Séminaire Dubreil.
Algèbre et théorie
des nombres

Marie-Paule Brameret

Groupes finis d'ordre impair

Séminaire Dubreil. Algèbre et théorie des nombres, tome 15, n° 1 (1961-1962), exp. n° 10, p. 1-11

<http://www.numdam.org/item?id=SD_1961-1962__15_1_A7_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
15e année, 1961/62, n° 10

5 février 1962

GROUPES FINIS D'ORDRE IMPAIR

par Mlle Marie-Paule BRAMERET.

Lorsque cet exposé a été fait, le mémoire de Walter FEIT et de John G. THOMPSON [1] intitulé "Solvability of groups of odd order", et désigné dans la suite par M_1, n'avait pas encore paru. Ce mémoire a fait l'objet d'une communication de J. G. THOMPSON, au congrès de Stockholm, en août 1962, sous le titre suivant : "Two results about finite groups".

Le but poursuivi par W. FEIT et J. G. THOMPSON est de démontrer le résultat suivant :

THÉORÈME. - Tout groupe fini d'ordre impair est résoluble.

La démonstration de ce théorème se trouve dans [1].

Le résultat principal de M_1 est le théorème suivant :

THÉORÈME. - Il n'existe pas de groupe simple minimal d'ordre impair, en appelant "groupe simple minimal" un groupe simple non cyclique dont tous les sous-groupes propres sont résolubles.

La démonstration de ce théorème se fait par l'absurde. Supposant l'existence d'un groupe simple minimal G d'ordre impair, on en donne une caractérisation vis-à-vis de ses sous-groupes maximaux. On montre ensuite que G satisfait à des conditions qui, elles, ne peuvent être vérifiées par aucun groupe.

Cet exposé n'est pas un résumé du travail de W. FEIL et J. G. THOMPSON. J'essaierai de donner une idée des méthodes et des résultats contenus dans les trois premiers chapitres de M_1. Ces résultats sont de deux sortes ; ils concernent :

1° La structure des groupes finis : au paragraphe 2, les démonstrations de deux lemmes sont données.

2° La théorie des caractères : au paragraphe 3, on définit les sous-ensembles "faiblement plongés" d'un groupe, ceci indépendamment de la parité de l'ordre du groupe.

1. Notations. Rappels.

Dans cet exposé groupe signifiera groupe fini. On note Ord G l'ordre d'un groupe G ; Ord x l'ordre d'un élément x de G .

π désignera un ensemble de nombres premiers et π' l'ensemble complémentaire. Lorsque π se réduit à un seul élément p , on écrira p et p' au lieu de $\{p\}$ et $\{p'\}$.

Un π-groupe G est un groupe tel que tous les facteurs premiers de Ord G appartiennent à π . Si x et $y \in G$, on désigne par $[x , y]$ le commutateur $x^{-1} y^{-1} xy$ de x et y .

Pour $n \geqslant 3$, on pose

$$[x_1 , \dots , x_n] = [[x_1 , \dots , x_{n-1}]x_n]$$

où $x_i \in G$, $i = 1 , 2 , \dots , n$.

Un groupe nilpotent G est dit de classe c si chaque commutateur $[a_1 , \dots , a_{c+1}] = 1$.

Rappelons le théorème [cf. [2]].

THÉORÈME 1. - Soit G un groupe (non nécessairement nilpotent). Si H et K sont deux sous-groupes normaux de G , H étant nilpotent de classe c et K nilpotent de classe d , le groupe HK engendré par H et K est nilpotent de classe c + d .

Si H et K sont deux sous-groupes d'un groupe G , on désigne par $[H , K]$ le groupe engendré par les commutateurs $[h , k]$ où $h \in H$ et $k \in K$.

Si $H_1 , H_2 , \dots , H_n$ sont des sous-groupes de G , on pose, pour $n \geqslant 3$,

$$[H_1 , \dots , H_n] = [[H_1 , \dots , H_{n-1}] , H_n] \quad ;$$

G' désignera le groupe dérivé $[G , G]$ de G .

Si H est une partie d'un groupe G , C(H) est le centralisateur de H dans G . Si K est une autre partie de G , on pose $C_K(H) = C(H) \cap K$.

