Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 20 (1947)

Artikel: Les groupes linéaires finis sans points fixes.
Autor: Vincent, Georges
DOI: https://doi.org/10.5169/seals-18054

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 03.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Les groupes linéaires finis sans points fixes

Par Georges Vincent, Lausanne

Introduction

Depuis les travaux de Killing, complétés et précisés par M. H. Hopf[1]), on sait que la totalité des formes de Clifford-Klein (espaces complets à courbure riemannienne constante positive, nulle ou négative) peut s'obtenir en déterminant les groupes discontinus de déplacements sans points fixes de l'espace sphérique, euclidien ou hyperbolique.

En particulier, les *formes spatiales sphériques*[1]) s'obtiennent par la détermination de tous les groupes *finis* de rotations sans points fixes de la sphère à n dimensions S^n. Au point de vue analytique, cela revient à étudier les groupes finis de substitutions linéaires homogènes, orthogonales, n'admettant pas la valeur propre $+1$.

Le problème qui fait l'objet de ce travail, soit la recherche des *formes spatiales sphériques*, se ramène par suite à la détermination des *groupes linéaires finis sans points fixes*.

On sait que toute représentation linéaire d'un groupe abstrait fini peut se déduire, par un procédé d'addition connu, des représentations irréductibles non équivalentes. Le nombre de ces dernières est fini, égal au nombre des classes des éléments du groupe. En particulier, les représentations sans points fixes sont les sommes de représentations irréductibles sans points fixes. Le problème peut par suite se ramener aux suivants:

1° Déterminer les groupes abstraits finis susceptibles d'admettre des représentations sans points fixes.

2° Déterminer les représentations irréductibles sans points fixes de chacun de ces groupes. Pour les applications géométriques, il convient de déterminer le degré de ces représentations, de reconnaître si elles sont équivalentes à une représentation réelle et, dans le cas contraire, si elles sont ou non équivalentes à l'imaginaire conjuguée.

---

[1]) Ces espaces ont été déterminés complètement, pour la dimension 3, par M.H. Hopf [1] puis par W. Threlfall et H. Seifert [2], par des méthodes particulières à cette dimension. — Les numéros entre crochets renvoient à l'index bibliographique placé à la fin du présent travail.

Le premier problème*) fait l'objet des chapitres I et II. Les groupes qui admettent des représentations sans points fixes sont relativement peu nombreux (par exemple, il s'en trouve cinq seulement parmi les quinze structures non isomorphes d'un groupe d'ordre 24). Leurs sous-groupes abéliens sont tous cycliques. Cette remarque et le fait qu'un p-groupe à sous-groupes abéliens cycliques est cyclique si $p \neq 2$, cyclique ou quaternionique (voir 1.2) si $p = 2$, permet d'établir par une nouvelle voie un théorème de Burnside (voir 2.5), base de ce travail. D'après ce théorème, les groupes cherchés appartiennent nécessairement à l'un ou l'autre des deux types suivants :

Le *premier type* est celui des groupes dont tous les sous-groupes de Sylow sont cycliques.

Le *deuxième type*, celui des groupes dont les p-sous-groupes de Sylow sont cycliques pour $p \neq 2$, quaternioniques pour $p = 2$.

Le chapitre II est consacré à l'étude de la structure des groupes abstraits finis des deux types. Les groupes du premier type sont connus (voir § 4) ; ils sont résolubles et ceux qui ne sont pas cycliques peuvent être engendrés par deux éléments générateurs liés par quelques relations simples. Les groupes du deuxième type se subdivisent en groupes résolubles et groupes non résolubles. Je montre que les premiers sont métabéliens de rang 2, 3 ou 4 et que les groupes non résolubles sont parfaits (identiques à leur dérivé) ou admettent un premier ou un deuxième dérivé parfait. En utilisant la théorie de l'extension de Schreier (voir 4.4), je construis tous les groupes du deuxième type métabéliens de rang 2.

Le second problème est abordé au chapitre III, où se trouve une étude complète des représentations irréductibles des groupes du premier type et d'une large classe de groupes du deuxième type, métabéliens de rang 2. Un critère simple, de nature arithmétique, permet de décider lesquels de ces groupes admettent des représentations sans points fixes (th. III 8.4 et IV 9.1).

Si un groupe fini du type considéré admet une représentation sans points fixes, toutes ses représentations irréductibles fidèles sont sans points fixes, elles sont toutes de même degré et non équivalentes à des représentations réelles (énoncés précis : th. III* 8.4 et IV* 9.1).

On peut déduire de là quelques conséquences très générales relatives aux groupes de rotations sans points fixes. Excluons d'emblée les dimensions paires pour lesquelles, c'est un fait bien connu, les seules formes spatiales sphériques sont la sphère elle-même et l'espace elliptique.

