Séminaire Dubreil.
Algèbre et théorie
des nombres

Richard Brauer

Les groupes d'ordre fini et leurs caractères

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 1 (1958-1959), exp. n° 6, p. 1-16

<http://www.numdam.org/item?id=SD_1958-1959__12_1_A6_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1958/59
-:-:-:-

5 et 6 janvier 1959

LES GROUPES D'ORDRE FINI ET LEURS CARACTÈRES

par Richard BRAUER

Soient G un groupe d'ordre fini et H un sous-groupe. Nous pouvons poser la question : combien d'informations pouvons-nous obtenir sur G si nous connaissons H ? Cela sera d'importance si nous voulons appliquer l'induction pour prouver des théorèmes dans la théorie des groupes d'ordre fini. Mais il est évident qu'il est nécessaire de modifier le problème, parce que, étant donné H, nous aurons une multitude extrêmement grande de groupes G qui contiennent H, et on ne peut pas espérer que tous ces G auront beaucoup de propriétés en commun. FROBENIUS est un des premiers mathématiciens qui aient considéré le problème dans un mémoire célèbre vers la fin du dernier siècle. Ce mémoire est instructif pour nous sous plusieurs rapports.

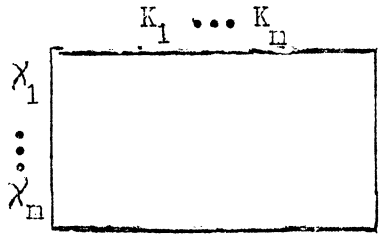
Premièrement, pour appliquer les résultats de FROBENIUS, il est nécessaire de savoir quelque chose sur la "position" du sous-groupe H dans G. Dans le cas de Frobenius, il faut qu'on sache comment les classes des éléments conjugués de H sont distribuées dans les classes de G. Une autre possibilité, c'est de supposer que H joue un rôle particulier dans G. Par exemple, nous pouvons supposer que H est le centralisateur $C(\sigma)$ d'un élément σ de G. Cela veut dire que H est le sous-groupe des éléments de G permutables avec σ. C'est cette hypothèse particulière qui sera importante pour nous plus tard.

Un autre point d'intérêt pour nous dans le travail de FORBENIUS, c'est qu'il s'agit de relations entre les caractères de H et ceux de G. Il me semble que la théorie des caractères nous offre le seul langage dans lequel nous pouvons exprimer des propriétés plus profondes des groupes d'ordre fini.

Je veux montrer que nous pouvons obtenir beaucoup d'informations sur les caractères de G, si nous connaissons les caractères de certains sous-groupes de G. Rappelons qu'un groupe G d'ordre fini g a n caractères irréductibles $\chi_1, \chi_2, \ldots, \chi_n$ où n est le nombre des classes $K_1, K_2, \ldots, K_n$

d'éléments conjugués de G. Ces caractères χ_i sont des fonctions à valeurs complexes sur G qui sont constantes dans chaque classe K_j. Nous pouvons disposer les valeurs des caractères en une table

(1)



Les résultats qui forment le sujet de cette conférence sont d'une nature arithmétique. Soit p un nombre premier qui restera fixe désormais. Nous supposons que p divise l'ordre g du groupe, et posons

$$g = p^n g_0 \qquad \text{où} \qquad (p\ ,\ g_0) = 1 \quad . \tag{2}$$

On sait que G possède des sous-groupes P d'ordre p^n, les sous-groupes de Sylow.

Peut-être puis-je indiquer la direction générale de ces recherches en discutant d'abord le cas spécial $n = 1$, cas dans lequel les résultats sont plus précis. Soit $N = N(P)$ le normalisateur d'un sous-groupe P de Sylow. Ce N se compose des éléments $\sigma \in G$ tels que $P\sigma = \sigma P$. Arrangeons les caractères χ_i de G en prenant d'abord les caractères χ_i, dont le degré $x_i = \chi_i(1)$ est premier à p, et puis les autres caractères. Prenons d'abord les classes K_j "p-régulières". Ce sont les classes dans lesquelles l'ordre des éléments est premier à p. Ainsi, la table (1) apparaît sous la forme

	classes K_j p-régulières	classes K_j p-singulières
caractères χ_i de degré x_i premier à p	I	II
caractères χ_i de degré x_i divisible par p	III	IV

Les résultats sont les suivants :

1° Dans la partie IV, toutes les valeurs sont 0

2° La partie II est à peu près égale à la partie correspondante de la table des caractères du groupe N, pourvu que l'arrangement des caractères et des classes soit convenable. Pour avoir égalité stricte, il faut multiplier chaque caractère χ_i par un signe $\delta_i = \pm 1$ convenable.

Du reste les relations d'orthogonalité des caractères donnent quelque information sur les parties I et III. Aussi, chaque élément p-singulier σ de G peut se mettre sous la forme

$$\sigma = \pi \sigma_0$$

où π et σ_0 sont des puissances de σ telle que π a l'ordre p et σ_0 a un ordre premier à p. Si $\mathfrak{p}$ est un idéal premier divisant p dans le corps engendré par les valeurs de χ_i, on voit facilement que

$$\chi_i(\sigma) \equiv \chi_i(\sigma_0) \pmod{\mathfrak{p}} . \tag{3}$$

Cela aussi donne des renseignements sur les parties I, III.

Par exemple, si le caractère χ_i de degré $x_i \not\equiv 0 \pmod p$ correspond au caractère $\tilde{\chi}_i$ de degré $\tilde{x}_i$ de N, nous aurons $\delta_i x_i \equiv \tilde{x}_i \pmod p$.