Un sous-groupe H est dit self-centralisant si $H = C(H)$. $S \subset N(G)$ est l'ensemble des sous-groupes normaux self-centralisants de G .

Dans [6] est démontré le théorème suivant.

THÉORÈME 2. - Si G est un groupe nilpotent et si E est un sous-groupe normal abélien de G, E est contenu dans un élément de $S \subset N(G)$.

On désigne par $N(S)$ le normalisateur d'un sous-ensemble S de G et par $N_T(S)$ l'ensemble $T \cap N(S)$ où T est un second sous-ensemble de G.

On désignera par $m(G)$ le nombre minimal de générateurs d'un groupe G.

Si G est un p-groupe, $\Omega(G)$ représente le sous-groupe de G engendré par les éléments d'ordre p. $\Omega(G)$ est un sous-groupe caractéristique de G.

On appelle p-groupe élémentaire, un groupe abélien d'exposant p.

Un p-groupe G est dit régulier si, pour tous les couples d'éléments a et b de G et tous les entiers $n = p^\alpha$, il existe des éléments $s_1, s_2, \dots, s_t$, appartenant au groupe dérivé du groupe engendré par a et b de telle sorte que l'on ait

$$(ab)^n = a^n b^n s_1^n \dots s_t^n \quad .$$

Dans [2] sont démontrés les théorèmes suivants.

THÉORÈME 3. - Un p-groupe de classe inférieure à p est régulier.

THÉORÈME 4. - Dans un p-groupe régulier, l'ordre d'un produit $a_1 \times a_2 \times \dots \times a_r$ est inférieur à l'ordre de l'un au moins des facteurs $a_1, \dots, a_r$.

2. Quelques résultats concernant la structure des groupes finis d'ordre impair.

LEMME 1. - Soit G un p-groupe, p impair. Soit H un élément de $S \subset N(G)$ pour lequel $m(H)$ est maximal. On a

$$\Omega[C[\Omega(H)]] = \Omega(H) \quad .$$

Remarque. - L'hypothèse faite sur la parité de p est nécessaire, G étant, naturellement, non abélien (sinon, le lemme est trivial). En effet, prenons pour G le groupe dihédral d'ordre 16. G est engendré par deux éléments a et b avec les relations :

$$a^8 = 1 \qquad b^2 = 1 \qquad ba = a^{-1} b \quad .$$

Les sous-groupes self-centralisants de G sont cycliques.

Soit $A = \{a\}$, on a

$$A \lhd G \quad \text{et} \quad \Omega(A) = \{a^4 , 1\} \quad .$$

L'élément a appartient à $C[\Omega(A)]$. D'autre part, on a :

$$ba^4 = a^4 b$$

d'où

$$b \in C[\Omega(A)] \quad .$$

Par suite, G est égal à $C[\Omega(A)]$. Mais $b \in \Omega[G]$ et $b \notin \Omega(A)$. On a donc l'inclusion stricte

$$\Omega(A) \subset \Omega[C[\Omega(A)]] \quad .$$

Démonstration. - Les groupes H et $\Omega(H)$ sont abéliens et l'on a

$$H \lhd G \qquad \Omega(H) \lhd G$$

$$m(H) = m[\Omega(H)] \quad .$$

Posons

$$D = \Omega[C[\Omega(H)]] \quad ;$$

on a, alors, $D \lhd G$.

La démonstration se fait par l'absurde ; on suppose que $\Omega(H) \not\subseteq D$.

(i) S'il existe un sous-groupe normal E de G tel que l'on ait

$$\Omega(H) \subset E \subseteq D$$

$$|E:\Omega(H)| = p \quad ,$$

alors $\Omega(H)$ est contenu dans le centre de E et E est abélien. De l'égalité $|E:\Omega(H)| = p$, il suit :

$$m(E) = 1 + m[\Omega(H)] = 1 + m(H) \quad .$$

D'après le théorème 1, il existe un élément A de $S \subset N(G)$ contenant E ; d'où $m(A) > m(H)$, ce qui contredit le choix de H.