*) Outre les références indiquées dans le texte, il convient de citer ici *H. Zassenhaus*, Über endliche Fastkörper, Hamb. Abh. 11 (1936), 187—220, venu à ma connaissance après la rédaction de ce mémoire.

Toute sphère de dimension impaire (supérieure à 1) admet une infinité de groupes finis de rotations sans points fixes, non abéliens, ne se présentant pas pour des dimensions inférieures (th. II 8.3).

Bien que l'étude des groupes du deuxième type ne soit pas achevée, le fait que les représentations irréductibles sans points fixes d'un groupe quaternionique sont de degré 2 et non équivalentes à une représentation réelle entraîne que seules les sphères S^{4k+3}, dont le nombre de dimensions est congru à 3 (mod. 4), peuvent admettre des groupes de rotations sans points fixes du deuxième type. Il en résulte le théorème suivant, qui achève en un certain sens la recherche des groupes de rotations sans points fixes des sphères de dimensions $4k+1$, et en même temps celle des formes spatiales sphériques de même dimension :

Les groupes finis de rotations sans points fixes d'une sphère S^{4k+1} sont tous du premier type. Il s'en présente de nouveaux, en nombre infini, pour toute dimension $4k+1$ et leur recherche se ramène à un problème purement arithmétique (th. VI 10.1).

L'étude des représentations des groupes du deuxième type, bien que très incomplète encore, permet cependant d'énoncer le théorème suivant :

Toute sphère S^{8k+3}, dont le nombre de dimensions est congru à 3 (mod. 8), admet une infinité de groupes finis de rotations sans points fixes du deuxième type, métabéliens de rang 2, ne se présentant pas pour des dimensions inférieures (th. V 9.2).

Au chapitre IV, je déduis quelques corollaires des théorèmes fondamentaux. Citons celui-ci :

Les groupes d'ordre impair de rotations sans points fixes d'une sphère de dimension $2^n - 1$ sont tous cycliques. Par contre, toute sphère dont la dimension est un nombre impair qui n'est pas de la forme $2^n - 1$ admet une infinité de groupes d'ordre impair, non abéliens, de rotations sans points fixes (th. VIII 10.3).

Je retrouve par voie algébrique un théorème démontré par M. H. Hopf (voir 10.4) comme conséquence d'un théorème topologique et j'établis une proposition relative aux „translations de Clifford" (voir 10.5) qui peut être déduite d'un théorème topologique de M. Stiefel.

Je détermine enfin la structure des groupes finis, abéliens, de déplacements elliptiques sans points fixes de l'espace elliptique, ainsi que celle du premier groupe de Betti des formes spatiales sphériques.

Qu'il me soit permis d'exprimer ici à M. H. Hopf, qui m'a proposé le sujet de ce travail, ainsi qu'à M. G. de Rham ma profonde reconnaissance pour leurs conseils si bienveillants et l'intérêt qu'ils n'ont cessé de me témoigner au cours de mes recherches.

Chapitre I

Conditions nécessaires pour l'existence de représentations sans points fixes

§ 1. Groupes finis à sous-groupes abéliens cycliques

1.1. Désignons par $g = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la décomposition en facteurs premiers distincts de l'ordre g du groupe abstrait fini $\mathfrak{G}$. Il existe des sous-groupes de $\mathfrak{G}$ de tous les ordres $p_i^{\beta_i}$ $(i = 1, 2, \ldots, k)$ où $1 \leqslant \beta_i \leqslant \alpha_i$. Ceux d'ordre maximum $p_i^{\alpha_i}$ sont conjugés dans $\mathfrak{G}$ (transformés les uns dans les autres par les éléments de $\mathfrak{G}$), isomorphes par conséquent, et en nombre congru à 1 modulo p_i. Ce sont les sous-groupes de Sylow[2]) de $\mathfrak{G}$ relatifs au diviseur premier p_i.

Tout sous-groupe d'ordre $p_i^{\beta_i}$ de $\mathfrak{G}$ est entièrement contenu dans au moins un p_i-sous-groupe de Sylow de $\mathfrak{G}$.

Un groupe abélien (multiplication commutative) est le produit direct de ses sous-groupes de Sylow.

1.2. Les p-groupes, groupes finis dont l'ordre est une puissance d'un entier premier p, jouissent de propriétés remarquables[2]). J'utilise ici deux de ces propriétés :

Lemme 1 : Un groupe d'ordre p premier est cyclique. Un groupe d'ordre p^2 est abélien, cyclique ou de type (p, p).

Lemme 2 : Un groupe d'ordre p^n, où pour un m fixé tel que $1 < m < n$, chaque sous-groupe d'ordre p^m est cyclique, est lui-même cyclique, excepté dans le cas $p = 2$, $m = 2$, où le groupe peut être aussi un groupe des quaternions généralisé[3]).