Il y a beaucoup de groupes pour lesquels ces résultats suffisent pour déterminer tous les caractères. Souvent, il suffit de connaître l'ordre g et un peu d'information supplémentaire. (Naturellement, il est nécessaire qu'il y ait des nombres premiers p qui divisent g avec l'exposant exact 1). Par exemple, si nous prenons les ordres g des groupes de Mathieu

$$7\,920 , 95\,040 , 443\,520 , 10\,200\,960 , 244\,823\,040$$

et si nous supposons que G soit simple, il a été démontré par R. G. STANTON en 1948 que les carctères de G sont déterminés complètement, d'où on peut démontrer que G est isomorphe au groupe de Mathieu du même ordre.

Je me suis intéressé depuis quelque temps à la généralisation de ces résultats dans le cas $n > 1$. Je veux indiquer ce que l'on peut démontrer, quoique je n'aie pas réussi à donner des résultats aussi précis que dans le cas $n = 1$.

Commençons par formuler les faits les plus simples de la théorie des représentations des groupes d'ordre fini. Etant donné le groupe G, nous pouvons former

l'algèbre de groupe Γ de G. C'est une algèbre associative Γ sur un corps quelconque Ω qui a une base dont les éléments forment un groupe multiplicatif isomorphe à G. En identifiant ces éléments avec les éléments de G nous pouvons écrire l'élément général $\gamma \in \Gamma$ sous la forme

$$\gamma = \sum_{\sigma \in G} a_\sigma \, \sigma \tag{4}$$

où les a_σ sont des éléments arbitraires de Ω.

Si Ω a la caractéristique 0, l'algèbre Ω est semi-simple et alors somme directe d'algèbres simples,

$$\Gamma = S_1 \oplus S_2 \oplus \ldots \oplus S_r \quad . \tag{5}$$

Si Ω est algébriquement clos, chaque algèbre simple S_i est isomorphe à une algèbre complète de matrices avec des coefficients dans Ω. L'homomorphisme canonique de Γ sur S_j nous donnera une représentation de Γ par des matrices ou, si nous le préférons par des transformations linéaires d'un espace vectoriel V sur Ω de dimension finie. La restriction aux éléments de G définira une représentation irréductible X_i de G par des transformations linéaires de V. Naturellement, des représentations équivalentes seront considérées comme la même chose. (Ce sont des représentations telles que l'une peut être obtenue à partir de l'autre par un automorphisme de V).

Réciproquement, toute représentation irréductible est obtenue de cette manière. Par conséquent, le nombre r des termes dans (5) est le nombre n des classes K_j d'éléments conjugués et on peut prendre la valeur $\chi_i(\sigma)$ du caractère χ_i comme trace de $X_i(\sigma)$, $(\sigma \in G)$.

Dans ce qui précède on peut prendre pour Ω le corps des complexes. Mais il suffit de prendre un corps Ω algébrique assez étendu de degré fini sur le corps rationnel (par exemple, on peut prendre le corps des g-ièmes racines de l'unité, mais ce n'est pas d'importance pour nous). Si nous voulons passer au cas d'un corps de caractéristique p, nous pouvons achever cela de la manière suivante. Soit $\mathfrak{p}$ un idéal premier de Ω divisant p. Si $\mathfrak{o}$ est l'anneau des entiers locaux de Ω et si Ω^* est le corps des classes résiduelles

$$\Omega^* = \mathfrak{o} / \mathfrak{p} \quad ,$$

il suffit de prendre Ω^* comme corps dans lequel nous prenons les représentations.

Je désignerai par Γ^* l'algèbre de groupe de G formée sur le corps Ω^*. Ce Γ^* n'est plus semi-simple et cela cause des complications. Pourtant, si M est un idéal maximal de Γ, l'algèbre Γ^*/M sera une algèbre complète de matrices avec des coefficients dans Ω^*. Comme on l'a vu dans le cas de la caractéristique 0, cela nous donne une représentation irréductible de G dans Ω^*. Réciproquement, toute représentation irréductible de G dans Ω^* (ou dans un surcorps de Ω^*) est obtenue de cette façon. C'est ce que nous appelons les représentations irréductibles "modulaires" de G. On peut montrer que le nombre ℓ de ces représentations $F_1, F_2, \cdots, F_\ell$ essentiellement différentes est le nombre ℓ des classes p-régulières de G. Ainsi, si p divise g, ℓ est inférieur au nombre total n des classes de G. Comme nous avons vu, les F_j sont en correspondance biunivoque avec les idéaux maximaux de Γ. D'ailleurs, les idéaux maximaux de Γ sont les idéaux premiers de Γ.

Si X_i est une représentation de G dans Ω on peut voir facilement qu'on peut choisir la base de l'espace vectoriel V_i correspondant telle que chaque $X_i(\sigma)$ a des coefficients dans l'anneau local $\mathfrak{o}$ pour $\mathfrak{p}$. Or, l'application canonique de $\mathfrak{o}$ sur $\Omega^* = \mathfrak{o}/\mathfrak{p}$ changera X_i dans une représentation X_i^* modulaire de G. Bien que X_i soit irréductible, en général, X_i^* est réductible. En décomposant X_i^* en composantes irréductibles, nous pouvons parler de la multiplicité d_{ij} d'une représentation irréductible F_j dans X_i^*. Il faut remarquer que la représentation X_i^* dépend de la base que nous avons choisie dans l'espace V_j. Heureusement, les entiers d_{ij} non-négatifs dépendent seulement de X_i, de F_j, et de l'idéal premier $\mathfrak{p}$. D'ailleurs, un autre choix de $\mathfrak{p}$ (gardant le nombre premier p) n'entraîne pas de changement essentiel. Nous appelons les d_{ij} les "nombres de décomposition" de G pour p.