(ii) L'existence d'un tel sous-groupe E et, par suite, l'absurdité de l'inclusion stricte $\Omega(H) \subset D$ découlera du fait que D est d'exposant p.

En effet supposons l'exposant de D égal à p.

$\frac{G}{\Omega(H)}$ est un p-groupe et $\frac{D}{\Omega(H)}$ est un sous-groupe normal de $\frac{G}{\Omega(H)}$; par conséquent, l'intersection de $\frac{D}{\Omega(H)}$ et du centre de $\frac{G}{\Omega(H)}$ est différent de l'unité.

Soit $x\Omega(H)$ un élément de cette intersection et soit E le sous-groupe de G engendré par $\Omega(H)$ et x. On a :

$$|E:\Omega(H)| = p$$

$$\Omega(H) \subset E \subseteq D$$

et E est un sous-groupe normal de G.

C. Q. F. D.

(iii) Il suffit donc de démontrer que D est d'exposant p. Soit x un élément de $C[\Omega(H)]$ d'ordre p. Soit

$$B_1 = \langle \Omega(H) , x \rangle$$

le sous-groupe de G engendré par $\Omega(H)$ et x ; B_1 est abélien.

$\langle H , x \rangle$ étant un p-groupe, il existe une suite :

$$B_1 \lhd B_2 \lhd \dots \lhd B_n = \langle H , x \rangle$$

dans laquelle

$$|B_{i+1}:B_i| = p \qquad i = 1 , 2 , \dots , n - 1 \quad .$$

On montre, par récurrence, que $B_1 \lhd B_n$. Supposons que $B_1 \lhd B_m$; B_1 et $H \cap B_m$ sont des sous-groupes abéliens et normaux de B_m ; ils sont par suite nilpotents, de classe c. D'autre part, B_1 et $H \cap B_m$ engendrent B_m. D'après le théorème 1, B_m est un groupe nilpotent de classe 2. Puisque $2 < p$, il résulte du théorème 3 que B_m est régulier.

Soit $z \in \Omega[B_m]$. On a $z = ax^k$ avec $a \in H$ et k entier. D'où

$$a = zx^{-k}$$

B_m étant régulier :

$$\text{ord } a \leqslant \text{ord}(z) \quad \text{ou} \quad \text{ord } a \leqslant \text{ord}(x^{-k}) \quad .$$

Par suite $\text{ord } a = 1$ ou p. Donc $a \in \Omega(H)$ et $z \in B_1$. On a donc

$$\Omega(B_m) \subseteq B_1 \quad .$$

Il est évident que $B_1 \subseteq \Omega(B_m)$. Donc :

$$B_1 = \Omega(B_m) \lhd B_{m+1} \quad .$$

Par conséquent, quel que soit $x \in D$, $\langle \Omega(H) , x \rangle$ est un sous-groupe normal de $\langle H , x \rangle$.

On en déduit que $[D , D]$ est contenu dans $C(H) = H$, et que $[H , D] \subseteq \Omega(H)$. D'où

$$[D , D , D] \subseteq \Omega(H) \quad .$$

Puisque $D \subseteq C[\Omega(H)]$, c'est-à-dire que $[\Omega(H) , D] = 1$, on a :

$$[D , D , D , D] = 1 \quad .$$

D est par conséquent un p-groupe de classe $\leqslant 3$.

Si $p \geqslant 5$, on en déduit que D est régulier et, comme il est engendré par des éléments d'ordre p, son exposant est égal à p.

Supposons que $p = 3$. Il suffit de montrer que les éléments de D, d'ordre 3,

forment un groupe. S'il n'en n'était pas ainsi, il existerait un sous-groupe $\langle x , y\rangle$ de D minimal pour les relations : $x^3 = y^3 = 1$, $(xy)^3 \neq 1$. On peut écrire :

$$(xy)^3 = y[y , x]^2 [y , x , x] y[y , x] y \quad .$$

Or

$$\langle y , x^{-1} yx\rangle \subsetneq \langle x , y\rangle \quad .$$

Par suite l'élément $[y , x]$ de $\langle y , x^{-1} yx\rangle$ est d'ordre 3 . Puisque $[y , x]$ appartient à D' et, donc, à H , $[y , x]$ est élément de $\Omega(H)$. Il commute avec x et y . On a alors

$$(xy)^3 = y^3[y , x]^3 = 1 \quad .$$

Par conséquent l'exposant de D est égal à p .