Le groupe des quaternions généralisé $\mathfrak{Q}2^\alpha$ est engendré par deux éléments A et B avec les relations :

$$A^{2^{\alpha-1}} = E \qquad B^2 = A^{2^{\alpha-2}} \qquad BAB^{-1} = A^{-1} \qquad (\alpha > 2) \ .$$

Son ordre est 2^α ; pour $\alpha = 3$, on retrouve le groupe des quaternions, d'ordre 8

$$A^4 = E \qquad B^2 = A^2 \qquad BAB^{-1} = A^{-1} \ .$$

Une étude plus approfondie de la structure du groupe des quaternions généralisé est donnée au chapitre II (3.2).

---

[2]) Pour tout ce qui a trait à la théorie des sous-groupes de Sylow et des p-groupes, voir [3] chap. IV ou [4] chap. 5.

[3]) [3] pp. 105 et 113.

1.3. Considérons un groupe abstrait fini $\mathfrak{G}$, dont tous les sous-groupes abéliens soient cycliques.

Soit $g = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ son ordre. Si les α_i sont tous égaux à l'unité, les sous-groupes de Sylow de $\mathfrak{G}$ étant d'ordre premier sont cycliques. Dans le cas contraire, désignons par $\mathfrak{P}_i$ l'un des sous-groupes de Sylow d'ordre $p_i^{\alpha_i}$ ($\alpha_i \geqslant 2$). Ses sous-groupes d'ordre p_i^2 sont abéliens en vertu du lemme 1 ; or, ce sont des sous-groupes de $\mathfrak{G}$, abéliens, donc cycliques par hypothèse. Le lemme 2 est applicable à $\mathfrak{P}_i$, qui est par conséquent cyclique ou quaternionique.

Réciproquement, soit $\mathfrak{G}$ un groupe fini dont les sous-groupes de Sylow sont cycliques ou quaternioniques, $\mathfrak{H}$ un sous-groupe abélien de $\mathfrak{G}$. L'ordre h de $\mathfrak{H}$ est un diviseur de l'ordre g de $\mathfrak{G}$. Un sous-groupe de Sylow de $\mathfrak{H}$ relatif au diviseur premier p_i est d'ordre $p_i^{\beta_i} \leqslant p_i^{\alpha_i}$. C'est un p_i-sous-groupe de $\mathfrak{G}$ contenu comme tel dans un $\mathfrak{P}_i$ (sous-groupe de Sylow de $\mathfrak{G}$). Les groupes de Sylow de $\mathfrak{H}$ sont des sous-groupes des groupes de Sylow de $\mathfrak{G}$. Or, ceux-ci étant cycliques ou quaternioniques, leurs sous-groupes sont cycliques ou quaternioniques (les sous-groupes d'un groupe quaternionique sont étudiés au chapitre II). Les groupes de Sylow de $\mathfrak{H}$ sont cycliques (quaternioniques exclus car $\mathfrak{H}$ est abélien) ; $\mathfrak{H}$ étant abélien est le produit direct de ses groupes de Sylow, il est cyclique. D'où le théorème :

La condition nécessaire et suffisante pour que les sous-groupes abéliens d'un groupe fini $\mathfrak{G}$ soient cycliques est que $\mathfrak{G}$ soit de l'un des deux types suivants :

Premier type : Les sous-groupes de Sylow de $\mathfrak{G}$ sont cycliques (y compris ceux relatifs au diviseur premier 2 si l'ordre de $\mathfrak{G}$ est pair).

Deuxième type : Les p-sous-groupes de Sylow de $\mathfrak{G}$ sont cycliques pour $p \neq 2$, quaternioniques pour $p = 2$.

Si $\mathfrak{G}$ est abélien, il est cyclique et se rattache au premier type. L'ordre d'un groupe du deuxième type est divisible par une puissance de 2 supérieure ou égale à la troisième.

§ 2. Représentations sans points fixes

2.1. Les substitutions linéaires, homogènes, définies par $x_i' = \sum_{k=1}^{n} a_{ik} x_k$, à coefficients a_{ik} dans un corps K et à déterminant différent de 0, forment le groupe linéaire $\mathfrak{L}^K(n)$ de degré n (nombre des variables). Chaque substitution est caractérisée par la matrice des coefficients $A = (a_{ik})$.

On nomme *représentation linéaire*[4]) d'un groupe abstrait $\mathfrak{G}$ tout *homomorphisme* de $\mathfrak{G}$ dans $\mathfrak{L}^K(n)$. Une telle représentation Γ fait correspondre à tout élément $x \in \mathfrak{G}$ une matrice bien déterminée $X = \Gamma(x)$ et au produit ab de deux éléments quelconques $a, b \in \mathfrak{G}$ la matrice produit AB.