Définissons les caractères irréductibles modulaires. Ce sont des fonctions à valeurs complexes (pas dans Ω^* !) définies sur l'ensemble G_0 des éléments p-réguliers de G. On peut démontrer qu'il y a des fonctions de cette espèce telles que l'on ait

$$\chi_i(\sigma) = \sum_j d_{ij} \varphi_j(\sigma), \qquad (\sigma \in G_0). \tag{6}$$

Ici, φ_j est le caractère de la représentation F_j. Les fonctions $\varphi_1, \varphi_2, \cdots, \varphi_\ell$ sont linéairement indépendantes.

Les sommes suivantes sont importantes :

$$\sum_{\alpha=1}^{n} d_{\alpha i} d_{\alpha j} = c_{ij} \tag{7}$$

On peut montrer que les c_{ij} sont égaux à des quantités introduites essentiellement par Elie CARTAN dans la théorie des algèbres, que nous appelons les invariants de Cartan de Γ^* (ou de G, pour p). Ici, c_{ij} dépend de deux idéaux maximaux M_i et M_j de Γ^* ou, ce qui est la même chose, de deux caractères irréductibles modulaires φ_i et φ_j de G. D'ailleurs, on peut calculer les c_{ij} si on connaît les caractères irréductibles modulaires de G.

Dans (6), l'élément σ est p-régulier. Nous avons besoin d'une formule semblable pour les autres éléments. Tout $\sigma \in G$ peut s'écrire sous la forme

$$\sigma = \pi \sigma_0$$

où π et σ_0 sont des puissances de σ et où l'ordre de π est une puissance $p^\alpha \geq 1$ de p et celui de σ_0 est premier à p. Appelons "p-élément" un élément π dont l'ordre est une puissance $p^\alpha \geq 1$ de p. Alors, σ_0 est un élément p-régulier du centralisateur $C(\pi)$ du p-élément $\pi \in G$. En appliquant (6) au groupe $C(\pi)$, on obtient sans peine la généralisation suivante de (6) :

$$(8) \qquad \chi_i(\sigma) = \sum_j d_{ij}^{\pi} \varphi_j^{\pi}(\sigma_0) \qquad \begin{cases} \sigma = \pi\sigma_0 ; \ \pi_0 \text{ d'un ordre } p^\alpha ; \\ \sigma_0 \in C(\pi), \ \text{p-régulier.} \end{cases}$$

Ici, les d_{ij}^{π} sont des entiers algébriques, qui dépendent de π, i et j, et $\varphi_1^{\pi}, \varphi_2^{\pi}, \ldots$ sont les caractères irréductibles modulaires du groupe $C(\pi)$. D'ailleurs, les d_{ij}^{π} sont contenus dans le corps des p^α-ièmes racines de l'unité. A la place de (7), nous avons les équations

$$(9) \qquad \sum_{i=1}^{n} d_{i\alpha}^{\pi} \bar{d}_{i\beta}^{\pi} = c_{\alpha\beta}^{\pi} .$$

Ici, $c_{\alpha\beta}^{\pi}$ est l'invariant de Cartan du groupe $C(\pi)$ appartenant aux caractères φ_α^{π}, φ_β^{π} de ce groupe.

Supposons que π soit un p-élément fixe de G et que nous connaissions le groupe $C(\pi)$ comme groupe abstrait. En conséquence, nous connaissons les nombres c_{ij}^{π}. Il s'ensuit que nous avons un nombre fini de cas pour les $d_{\alpha j}^{\pi}$. Dans chaque cas, nous pouvons donner les valeurs des $d_{i\alpha}^{\pi}$ si les χ_i sont pris dans un ordre convenable, avec l'exception suivante : nous ne savons pas pour combien de χ_i tous les $d_{ij}^{\pi} = 0$. Ce sont les χ_i qui s'annulent pour tous les σ dans (8). Pour chaque cas, nous pouvons trouver toutes les valeurs $\chi_i(\sigma)$ pour les σ dans (8).

Si π appartient au centre de G, $G = C(\pi)$, et nous n'avons pas de réduction. Pourtant, il est facile de montrer qu'il suffit de connaître le groupe $C(\pi)/\{\pi\}$ (ou seulement les caractères irréductibles modulaires de ce groupe) et aussi l'ordre p^α du p-élément π. Naturellement, l'ordre de $C(\pi)/\{\pi\}$ est inférieur à g, sauf pour $\pi = 1$.

Si nous faisons varier π, il est clair qu'il suffit de prendre pour π les éléments

$$\pi_0 = 1, \quad \pi_1, \pi_2, \cdots, \pi_h \tag{10}$$

d'un système des représentants pour les p-classes de G (ce sont les classes d'éléments conjugués dont l'ordre est une puissance de p). Si nous connaissons tous les groupes $C(\pi_j)/\{\pi_j\}$ avec $j > 0$, nous aurons un nombre fini de possibilités. Pour chacun de ces cas, nous pouvons donner explicitement les valeurs des caractères irréductibles χ_i de G pour tous les éléments p-singuliers σ de G, excepté que nous ne savons pas combien de caractères χ_i s'annulent pour tous ces σ.