Dans [3], P. HALL appelle <u>groupe de stabilité</u> A d'une chaîne :

$$G_0 = G \supseteq G_1 \supseteq \ldots \supseteq G_n = 1$$

de sous-groupes d'un groupe G , le groupe des automorphismes α de G tels que :

$$\alpha[G_i x] = G_i x$$

pour tous les éléments x de G_{i-1} .

Si G est un π-groupe, on montre, par récurrence sur n , que A est un π-groupe.

LEMME 2. - Soit G un p-groupe, p impair. Soit E un sous-groupe élémentaire de G . Si α est un p'-automorphisme de G qui est trivial sur $\Omega[C(E)]$, alors $\alpha = 1$.

<u>Démonstration</u>. - α , étant trivial sur $\Omega[C(E)]$, est trivial sur E . Donc $C(E)$ est α-invariant. La restriction de α à $C(E)$ est alors l'identité

(cf. [4], HILFSSATZ 1.5). Si $C(E) = G$, le lemme est démontré. Supposons $C(E) \subsetneq G$. Il existe une suite

$$B_1 = C(E) \lhd B_2 \lhd \dots \lhd B_n = G \quad .$$

Supposons que α soit trivial sur B_m avec $m < n$.

Pour tout $y \in B_{m+1}$, on a

$$y^{-1}\, \alpha(y) \in C(B_m) \quad .$$

Il en résulte que α stabilise la chaîne :

$$B_{m+1} \supset C(B_m) \supset 1 \quad .$$

La restriction de α à B_{m+1} , étant à la fois un p-automorphisme et un p'-automorphisme, est l'identité. Par suite, α est l'automorphisme identique de G .

3. Sous-ensembles faiblement plongés d'un groupe.

Par "caractère" d'un groupe G , on entendra "caractère complexe" de G . Un caractère généralisé est une combinaison linéaire de caractères dont les coefficients sont entiers. On peut définir sur l'ensemble des caractères généralisés de G une structure d'anneau. Cet anneau est muni d'une structure métrique dérivée du produit intérieur :

$$(\alpha\ ,\ \beta)_G = \frac{1}{\operatorname{ord} G} \sum_{x \in G} \alpha(x)\ \overline{\beta(x)} \quad .$$

On pose

$$\|\alpha\|_G^2 = (\alpha\ ,\ \alpha)_G \quad .$$

Si $\mathbb{S}$ est un ensemble de caractères généralisés d'un groupe G , $\mathbb{C}(\mathbb{S})$ [resp. $\mathfrak{Z}(\mathbb{S})$] désigne l'ensemble des combinaisons linéaires complexes [resp. entières] d'éléments de $\mathbb{S}$.

Soient :

$$\mathcal{C}_0(\mathbb{S}) = \{\alpha\ ,\ \alpha \in \mathcal{C}(\mathbb{S})\ ,\ \alpha(1) = 0\}$$

$$\mathcal{J}_0(\mathbb{S}) = \{\alpha\ ,\ \alpha \in \mathcal{J}(\mathbb{S})\ ,\ \alpha(1) = 0\} \quad .$$

On appelle fonction de classe de G , une application à valeurs complexes α vérifiant :

$$\alpha(y^{-1}\, xy) = \alpha(x)$$

pour tous les éléments x et y de G .

Si H est un sous-groupe de G et si α est une fonction de classe de H , on désigne par α^* la fonction de classe de G induite par α .

Si K est une partie de G contenant l'élément unité 1 , on désigne par $K^{\#}$ le complémentaire de 1 dans K .

Il s'agit de définir une isométrie appliquant certains sous-ensembles de l'anneau des caractères d'un sous-groupe L de G dans l'anneau des caractères de G . Pour cela, on introduit la notion de sous-ensembles faiblement plongés dans G . Si $\hat{L}$ est un tel sous-ensemble avec $L = N(\hat{L})$, on désigne par $\mathfrak{L}$ l'ensemble des caractères généralisés du sous-groupe L qui s'annulent hors de $\hat{L}$.