Si la correspondance est un *isomorphisme* (c'est-à-dire si $\Gamma(x)$ est l'image d'un seul élément $x \in \mathfrak{G}$), la représentation est dite *fidèle*.

Deux représentations linéaires Γ et Γ' d'un même groupe $\mathfrak{G}$ sont dites *équivalentes* si : $\Gamma'(x) = S\,\Gamma(x)\,S^{-1}$ quel que soit $x \in \mathfrak{G}$, S désignant une matrice fixe de $\mathfrak{L}^K(n)$. Cette relation d'équivalence étant réflexive, symétrique et transitive permet la répartition des représentations linéaires de $\mathfrak{G}$ en *classes de représentations équivalentes*.

Je désignerai dans la suite par r le corps des nombres réels et par k celui des nombres complexes.

2.2. Les substitutions linéaires et homogènes, à coefficients dans k, *unitaires* (c'est-à-dire où l'inverse de la matrice A est la transposée de la matrice complexe conjuguée : $A\overline{A}' = E$, E désignant la matrice unité) forment un groupe continu, le *groupe unitaire* $\mathfrak{U}(n)$, sous-groupe de $\mathfrak{L}^k(n)$. Une représentation du groupe abstrait $\mathfrak{G}$ dans $\mathfrak{U}(n)$ est dite *représentation linéaire unitaire*, de degré n.

Les substitutions de $\mathfrak{U}(n)$ à coefficients réels (caractérisées par $AA' = E$) forment le *groupe orthogonal* $\mathfrak{U}^r(n)$, sous-groupe de $\mathfrak{L}^r(n)$. Une représentation du groupe abstrait $\mathfrak{G}$ dans $\mathfrak{U}^r(n)$ est dite *représentation linéaire orthogonale*[5]), de degré n.

Toute représentation linéaire d'un groupe fini $\mathfrak{G}$ dans $\mathfrak{L}^k(n)$ est équivalente à une représentation unitaire.

Toute représentation linéaire d'un groupe fini $\mathfrak{G}$ dans $\mathfrak{L}^r(n)$, c'est-à-dire à coefficients réels, est équivalente à une représentation orthogonale[6]).

Il peut être commode d'utiliser un langage géométrique et d'appeler *rotation* une substitution orthogonale d'ordre n quelconque. Une telle substitution transforme en elle-même la sphère à $(n-1)$ dimensions S^{n-1} définie par $\sum_{i=1}^{n} x_i^2 = 1$ dans l'espace euclidien réel E^n. Les substitutions orthogonales de déterminant $+1$ sont les rotations proprement dites

[4]) La théorie des représentations linéaires des groupes finis est exposée dans Speiser [4] chapitres 11 à 15. On y trouve les indications bibliographiques relatives aux travaux de Frobenius et Schur. Voir également [5] chap. XIII à XVII.

[5]) Je prends systématiquement la locution „représentation orthogonale" dans le sens de représentation orthogonale réelle.

[6]) Les démonstrations de ces deux théorèmes sont données par exemple dans [4] Sätze 134 und 132. Le premier a été étendu par H. Weyl aux groupes continus compacts.

(elles forment le groupe orthogonal propre $\mathfrak{U}_1^r(n)$), celles de déterminant -1, des rotations suivies de certaines symétries.

J'envisage souvent dans la suite un groupe de substitutions linéaires comme représentation d'un groupe abstrait.

2.3. *Définition : Une représentation Γ d'un groupe abstrait $\mathfrak{G}$ par des substitutions linéaires homogènes, à coefficients réels ou complexes, est dite sans points fixes si, pour aucun élément $a \in \mathfrak{G}$, différent de l'élément unité e, la matrice $\Gamma(a)$ n'admet la valeur propre $+1$.*

Le déterminant $|\Gamma(a) - E|$ est alors $\neq 0$. $\Gamma(a)$, envisagée comme transformation linéaire d'un espace vectoriel, n'admet aucun point fixe en dehors de l'origine de cet espace.

Une représentation sans points fixes est nécessairement fidèle.

Dans deux représentations équivalentes, les matrices correspondant au même élément de $\mathfrak{G}$ ont les mêmes valeurs propres. *La recherche de tous les groupes linéaires finis sans points fixes se ramène à celle des groupes linéaires finis unitaires sans points fixes.*

2.4. *Un groupe abélien fini $\mathfrak{G}$ qui admet une représentation linéaire sans points fixes est nécessairement cyclique.*

En effet, cette représentation peut être décomposée en ses composantes irréductibles (unitaires) qui toutes sont sans points fixes. Soit Γ l'une d'elles : la correspondance $\mathfrak{G} \to \Gamma$ est fidèle, c'est un isomorphisme (conséquence de l'absence de points fixes). Les représentations linéaires irréductibles d'un groupe abélien étant de degré 1, les éléments de Γ sont les g matrices (ε^k) $k = 1, 2, \ldots, g$ où g désigne l'ordre de $\mathfrak{G}$ et ε une racine primitive $g^{\text{ième}}$ de l'unité. Γ est un groupe cyclique, donc $\mathfrak{G}$ est cyclique.