Pour le cas $n = 1$, j'ai indiqué plus haut un résultat plus précis. Ici, seulement quelque signes $\delta_i = \pm 1$ restent indéterminés. Dans le cas général, la discussion des équations (9) sera très compliquée parce que le nombre n des termes à droite peut être grand. Je vais montrer que l'on peut grouper tous les caractères χ_i et φ_j^π dans des systèmes tels qu'il suffit de se borner aux caractères d'un système dans les formules (8) et (9). Ces systèmes sont les "blocs" de caractères. Dans chaque bloc, nous aurons au plus p^{2n} caractères χ_i. Ainsi, le nombre des termes que nous aurons à considérer est borné, si p^n est donné. Cela est important pour les applications que je donnerai plus tard.

L'origine des blocs se trouve dans l'arithmétique de l'algèbre Γ. D'abord, je veux donner une définition directe. On sait que, pour étudier la structure d'une algèbre, il est important de connaître le centre. Soit Z le centre de T. Nous appelons Z "l'algèbre de classes" de G pour le raison suivante. Soit ξ_α la somme des éléments de G qui appartiennent à la classe K des éléments conjugués de G ;

$$\xi_\alpha = \sum_{\sigma \in K_\alpha} \sigma \ . \tag{11}$$

On voit immédiatement que si K_1 , K_2 , ... , K_m sont toutes les classes des éléments conjugués de G , les éléments ζ_1 , ζ_2 , ... , ζ_m forment une base de Z .

Une représentation irréductible X_i de Γ représente un élément $\zeta \in Z$ par un multiple scalaire $\omega_i(\zeta)I$ de l'unité I ; $\omega_i(\zeta) \in \Omega$. Il est évident que l'application $\zeta \longrightarrow \omega_i(\zeta)$ est un homomorphisme ω_i de l'algèbre Z sur Ω . Il suffit de connaître les valeurs $\omega_i(\zeta_\alpha)$. On déduit de (11) que

$$\sum_{\sigma \in K_\alpha} X_i(\sigma) = \omega_i(\zeta_\alpha)I \quad . \tag{12}$$

Soit $c(\sigma)$ l'ordre du centralisateur $C(\sigma)$ de σ . Soit σ_α un élément de K_α . En formant la trace dans (12), nous trouvons l'équation de Frobenius

$$\omega_i(\zeta_\alpha) = \frac{g}{c(\sigma_\alpha)} \frac{\chi_i(\sigma_\alpha)}{x_i} \tag{13}$$

où $\frac{g}{c(\sigma_\alpha)}$ est le nombre des éléments dans K_α . Il est clair que ce nombre $\omega_i(\zeta_\alpha)$ est un entier algébrique.

Réciproquement, tout homomorphisme de Z sur Ω est obtenu sous la forme ω_i avec $1 \leq i \leq m$.

Soit Z^* le centre de l'algèbre Γ^* de G sur le corps Ω^* . Les éléments (11), pris comme éléments de Γ^* , forment une base de Z^* . L'application canonique de o sur $o/\mathfrak{p} = \Omega^*$ change l'homomorphisme ω_i de Z sur Ω en un homomorphisme ω_i^* de Z^* sur Ω^* . Formulé plus précisément, ω_i^* est défini par la condition que $\omega_i^*(\zeta_j)$ soit l'image de $\omega_i(\zeta_j)$ pour l'application canonique. Chaque homomorphisme de Z^* sur Ω^* apparaît sous la forme ω_i^* , $1 \leq i \leq m$. Pourtant, ω_1^* , ω_2^* , ... , ω_m^* ne sont plus distincts. Nous disons que deux caractères irréductibles de G_0 , χ_i et χ_j , appartiennent au même "bloc", si $\omega_i^* = \omega_j^*$, cela veut dire, que

$$\frac{g}{c(\sigma)} \frac{\chi_i(\sigma)}{x_i} \equiv \frac{g}{c(\sigma)} \frac{\chi_j(\sigma)}{x_j} \pmod{\mathfrak{p}} \tag{14}$$

pour tous les $\sigma \in G$. De cette façon, les caractères χ_1 , χ_2 , ... , χ_m de G sont distribués en blocs, et chaque caractère irréductible χ_i appartient à un bloc et à un seul.

Soient B_1 , B_2 , ... , B_n la totalité des blocs de G . Choisissons des notations telles que $\chi_i \in B_i$ pour $i = 1$, 2 , ... , n . Alors,

$$\omega_1^*, \omega_2^*, \ldots, \omega_n^*$$

sont tous les homomorphismes de Z^* sur Ω^*. Par dualité, chaque ω_i^* correspond à un idéal primaire T_i de Z^* et Z^* est la somme directe de ces algèbres T_i,

$$Z^* = T_1 \oplus T_2 \oplus \dots \oplus T_n \quad . \tag{15}$$

La décomposition du centre Z^* de Γ^* correspond à une décomposition de Γ^* en une somme directe d'algèbres primaires U_i,

$$\Gamma^* = U_1 \oplus U_2 \oplus \dots \oplus U_n \quad . \tag{16}$$

(Ce fait est immédiat, si nous utilisons la décomposition de l'unité en une somme d'idempotents orthogonaux, qui correspond à la décomposition (15)).