Définition. - Soit $\hat{L}$ un sous-ensemble d'un groupe G tel que

$$1 \in \hat{L} \subseteq N(\hat{L}) = L \quad ;$$

Soit

$$L_0 = \{\ell\ ,\ \ell \in \hat{L}\ ;\ c(\ell) \subseteq L\}$$

et soit

$$D = \hat{L}^{\#} - L_0 \quad .$$

$\hat{L}$ est dit faiblement plongé dans G si les conditions suivantes sont satisfaites :

1° Dès que deux éléments de $\hat{L}$ sont conjugués dans G , ils sont conjugués

dans L .

2° Si D n'est pas vide, il existe des sous-groupes, autres que le sous-groupe unité, H_1 , H_2 , ... , H_n de G , $n \geqslant 1$, possédant les propriétés suivantes :

a. $(\text{ord } H_i , \text{ord } H_j) = 1$ pour $i \neq j$;

b. H_i est un S-sous-groupe de $N_i = N(H_i)$;

c. $N_i = H_i(L \cap N_i)$ et $H_i \cap L = 1$;

d. $(\text{ord } H_i , \text{ord } C_L(\ell)) = 1$ pour $\ell \in \hat{L}^{\#\#}$;

e. Pour $1 \leqslant i \leqslant n$, on pose

$$\hat{N}_i = \{ \bigcup_{h \in H_i^{\#\#}} C_{N_i}(h) \} - H_i^{\#\#}$$

et alors, pour tout $x \in G$, on a

$$\text{soit} \qquad x^{-1} \hat{N}_i x \cap \hat{N}_i = 1$$

$$\text{soit} \qquad x^{-1} \hat{N}_i x = \hat{N}_i \quad .$$

De plus,

$$N_i = N(\hat{N}_i) \quad .$$

3° Si $\ell_0 \in D$, il existe un conjugué ℓ de ℓ_0 dans $\hat{L}$ et un indice i tel que :

$$C(\ell) = C_{H_i}(\ell) . C_L(\ell) \subseteq N_i \quad .$$

Le plus simple exemple d'ensemble faiblement plongé dans un groupe G est un <u>T. I.-ensemble</u> $\hat{L}$, ensemble à intersection trivial dans G [c'est-à-dire un ensemble $\hat{L}$ tel que, pour tout $x \in G$, on ait : soit $x^{-1} \hat{L} x = \hat{L}$, soit $x^{-1} \hat{L} x \cap \hat{L} \subseteq \langle 1 \rangle$] vérifiant en outre la condition :

$$\langle 1 \rangle \subseteq \hat{L} \subseteq N(\hat{L}) = L \quad .$$

Dans [5], M. SUZUKI a montré que si $\hat{L}$ était un T. I.-ensemble de G ,

l'application τ de $\mathcal{C}_0(\hat{L})$ dans l'anneau des caractères de G définie par

$$\alpha^\tau = \alpha^*$$

est une isométrie.

Ce résultat est généralisé, en considérant, au lieu de T. I.-ensembles, des ensembles faiblement plongés de G et, d'autre part, en étendant l'isométrie τ, sous certaines conditions, à de plus grands sous-ensembles de $\mathcal{C}(\hat{L})$.

BIBLIOGRAPHIE

[1] FEIT (W.) and THOMPSON (J. G.). - A solvability criterion for finite groups and some consequences (à paraître).

[2] HALL (Marshall, Jr). - The theory of groups. - New York, Macmillan Company, 1959.

[3] HALL (Philip). - Some sufficient conditions for a group to be nilpotent, Illinois J. Math., t. 2, 1958, p. 787-801.

[4] HUPPERT (B.). - Gruppen mit modularer Sylow-Gruppe, Math. Z., t. 75, 1961, p. 140-153.

[5] SUZUKI (M.). - On finite groups with cyclic Sylow-subgroups for all odd primes, Amer. J. Math., t. 77, 1955, p. 657-691.

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