2.5. Passons au cas d'un groupe fini quelconque $\mathfrak{G}$ admettant une représentation linéaire Γ sans points fixes. Les matrices de Γ correspondant aux éléments d'un sous-groupe $\mathfrak{H}$ de $\mathfrak{G}$ forment une représentation linéaire sans points fixes de $\mathfrak{H}$. Si $\mathfrak{H}$ est abélien, il est forcément cyclique (2.4). $\mathfrak{G}$ est donc tel que ses sous-groupes abéliens sont tous cycliques. Le théorème 1.3 permet d'affirmer que :

Tout groupe abstrait fini $\mathfrak{G}$ qui admet une représentation linéaire sans points fixes est du premier ou du deuxième type, c'est-à-dire que ses p-sous-groupes de Sylow sont cycliques pour $p \neq 2$, cycliques ou quaternioniques pour $p = 2$.

Ce théorème est dû à Burnside [7] qui l'a établi par une voie différente. Il montre qu'un p-groupe admettant des représentations sans points fixes est cyclique pour $p \neq 2$ et cyclique ou quaternionique pour $p = 2$.

Chapitre II

Structure des groupes du premier et du deuxième type

§ 3. Groupes cycliques et quaternioniques, quelques lemmes

Je rappelle tout d'abord quelques propriétés des groupes cycliques et quaternioniques, en précisant la nature du groupe de leurs automorphismes.

3.1. Les sous-groupes (tous invariants) d'un groupe abélien sont abéliens ainsi que les groupes-quotient correspondants. Plus particulièrement, les sous-groupes et les groupes-quotient d'un groupe cyclique sont cycliques. Le groupe des automorphismes d'un groupe cyclique d'ordre m est abélien : c'est le groupe multiplicatif des classes de restes modulo m premières au module[7]). Je le désigne par $\mathfrak{G}m$. Son ordre est donné par la fonction d'Euler $\varphi(m) = m \prod_{p_i/m}\left(1 - \frac{1}{p_i}\right)$.

L'exposant d'un groupe $\mathfrak{G}$ est le plus petit entier n tel que $a^n = e$ quel que soit $a \in \mathfrak{G}$. C'est le p.p.c.m. des ordres des éléments de $\mathfrak{G}$. Pour un groupe abélien où $(ab)^n = a^n b^n$, c'est l'ordre maximum des éléments du groupe. L'exposant de $\mathfrak{G}m$ est donné par la fonction $\lambda(m)$, définie de la façon suivante :

$$\lambda(2^\alpha) = \left\{ \begin{array}{ll} \varphi(2^\alpha) & \alpha = 1, 2 \\ \frac{1}{2}\varphi(2^\alpha) & \alpha > 2 \end{array} \right\} \qquad \lambda(p^\alpha) = \varphi(p^\alpha) \quad p \text{ premier impair}$$

$$\lambda(m) = \text{p.p.c.m. des } \lambda(p_i^{\alpha_i})$$

$m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ étant la décomposition de m en facteurs premiers distincts.

Lorsque $\lambda(m) = \varphi(m)$, $\mathfrak{G}m$ contient un élément d'ordre $\varphi(m)$ et il est cyclique. Ce cas ne se présente que pour $m = 2, 4, p^\alpha, 2p^\alpha$ (p premier impair). Ainsi, $\mathfrak{G}2^\alpha$, d'ordre $2^{\alpha-1}$, est cyclique pour $\alpha = 1, 2$ mais abélien de type $(2^{\alpha-2}, 2)$ pour $\alpha > 2$.

Le groupe des automorphismes d'un groupe abélien non cyclique n'est pas abélien.