Soit F_j une représentation irréductible modulaire de G. Comme on l'a vu, F_j correspond à un idéal maximal M_j de Γ^*. Or, M_j contient un et un seul des idéaux U_ν dans (16). Si $M_j \supseteq U_\nu$, on dit que le caractère φ_j de F_j appartient au bloc B_ν.

Alors, les caractères irréductibles modulaires $\varphi_1, \varphi_2, \dots, \varphi_\ell$ de G sont aussi distribués dans les blocs $B_1, B_2, \dots, B_n$. On peut démontrer sans difficulté que, dans (6), $d_{ij} = 0$, si χ_i et φ_j appartiennent à différents blocs. Autrement dit, si χ_i appartient au bloc B_ν, seulement les φ_j de B_ν peuvent avoir des coefficients $d_{ij} \neq 0$ dans (6). Cela peut être utilisé pour une autre définition des blocs.

Il est plus difficile de montrer que nous avons une situation semblable pour les formules (8). Soit π un p-élément fixe. D'abord, il est nécessaire d'exposer une connexion entre les blocs de $C(\pi)$ et ceux de G. Soit B^π un bloc de $C(\pi)$. Nous désignons par $(Z^\pi)^*$ le centre de l'algèbre $(\Gamma^\pi)^*$ de groupe de $C(\pi)$ sur le corps Ω^*. Si $K_1^\pi, K_2^\pi, \dots$ sont les classes d'éléments conjugués de $C(\pi)$ et si $\mathfrak{k}_\alpha^\pi$ est la somme des éléments de K_α^π, les éléments $\mathfrak{k}_1^\pi, \mathfrak{k}_2^\pi, \dots$ forment une base de $(Z^\pi)^*$.

Or, B^π correspond à un homomorphisme $(\omega^\pi)^*$ de $(Z^\pi)^*$ sur Ω^*. On peut montrer qu'il existe un homomorphisme ω^* de Z^* sur Ω^* tel que

$$\omega^*(\mathfrak{k}_\alpha) = \sum_{K_\beta^\pi \subseteq K_\alpha^\pi \cap C(\pi)} (\omega^\pi)^* (\mathfrak{k}_\beta^\pi) \tag{17}$$

où K_β^π parcourt toutes les classes de $C(\pi)$ contenues dans K_α. L'homomorphisme ω^* de Z^* détermine un bloc B de G. De cette façon, nous avons

associé un bloc B de G au bloc B^π de $C(\pi)$. On peut montrer que si φ_j^π dans (8) appartient au bloc B^π, le coefficient d_{ij}^π peut seulement être non-nul si χ_i appartient au bloc B associé à B^π.

Soit t le nombre des caractères χ_i irréductibles de G dans un bloc B de G. Laissons π parcourir le système (10) de représentants et, pour chaque π, déterminons tous les caractères modulaires φ_j^π de tous les blocs B^π de $C(\pi)$ qui sont associés au bloc B. On peut montrer que le nombre total de ces φ_j^π est exactement égal à t. Ainsi, si l'on se restreint aux caractères χ_i du bloc B, on peut écrire les équations (8) et (9) de telle façon que les sommes ont t termes. J'ai déjà remarqué que $t \leq p^{2n}$. Si nous ajoutons qu'il est possible d'obtenir des congruences modulo puissances de p entre les d_{ij}^π pour les divers π, on verra qu'on peut souvent trouver toutes les valeurs possibles pour les d_{ij}^π dans (9). (Par exemple, c'est possible si p^n est petit).

La formule (17) est d'un intérêt indépendant.

Si nous connaissons $C(\pi)$ et la "position" de $C(\pi)$ dans G, nous pouvons trouver tous les $(\omega^\pi)^*$ et les ω^* associés avec eux. Si nous rappelons la relation (13), nous voyons que cela nous donne quelque information sur les valeurs des caractères χ_i.

De plus, si nous faisons varier le p-élément π, excluant $\pi = 1$, et prenons tous les $(\omega^\pi)^*$, tous les homomorphismes ω^* de Z^* sont obtenues sauf ceux qui correspondent à des blocs B de G de "défaut" 0. Ici, les blocs B de défaut 0 sont les blocs que l'on peut caractériser par chacune des propriétés suivantes :

1° Il y a un seul caractère irréductible χ_i dans B.

2° Le degré d'un caractère de B est divisible par la puissance p^n la plus haute de p qui divise l'ordre g de G.

3° Un caractère de B s'annule pour tous les éléments p-singuliers de G.

Au lieu de poursuivre la théorie des blocs, je préfère donner quelques applications à la théorie des groupes abstraits. Pour les applications que je veux discuter, il faut supposer que l'ordre g du groupe G soit un nombre pair. Bien sûr, on peut douter que cela soit une hypothèse naturelle. Mais on ne sait pas si les résultats que l'on va donner ont des analogues quand l'ordre du groupe est impair. Peut-être, peut-on se consoler avec le fait qu'il est probable que tous les groupes d'ordre impair soient résolubles. Tout au moins, on ne connaît pas de groupe non-résoluble d'ordre impair.

