\ell_p + 1} - \ell_p(p - 3) - p + 2)/(p - 3)^2 .$$

Si p = 3 :

(1) $$c_p \geq 2^{\ell_p - 1}$$

(2) $$b_p \geq 2^{\ell_p - 1} + \ell_p - 1 .$$

Les démonstrations procèdent par récurrence sur l_p , en utilisant les relations $\ell_p(G/P_1) = \ell_p(G) - 1$, $\ell_p(G/F) = \ell_p(G)$, établies à la fin du numéro 3 .

Considérons généralement un groupe H d'automorphismes linéaires d'un espace vectoriel de dimension finie sur un corps de caractéristique p . Soit $g \in H$ d'ordre p^m . Alors $g^{p^m} - 1 = (g - 1)^{p^m} = 0$, ce qui montre que g est unipotent (a toutes ses valeurs propres égales à 1). De même $(g - 1)^{p^{m-1}} = g^{p^{m-1}} - 1 \neq 0$.

Le polynôme minimal de g est donc $(X-1)^r$, avec $p^{m-1} < r \leqslant p^m$. Cette double inégalité vérifiée par r ne peut évidemment pas être améliorée dans le cas général. Par contre HALL et HIGMAN ont obtenu des inégalités bien plus fines en faisant les hypothèses suivantes sur H : H est p-résoluble et ne contient pas de p-sous-groupe distingué non trivial. Ces hypothèses sont vérifiées quand H est le groupe G/P_1, considéré comme groupe d'automorphismes de P_1/F (notations du n° 3). Appelons alors "exceptionnel" un élément $g \in H$ d'ordre p^m tel que $r < p^m$, c'est-à-dire tel que $(g-1)^{p^m-1} = 0$. On a les résultats suivants :

Si $p \neq 2$ n'est pas un nombre de Fermat, alors g n'est pas exceptionnel.

Si p est un nombre de Fermat, alors $p^{m-1}(p-1) \leqslant r$ dans tous les cas, et g n'est pas exceptionnel si le 2-groupe de Sylow de H est abélien.

Si $p = 2$, alors $3.2^{m-2} \leqslant r$ dans tous les cas ; si $q = 2^{m_0} - 1$ est le plus petit nombre de Mersenne pour lequel H possède un q-sous-groupe non abélien, alors $q.2^{m-m_0} \leqslant r$; si H a des q-sous-groupes de Sylow abéliens pour tous les nombres de Mersenne inférieur à 2^m, alors g est non exceptionnel.

De plus, si les éléments g et h du même p-sous-groupe de Sylow S de H sont tous deux exceptionnels, alors les éléments d'ordre p dans les groupes cycliques engendrés par g et h commutent.

Contentons nous de dire que HALL et HIGMAN démontrent ces résultats par un dévissage fort long et ingénieux.

Montrons, par contre, comment ils en déduisent les relations entre e_p et ℓ_p (p impair).

Reprenons le groupe p-résoluble G, où nous supposerons $F = 1$. Alors G/P_1 opère sur P_1 par automorphismes intérieurs. Nous posons $h^g = g^{-1} h g$, $(g, g_1) = g^{-1} g_1^{-1} g g_1$. Nous notons additivement, un exposant, les opérateurs sur P_1.

LEMME 3. - Soient $g \in G$, $h \in P_1$, et soit q une puissance de p. Alors

$$(gh)^q = g^q \, h^{(g-1)^{q-1}}$$

$$((gh)^q, g^q) = h^{(g-1)^{2q-1}} .$$

On a, pour tout entier r :

$$(gh)^r = g^r\, h^{g^{r-1}}\, h^{g^{r-2}} \ldots h = g^r\, h^{g^{r-1}+\ldots+g+1} \quad .$$

Si $q = r$ est une puissance de p, on a, en caractéristique p (rappelons que P_1 est un groupe abélien élémentaire) :

$$g^{q-1} + g^{q-2} + \ldots + g + 1 = (g-1)^{q-1} \quad ,$$

d'où la première relation. Ensuite :

$$\begin{aligned}((gh)^q\ ,\ g^q) &= (g^q\, h^{(g-1)^{q-1}}\ ,\ g^q) = (h^{(g-1)^{q-1}}\ ,\ g^q) \\ &= h^{-(g-1)^{q-1}}\, h^{(g-1)^{q-1}}\, g^q = h^{(g-1)^{q-1}(g^q-1)} \\ &= h^{(g-1)^{2q-1}} \quad .\end{aligned}$$

Soit S un p-groupe, d'exposant m. Introduisons l'invariant $e^*(S)$ égal à $2m-1$ si toutes les puissances p^{m-1}-ièmes commutent dans S, et à $2m$ dans le cas contraire. Dans chaque cas, $e(S) = m = [\frac{1}{2}(e^*(S)+1)]$. Si S est un p-sous-groupe de Sylow d'un groupe G, nous posons

$$e_p^*(G) = e^*(S) \quad .$$

<u>Si</u> G/P_1 <u>contient un élément d'ordre maximum</u> gP_1 <u>non exceptionnel (pour la représentation sur</u> P_1 <u>) alors</u>

$$e_p(G) = e_p(G/P_1) + 1 \quad .$$

Soit un gP_1 d'ordre maximum p^m dans G/P_1. Si $g^{p^m} \neq 1$, alors

$$e_p(G) = e_p(G/P_1) + 1$$

(la relation $e_p(G) \leqslant e_p(G/P_1) + 1$ est évidente). Sinon, calculons $(gh)^{p^m}$ pour $h \in P_i$. Nous avons, d'après le lemme 3 :

$$(gh)^{p^m} = h^{(g-1)^{p^m}-1} \quad ,$$

et dire que gP_1 n'est pas exceptionnel signifie précisément qu'il existe $h \in P_1$ avec $h^{(g-1)^{p^m}} \neq 1$.