3.2. Pour l'étude des groupes quaternioniques $\mathfrak{Q}\,2^\alpha$ (1.2), il faut distinguer le cas $\alpha = 3$ du cas $\alpha > 3$. Le groupe des quaternions $\mathfrak{Q}8$, donné par :

$$A^4 = E \qquad B^2 = A^2 \qquad BAB^{-1} = A^{-1}$$

---

[7]) [3] p. 109.

admet la répartition suivante en classes d'éléments conjugués, les éléments d'une même classe étant rangés dans la même colonne :

$$\begin{array}{ccccc} E & A^2 & A & B & BA \\ & & A^3 & BA^2 & BA^3 \end{array}$$

Tous ses sous-groupes sont invariants (un tel groupe est dit hamiltonien). $\{A^2\}$ est le seul d'ordre 2 ; c'est le centre (sous-groupe formé des éléments permutables avec tous les éléments du groupe) et en même temps le groupe des commutateurs (3.4). Le groupe-quotient correspondant est abélien de type (2, 2), c'est le groupe rectangle $D2$. Les sous-groupes d'ordre 4 sont au nombre de trois : $\{A\}$, $\{B\}$, $\{BA\}$. Ils sont cycliques et le groupe-quotient correspondant est cyclique d'ordre 2. Le groupe des automorphismes, d'ordre 24, est isomorphe au groupe symétrique $\mathfrak{S}_4$ [8]). Son ordre est divisible par 3, ce qui n'est plus le cas pour le groupe des automorphismes d'un groupe généralisé $\mathfrak{Q}\, 2^\alpha$ où $\alpha > 3$.

Un tel groupe, defini par :

$$A^{2^{\alpha-1}} = E \qquad B^2 = A^{2^{\alpha-2}} \qquad BAB^{-1} = A^{-1}$$

admet la répartition suivante en classes d'éléments conjugués où, comme ci-dessus, les éléments d'une même classe sont dans la même colonne :

$$\begin{array}{cccccccc} E & A^{2^{\alpha-2}} & A & A^2 & A^3 & A^4 \ldots A^{2^{\alpha-2}-1} & B & BA \\ & & A^{-1} & A^{-2} & A^{-3} & A^{-4} \ldots A^{-2^{\alpha-2}+1} & BA^2 & BA^3 \\ & & & & & & \vdots & \vdots \\ & & & & & & BA^{2^{\alpha-1}-2} & BA^{2^{\alpha-1}-1} \end{array}$$

$\{A^{2^{\alpha-2}}\}$ est le seul sous-groupe d'ordre 2 ; c'est le centre et le groupe-quotient correspondant est le groupe diédrique $D2^{\alpha-2}$ d'ordre $2^{\alpha-1}$.

Les sous-groupes d'ordre 4 sont tous cycliques, un seul est invariant $\{A^{2^{\alpha-3}}\}$, le groupe-quotient correspondant est $D2^{\alpha-3}$ d'ordre $2^{\alpha-2}$. Les autres, tels que $\{B\}$, $\{BA\}$, $\{BA^2\}, \ldots$ sont en nombre égal à $2^{\alpha-2}$.

Si $\alpha > 4$, un seul sous-groupe d'ordre 8 est invariant c'est le groupe cyclique $\{A^{2^{\alpha-4}}\}$, le groupe-quotient est $D2^{\alpha-4}$ d'ordre $2^{\alpha-3}$. Il existe $2^{\alpha-3}$ sous-groupes non invariants tels que $\{A^{2\alpha-3}, B\}$, $\{A^{2^{\alpha-3}}, BA\}$, $\{A^{2^{\alpha-3}}, BA^2\}$, isomorphes au groupe des quaternions $\mathfrak{Q}8$.

---

[8]) [3] p. 111.

Les sous-groupes d'ordre $2^\beta (2 < \beta < \alpha - 2, \alpha > 4)$ sont, l'un cyclique invariant à groupe-quotient diédrique, les autres non invariants isomorphes au groupe $\mathfrak{Q}2^\beta$.

Mais voici les plus intéressants : tout d'abord le groupe des commutateurs (3.4) d'ordre $2^{\alpha-2}$, cyclique, engendré par $A^2 = BA^{-1}B^{-1}A$, dont le groupe-quotient est le groupe rectangle $D2$, abélien d'ordre 4 et de type (2,2). Les autres sous-groupes du même ordre sont non invariants, en nombre égal à 4, engendrés par A^4 et l'un des éléments B, BA^2, BA ou BA^3, isomorphes à $\mathfrak{Q}2^{\alpha-2}$.

Les sous-groupes d'ordre $2^{\alpha-1}$ sont invariants, parce que d'indice 2. Ils sont en nombre égal à 3 : l'un est cyclique, $\{A\}$, les deux autres isomorphes à $\mathfrak{Q}2^{\alpha-1}$, $\{A^2, B\}$ et $\{A^2, BA\}$. Dans chaque cas, le groupe-quotient est cyclique d'ordre 2.

Tout automorphisme de $\mathfrak{Q}2^\alpha (\alpha > 3)$ s'obtient par la substitution d'éléments générateurs $A \to A^\mu$, $B \to BA^\nu$ (μ impair, ν quelconque) ; leur nombre est $2^{\alpha-2} \cdot 2^{\alpha-1} = 2^{2\alpha-3}$. C'est l'ordre du groupe des automorphismes de $\mathfrak{Q}2^\alpha$. Pour $\alpha = 3$, les classes de B et BA, renfermant deux éléments, peuvent s'échanger avec la classe de A, d'où un nombre plus grand d'automorphismes.