Si l'ordre g de G est pair, il y a des éléments d'ordre 2 dans G. Nous appelons ces éléments les "involutions" de G. Certaines des classes $K_1, K_2, \dots, K_m$ se composent d'involutions. Supposons que ce soient les classes $K_1, K_2, \dots, K_s$. Posons

$$q = \xi_1 + \xi_2 + \dots + \xi_s = \sum_{\sigma^2 = 1} \sigma \quad . \tag{18}$$

Or, $\{\xi_1, \xi_2, \dots, \xi_m\}$ est une base de Z et nous avons des formules

$$\xi_\alpha \xi_\beta = \sum_{\gamma=1}^{m} a_{\alpha\beta\gamma} \xi_\gamma \qquad (\alpha, \beta = 1, 2, \dots, m) \tag{19}$$

avec des coefficients rationnels (En effet, les $a_{\alpha\beta\gamma}$ sont des entiers non-négatifs). En appliquant l'homomorphisme ω_i, il s'ensuit que

$$\omega_i(\xi_\alpha)\ \omega_i(\xi_\beta) = \sum_{\gamma=1}^{m} a_{\alpha\beta\gamma}\ \omega_i(\xi_\gamma) \quad .$$

Soit σ_λ un élément de K_λ, $1 \leq \lambda \leq m$. En utilisant (13) et les relations d'orthogonalité des caractères, on obtient, après un calcul facile,

$$a_{\alpha\beta\gamma} = \frac{g}{c(\sigma_\alpha)\, c(\sigma_\beta)} \sum_{i=1}^{m} \frac{\chi_i(\sigma_\alpha)\ \chi_i(\sigma_\beta)\ \overline{\chi}_i(\sigma_\gamma)}{x_i} \quad . \tag{20}$$

En combinant (18), (19) et (20), on voit que l'on peut poser

$$q^2 = \sum_{\gamma=1}^{m} b_\gamma \xi_\gamma \tag{21}$$

où

$$b_\gamma = g \sum_{i=1}^{m} \frac{h_i^2}{x_i}\, \chi_i(\sigma_\gamma) \tag{22}$$

avec

$$h_i = \sum_{\alpha=1}^{s} \frac{\chi_i(\sigma_\alpha)}{c(\sigma_\alpha)} \quad . \tag{23}$$

Les h_i sont des nombres rationnels, parce que σ_α est une involution pour $\alpha = 1, 2, \dots, S$.

D'autre part, en comparant le coefficient de σ_γ à droite et à gauche dans (21) on déduit que b_γ est le nombre des couples ordonnés $\langle \rho, \tau \rangle$ d'involutions de G tels que

$$\rho^{\tau} = \sigma_\gamma \quad ,$$

ce qui implique $\rho^{-1} \sigma_\gamma \rho = \sigma_\gamma^{-1}$.

Soit $\sigma \in G$. Les éléments $\xi \in G$ pour lesquels $\xi^{-1} \sigma \xi = \sigma^{\pm 1}$ forment un sous-groupe $C^*(\sigma)$ de G . Evidemment, ou bien $C^*(\sigma) = C(\sigma)$ ou bien $C(\sigma)$ est un sous-groupe normal d'indice 2 de $C^*(\sigma)$. L'observation précédente montre que, si σ_γ n'est pas une involution, b_γ est le nombre des involutions ρ de G qui appartiennent à $C^*(\sigma_\gamma)$, mais pas à $C(\sigma_\gamma)$. Si σ_γ est une involution, b_γ est le nombre des involutions $\rho \neq \sigma_\gamma$ dans $C(\sigma_\gamma)$.

Soit $\tilde{G}$ un sous-groupe quelconque de G . Si nous avons introduit un concept pour G et utilisé une lettre pour le dénoter, nous emploierons la même lettre avec un tilda pour le concept correspondant de $\tilde{G}$. Ainsi, $\tilde{g}$ est l'ordre de $\tilde{G}$, $\{\tilde{\chi}_1 , \tilde{\chi}_2 , \dots\}$ est l'ensemble des caractères irréductibles de $\tilde{G}$, etc.

Soit $\sigma = \sigma_\chi$ un élément de G et supposons que

$$\tilde{G} \supseteq C^*(\sigma) \quad . \tag{24}$$

Il est immédiat, d'après l'interprétation de b_γ comme nombre de certaines involutions, que $b_\chi = \tilde{b}_\chi$. En substituant l'expression (22), on trouve

$$g \sum_i \frac{h_i^2}{x_i} \chi_i(\sigma) = \tilde{g} \sum_i \frac{\tilde{h}_i^2}{\tilde{x}_i} \tilde{\chi}_i(\sigma) \quad .$$

Soit π un p-élément fixe de G et supposons que

$$\tilde{G} \supseteq C^*(\pi) \quad . \tag{25}$$

Il est immédiat que l'hypothèse (24) est satisfaite pour tous les éléments $\sigma = \pi \sigma_0$ avec σ_0 p-régulier dans $C(\pi)$. Pour ces σ , on peut appliquer (8) et, en utilisant l'indépendance linéaire des φ_j^{π} on obtient

$$g \sum_i \frac{h_i^2}{x_i} d_{i\rho}^{\pi} = \tilde{g} \sum_i \frac{\tilde{h}_i^2}{\tilde{x}_i} \tilde{d}_{i\rho}^{\pi} \tag{26}$$

Si le groupe $\tilde{G}$ est connu, on peut calculer le second membre. Notre formule donnera un renseignement sur l'ordre g de G pourvu que l'on puisse dire quelque chose sur la valeur de la somme

$$\sum_i \frac{h_i^2}{x_i} d_{i\rho}^{\pi} \tag{27}$$

Nous avons observé que, $\tilde{G} \geq C^*(\pi) \geq C(\pi)$ étant donné, nous avons un nombre fini de cas tels que, dans chaque cas, les $d_{i\rho}^{\pi}$ sont connus. En outre, le nombre des termes dans la somme (27) est au plus p^{2n}.