Nous en déduisons tout de suite, par récurrence sur ℓ_p (le cas $\ell_p = 1$ étant trivial), la relation

$$e_p(G) \geqslant \ell_p(G) \quad ,$$

<u>dans le cas où</u> $p > 2$ <u>n'est pas un nombre de Fermat</u> (il n'y a pas d'élément exceptionnel).

Si maintenant p est un nombre de Fermat, démontrons de même la relation

$$e_p^*(G) \geqslant \ell_p(G) \quad .$$

Supposons d'abord $e_p^*(G/P_1) = 2m$. Alors tous les éléments de G/P_1 ne peuvent pas être exceptionnels, puisque les puissances p^{m-1}-ièmes ne commutent pas, et on voit comme précédemment que

$$e_p(G) = m + 1 ,$$

donc

$$e_p^*(G) \geqslant 2m + 1 = e_p^*(G/P_1) + 1 \quad .$$

Supposons maintenant $e_p^*(G/P_1) = 2m - 1$. Si l'exposant de G est $m + 1$, $e_p^*(G) \geqslant 2m + 1 = e_p^*(G/P_1) + 2$. Sinon l'exposant de G est m , et, pour démontrer que $e_p^*(G) = 2m$, il nous faut démontrer que toutes les puissances p^{m-1}-ièmes ne commutent pas dans G . Soit $g \in G$ tel que gP_1 soit d'ordre p^m . Nous avons, d'après le lemme 3 :

$$((gh)^{p^{m-1}} , g^{p^{m-1}}) = h^{(g-1)2p^{m-1}-1} \quad .$$

Mais nous savons que le polynôme minimal annulé par l'opérateur associé à g est $(X - 1)^r$, où $r \geqslant (p - 1)\, p^{m-1} \geqslant 2p^{m-1}$, puisque $p \geqslant 3$. Par définition, il existe alors $h \in P_i$, tel que

$$h^{(g-1)2p^{m-1}-1} \neq 1 \quad .$$

Dans tous les cas, nous avons donc $e_p^*(G) \geqslant e_p^*(G/P_1) + 1$, et les relations : $e_p^*(G) \geqslant \ell_p(G)$, $e_p(G) \geqslant [\frac{1}{2}(\ell_p(G) + 1)]$ en résultent par récurrence sur ℓ_p .

5. Applications au problème de Burnside.

Désignons par (S_n) l'énoncé suivant :

(S_n) Il existe, pour chaque entier positif k , un entier $s_{n,k}$ tel que tout groupe résoluble d'exposant n qui peut-être engendré par n éléments ait un ordre au plus égal à $s_{n,k}$.

Parmi les résultats de HALL et HIGMAN, nous signalerons le théorème suivant :

THÉORÈME. - (S_n) est vrai pourvu que (S_q) soit vrai pour chaque puissance de nombre premier q divisant n .

Disons qu'un classe C de groupes (finis), ou, plus précisément, de types d'isomorphismes de groupes, a la propriété de Burnside si, pour tout entier k, il n'y a qu'un nombre fini de groupes de C (aux isomorphismes près) qui peuvent être engendrés par k éléments.

Soient C_1 et C_2 deux classes de groupes. Désignons par $C_1\ C_2$ la classe des groupes G qui ont un sous-groupe normal N tel que G/N appartienne à C_1 et à C_2.

LEMME 4. - Si C_1 et C_2 ont la propriété de Burnside, il en est de même de $C_1\ C_2$.

Soit G un groupe, $N \lhd G$, $G/N \in C_1$, $N \in C_2$. Si G, donc G/N, a k générateurs, l'ordre de G/N est majoré par un entier $n(k)$. D'après un théorème Schreier sur les sous-groupes des groupes libres, N peut-être engendré par $k' = 1 + n(k)(k - 1)$ éléments. Son ordre est donc majoré par un entier $n'(k')$, et celui de G par $n(k)\ n'(k')$.

COROLLAIRE. - Si $C_1, \ldots, C_r$ sont des classes ayant toutes la propriété de Burnside, il en est de même de $C_1, \ldots, C_3$, où le produit est calculé après introduction de parenthèses, d'une manière quelconque.

En ce qui concerne les parenthèses, on peut remarquer que $(C_1\ C_2)\ C_3 \subset C_1(C_2\ C_3)$. Il suffit donc d'introduire les parenthèses à droite.

Démontrons maintenant le théorème par récurrence sur le nombre de facteurs premiers de n. Si ce nombre est 1, rien à démontrer. Sinon n a au moins un facteur premier impair, soit p. Posons $n = p^e m$, m non divisible par p. La p-longueur d'un groupe résoluble d'exposant n est au plus $2e$. Ainsi, si l'on note C_n la classe des groupes résolubles d'exposant n.

$$C_n \subset C_m\ C_{p^e}\ C_m \cdots C_m\ C_{p^e}\ C_m \quad ,$$

avec $(4e + 1)$ facteurs. C_{p^e} a la propriété de Burnside par hypothèse, et C_m d'après la récurrence. Il en est donc de même de C_n, ce qui constitue l'énoncé (S_n).

BIBLIOGRAPHIE

[1] HALL (Philip) and HIGMAN (Graham). - On the p-length of p-soluble groups and reduction theorems for Burnside's problem, Proc. London math. Soc., Series 3, t. 6, 1958, p. 1-42.

[2] ZASSENHAUS (Hans). - The theory of groups. 2nd edition. - Göttingen, Vandenhoeck and Ruprecht ; New York, Chelsea, 1958.