3.3. Lemme : *Soit $\mathfrak{P}$ un des p-sous-groupes de Sylow de $\mathfrak{G}$ et $\mathfrak{N}$ un sous-groupe invariant de $\mathfrak{G}$; alors $\mathfrak{N} \cap \mathfrak{P}$ est p-sous-groupe de Sylow de $\mathfrak{N}$ et $\mathfrak{P}\mathfrak{N}/\mathfrak{N} \cong \mathfrak{P}/\mathfrak{N} \cap \mathfrak{P}$ est p-sous-groupe de Sylow de $\mathfrak{G}/\mathfrak{N}$.*

Une démonstration de ce théorème, due à Witt, est exposée à la page 100 du livre de Zassenhaus [3].

Remarquons que l'intersection $\mathfrak{N} \cap \mathfrak{P}$ du sous-groupe invariant $\mathfrak{N}$ avec un p-sous-groupe de Sylow $\mathfrak{P}$ est un sous-groupe invariant de $\mathfrak{P}$ (égal à $\mathfrak{P}$ si $\mathfrak{P}$ est dans $\mathfrak{N}$). Ce lemme permet de trouver les p-sous-groupes de Sylow de $\mathfrak{G}/\mathfrak{N}$. En particulier, pour un groupe du premier type, $\mathfrak{P}$ étant cyclique, les p-sous-groupes de Sylow de $\mathfrak{G}/\mathfrak{N}$ sont cycliques quel que soit le sous-groupe invariant $\mathfrak{N}$; $\mathfrak{G}/\mathfrak{N}$ est donc aussi du premier type. Pour un groupe du deuxième type, $\mathfrak{G}/\mathfrak{N}$ a ses p-sous-groupes de Sylow ($p \neq 2$) cycliques ; quant à ses 2-sous-groupes de Sylow, ils sont : non abéliens (diédriques ou quaternioniques), abéliens d'ordre 4 (isomorphes au groupe rectangle $D2$), cycliques d'ordre 2 ou inexistants si $\mathfrak{Q} \subset \mathfrak{N}$.

3.4. $\mathfrak{G}$ étant un groupe abstrait quelconque, je désigne par $\mathfrak{G}'$ son *groupe dérivé* ou *groupe des commutateurs*. C'est le sous-groupe caractéristique (invariant par les automorphismes de $\mathfrak{G}$) engendré par les commutateurs $(a, b) = aba^{-1}b^{-1}$, a et b étant deux éléments quelconques de $\mathfrak{G}$. Les deux produits ab et ba, qui peuvent ne pas être identiques

dans un groupe non abélien, sont congrus modulo le sous-groupe des commutateurs car $ab = (aba^{-1}b^{-1})ba$. En conséquence, le groupe-quotient $\mathfrak{G}/\mathfrak{G}'$ est abélien. Le groupe dérivé de $\mathfrak{G}'$ est le deuxième dérivé de $\mathfrak{G}$ et je le représente par $\mathfrak{G}''$. Les sous-groupes dérivés successifs sont tous caractéristiques et même complètement invariants en ce sens qu'un opérateur quelconque les applique sur eux-mêmes ou sur une partie d'eux-mêmes.

Considérons la série des groupes dérivés : $\mathfrak{G} \supseteq \mathfrak{G}' \supseteq \mathfrak{G}'' \supseteq \cdots$. $\mathfrak{G}$ est dit *résoluble* si elle se termine par E (le groupe formé seulement de l'élément unité). Pour un groupe fini, cette condition est équivalente à celle-ci : $\mathfrak{G}$ admet une série de composition à groupes-quotient cycliques d'ordre premier. Un groupe $\mathfrak{G}$ résoluble pour lequel $\mathfrak{G}^{k-1} \neq \mathfrak{G}^k = E$ est dit *métabélien de rang k*, la série des groupes dérivés admettant k groupes-quotient abéliens. Métabélien de rang 1 est synonyme d'abélien différent de E.

Le $r^{\text{ième}}$ dérivé du groupe $\mathfrak{G}/\mathfrak{N}$, quotient de $\mathfrak{G}$ par un sous-groupe invariant $\mathfrak{N}$ est donné par :

$(\mathfrak{G}/\mathfrak{N})^{(r)} = \mathfrak{G}^{(r)}\mathfrak{N}/\mathfrak{N}$; ainsi, lorsque le $r^{\text{ième}}$ groupe dérivé de $\mathfrak{G}/\mathfrak{N}$ est E, le $r^{\text{ième}}$ groupe dérivé de $\mathfrak{G}$ est dans $\mathfrak{N}$ [9]).