En particulier, nous nous intéressons au cas $p = 2$. Supposons, pour plus de simplicité, que G contienne seulement une classe K_i dont les éléments sont des involutions. Ici, (23) devient

$$h_i = \frac{\chi_i(\tau)}{c(\tau)}$$

où τ est une involution arbitraire de G. Prenons $\tilde{G} = C(\tau)$, $\tilde{g} = c(\tau)$. Chaque classe K_j de 2 éléments contient un élément π dont une puissance est τ. Cela implique que l'hypothèse (25) est satisfaite pour π. En prenant $\pi = \tau$, on peut obtenir $\chi_i(\tau)$ de (8), (si les $d_{i\rho}^{\tau}$ sont connus). L'équation (26) devient :

$$g \sum_i \frac{\chi_i(\tau)}{x_i} d_{i\rho}^{\pi} = c(\tau)^3 \sum_i \frac{\tilde{h}_i^2}{\tilde{x}_i} \tilde{d}_{i\rho}^{\pi} \tag{28}$$

Ici, tout est connu, sauf g et les x_i. On connaît la puissance 2^n la plus haute de 2 qui divise g parce que $C(\tau)$ contient un 2-sous-groupe de Sylow P de G. Par conséquent, le nombre des termes de la somme figurant à gauche dans (28) est borné.

Prenons, par exemple, pour φ_ρ^π le caractère principal modulaire de $C(\pi)$; $\varphi_\rho^\pi(\sigma_0) = 1$ pour tous les p-réguliers de $C(\pi)$. Si nous disons que χ_1 est le caractère principal ordinaire de G ($\chi_1(\sigma) = 1$ pour tous les $\sigma \in G$), le terme correspondant à la valeur 1 de l'indice i à gauche dans (28) est égal à 1 et la somme a la forme

$$1 + \frac{\chi_2(\tau)}{x_2} d_{2\rho}^{\pi} + \frac{\chi_3(\tau)}{x_3} d_{3\rho}^{\pi} + \cdots$$

Si nous supposons que les degrés x_2, x_3, ... sont grands, la valeur de la somme est voisine de 1, et (28) donne une valeur approximative pour l'ordre g du groupe G, pourvu que nous connaissions le sous-groupe $C(\tau)$. Pour rendre notre argument rigoureux, il faut examiner, dans chaque cas concret, si l'hypothèse relative aux degrés x_2, x_3, ... est satisfaite. Nous avons des congruences mod 2^n pour ces degrés inconnus.

Nous avons aussi supposé que G contient seulement une classe d'involutions. Il est intéressant de noter, à ce sujet, que, si G possède plus qu'une classe d'involutions, on peut démontrer que

$$g \leqslant c(\tau)^3$$

où τ est une involution convenable.

Si nous voulons arriver à des résultats plus définitifs, il est nécessaire de pouvoir trouver toutes les possibilités pour les $d_{i\rho}^{\pi}$. Je vais discuter quelques cas où c'est possible. Si l'on a beaucoup de patience et si l'on vit longtemps, on peut augmenter la liste !

<u>Désormais, nous ferons l'hypothèse que G ne possède pas un sous-groupe normal d'ordre $\frac{1}{2} g$.</u>

I. Supposons que le 2-Sylow groupe P de G est un groupe de quaternions (ordinaire ou généralisé) d'ordre 2^n , $n \geqslant 3$,

$$P = \{\rho, \sigma\} \text{ avec } \rho^{2^{n-1}} = 1 , \quad \sigma^2 = \rho^{2^{n-2}} , \quad \sigma^{-1} \rho \sigma = \rho^{-1} .$$

Dans ce cas, la méthode montre que G n'est pas simple. Plus précisément, si G_0 est l'unique sous-groupe normal maximal d'ordre impair $\geqslant 1$, on peut prouver que G/G_0 a un centre d'ordre pair. Le point essentiel de la méthode est que l'on peut utiliser les équations obtenues pour trouver un caractère non-principal χ_i tel que $\chi_i(\tau) = \chi_i(1)$ pour une involution τ , ce qui est impossible dans un groupe simple.

II. Le 2-sous-groupe P de Sylow de G est un groupe de dièdre :

$$P = \{\rho, \sigma\} \text{ avec } \rho^{2^{n-1}} = 1 , \quad \sigma^2 = 1 , \quad \sigma^{-1} \rho \sigma = \rho^{-1}$$

d'ordre 2^n .

Ici, $\tau = \rho^{2^{n-2}}$ est une involution, et G a seulement une classe d'involutions

a. Soit d'abord $n \geqslant 3$. On peut montrer que l'ordre g de G a la forme

$$g = 2 \alpha \, c(\tau)^3 \left(\frac{1}{c(\tau, \sigma)} + \frac{1}{c(\tau, \rho\sigma)}\right)^2$$

où α est un nombre rationnel qui satisfait les inégalités

$$\left(1 - \frac{1}{2^{n-1}}\right)\left(1 - \frac{1}{2^n}\right) \leqslant \alpha \leqslant \left(1 + \frac{1}{2^{n-1}}\right)\left(1 + \frac{1}{2^n}\right)$$

et où $c(\xi , \eta)$ désigne l'ordre de l'intersection $C(\xi) \cap C(\eta)$ (pour $\xi , \eta \in G$).

De plus, α a la forme

$$\alpha = \frac{x(x+\delta)}{(x-\delta)^2}$$

où $\delta = \pm 1$ et où x est le degré d'un caractère irréductible de G ; $x \equiv \delta \mod 2^n$, $x > 1$.

Si $c(\tau , \sigma) = c(\tau , \rho\sigma)$, nous parlerons du "cas régulier". Ici, g a la forme

$$g = \beta \frac{x(x+1)(x-1)}{2} \quad , \quad \beta \text{ entier}$$

Nous ne savons pas s'il y a des groupes G pour lesquels x n'est pas une puissance d'un nombre premier.

Les groupes simples $L_2(x)$, (x puissance d'un nombre premier avec $x \equiv \pm 1 + 2^n \pmod{2^{n+1}}$) forment des exemples. Il n'est pas connu si ce sont les seuls groupes simples qui vérifient nos conditions. On a besoin d'hypothèses supplémentaires, si on veut caractériser ces groupes.

Considérons le cas irrégulier, $c(\tau , \sigma) \neq c(\tau , \rho\sigma)$. On peut montrer que le quotient $c(\tau , \sigma)/c(\tau , \rho\sigma)$ ne diffère pas beaucoup de 1. D'ailleurs, on peut remplacer les inégalités pour α par des conditions de divisibilité, ce qui précise le résultat. Le seul exemple connu d'un groupe simple de cette espèce est donné par le groupe alterné A_7 d'ordre $g = 2\,520$.

b. Dans le cas $n = 2$, P a l'ordre 4. Ici, le caractère principal de G appartient à un bloc B qui contient quatre caractères χ_i. On peut prendre les degrés x_1 , x_2 , x_3 , x_4 de ces caractères tels que l'on ait

$$x_1 = 1 \; , \; x_2 \equiv 1 \pmod 4 \; , \; x_3 \equiv \delta = \pm 1 \pmod 4 \; , \; x_4 \equiv -1 \pmod 4 \; ;$$

$$1 + x_2 + \delta x_3 = x_4 \qquad (x_2 \neq 1 \; , \; x_3 \neq 1) \; .$$

L'ordre g de G est

$$g = 8\alpha \frac{c(\rho\sigma)^3}{c(\rho,\sigma)^2} \qquad \text{avec} \qquad \alpha = \frac{x_2 x_3 x_4}{(x_2+1)(x_3+\delta)(x_4-1)}$$

Ici,

$$\frac{25}{36} \leq \alpha \leq \frac{15}{8} \; .$$

Si $\varepsilon = 1$, on peut montrer que $x_2 = x_3$ et que $g = \beta \frac{(x_4-1)x_4(x_4+1)}{2}$ avec β entier. Si $\varepsilon = -1$ et si $x_3 = x_4$, on a $g = \frac{(x_2-1)x_2(x_2+1)}{2}$ avec β entier. Ici, les groupes $L_2(q)$ avec $q \equiv \pm 5 \pmod 8$, q puissance d'un nombre premier, forment des exemples.

Je ne sais pas s'il y a des groupes G avec $\varepsilon = -1$ et $x_3 \neq x_4$, ni s'il y a des groupes simples qui satisfont nos conditions et n'ont pas la forme $L_2(q)$.

III. Le groupe P de Sylow de G est défini par les relations

$$P = \{\rho , \sigma\} , \quad \rho^{2^{n-1}} = 1 , \quad \sigma^2 = 1 , \quad \sigma^{-1} \rho \sigma = \rho^{2^{n-1}-1} .$$

Soit τ l'involution $\rho^{2^{n-2}}$. Ici, g est voisin de $\frac{c(\tau)^3}{c(\tau,\sigma)^2}$

Plus précisément, nous avons

$$g = \frac{c(\tau)^3}{c(\tau,\sigma)^2} \; \frac{x(x+\varepsilon)}{(x-\varepsilon f)^2} \frac{f+1}{f}$$

où $\varepsilon = \pm 1$, $x \neq 1$ est le degré d'un caractère irréductible de G , et f est le degré d'un caractère irréductible de $C(\tau)$. D'ailleurs on peut exprimer f avec l'aide des ordres de certains sous-groupes de $C(\tau)$.

Les groupes $L_3(q)$ pour $q \equiv -1 \pmod 4$ et les groupes unitaires $HO(3 , q)$ avec $q \equiv 1 \pmod 4$ forment des exemples pour notre type. Si on fait des hypothèses supplémentaires, on peut caractériser les groupes $L_3(q)$.

IV. Les groupes $L_3(q)$ pour $q \equiv -1 \pmod 4$ et les groupes $HO(3 , q)$ pour $q \equiv 1 \pmod 4$ ont le groupe de Sylow défini par

$$P = \{\rho_1 , \rho_2 , \sigma\} \text{ avec } \rho_1^{2^h} = 1 , \quad \rho_2^{2^h} = 1 , \quad \sigma^2 = 1 , \quad \sigma^{-1} \rho_1 \sigma = \rho_2 .$$

L'ordre 2^n est 2^{2h+1} . Je peux traiter ces groupes seulement dans le premier cas $n = 5$. Ici, l'ordre g de G est déterminé uniquement par $C(\sigma)$. Il est possible qu'un résultat semblable soit vrai pour $n > 5$.

Ces résultats indiquent qu'on peut espérer qu'il sera possible d'obtenir quelque information sur les groupes simples en utilisant la méthode générale. Bien sûr, les cas traités sont les cas les plus simples et on est loin de la solution du problème de trouver tous les groupes simples d'ordre fini.