3.5. Lemme: *Si dans la série $\mathfrak{G}' \supseteq \mathfrak{G}'' \supseteq \mathfrak{G}'' \ldots$ des dérivés d'un groupe $\mathfrak{G}$, deux groupes-quotient consécutifs sont cycliques, le second se réduit à l'identité.*

Ce théorème est démontré par Zassenhaus [3] th. 9 p. 138.

Il importe de remarquer que la série dont il est question dans le lemme débute par $\mathfrak{G}'$, le premier groupe dérivé, et non par $\mathfrak{G}$ comme dans 3.4.

§ 4. Groupes du premier type

Rappelons qu'un groupe $\mathfrak{G}$ fini est dit du premier type si ses sous-groupes de Sylow sont tous cycliques (1.3). Ces groupes sont étudiés dans les traités classiques [10]). Voici les points essentiels accompagnés de quelques remarques utiles pour la suite.

4.1. *Un groupe fini $\mathfrak{G}$, dont tous les sous-groupes de Sylow sont cycliques, est résoluble.*

Pour démontrer ce théorème, Zassenhaus [11]) procède par induction complète sur le nombre des facteurs premiers distincts de l'ordre de $\mathfrak{G}$.

---

[9]) Pour les démonstrations, voir par exemple [3] pp. 55 et 56.

[10]) Zassenhaus [3] p. 139, Burnside [5] pp. 163 à 166 et [6]. Je suis de préférence Zassenhaus.

[11]) [3] p. 139.

Soit $g = p_1^{\alpha_1} p_2^{a_2} \ldots p_k^{\alpha_k}$ cet ordre, où les p_i vont en croissant. Il montre qu'un p_1-sous-groupe de Sylow $\mathfrak{P}_1$ de $\mathfrak{G}$ est contenu dans le centre de son normalisateur (sous-groupe formé des éléments de $\mathfrak{G}$ permutables avec $\mathfrak{P}_1$). $\mathfrak{G}$ contient dès lors un sous-groupe invariant $\mathfrak{N}$ avec $\mathfrak{P}_1$ comme système de représentants (théorème de Burnside) [12]). L'hypothèse d'induction est applicable à $\mathfrak{N}$: $\mathfrak{N}$ est résoluble, donc $\mathfrak{G}$ est résoluble (3.4).

Un fait n'est pas établi par Zassenhaus, mais par contre par Burnside [10]): c'est que le sous-groupe invariant $\mathfrak{N}$ d'ordre $p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ est caractéristique. Plus exactement encore, il existe une suite de sous-groupes caractéristiques d'ordres $p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \ldots p_k^{\alpha_k}$ $(i = 2, 3, \ldots, k)$. Chacun de ces sous-groupes invariants est en effet d'ordre premier à son indice. Les théorèmes de Sylow généralisés, dus à Hall [13]), permettent d'affirmer qu'un tel sous-groupe est seul de son espèce. Il est par conséquent transformé en lui-même par tout automorphisme de $\mathfrak{G}$.

4.2. *La série des groupes dérivés d'un groupe $\mathfrak{G}$ du premier type est $\mathfrak{G} \supset \mathfrak{G}' \supset E$ où le groupe des commutateurs $\mathfrak{G}'$ est cyclique, à groupe-quotient $\mathfrak{G}/\mathfrak{G}'$ également cyclique* [11]).

En effet, tous les groupes de la série des dérivés de $\mathfrak{G}$ (3.4) $\mathfrak{G} \supseteq \mathfrak{G}' \supseteq \mathfrak{G}''$... sont du premier type. Les groupes-quotient sont abéliens à sous-groupes de Sylow cycliques (3.3), donc cycliques. $\mathfrak{G}'/\mathfrak{G}''$ cyclique et $\mathfrak{G}''/\mathfrak{G}'''$ cyclique entraînent, d'après le lemme 3.5, $\mathfrak{G}''/\mathfrak{G}''' = E$; d'où $\mathfrak{G}'' = \mathfrak{G}''' = E$, le groupe étant résoluble (4.1). La suite des groupes dérivés se réduit bien à $\mathfrak{G} \supset \mathfrak{G}' \supset E$. Les groupes-quotient restent cycliques, d'où $\mathfrak{G}/\mathfrak{G}'$ cyclique, $\mathfrak{G}'$ cyclique. Ces conditions sont nécessaires pour que $\mathfrak{G}$ soit du premier type, mais pas suffisantes, comme le montre l'exemple du groupe diédrique $D4$ d'ordre 8, dont le groupe des commutateurs est cyclique d'ordre 4 à groupe-quotient cyclique d'ordre 2, et n'est pourtant pas du premier type (le seul groupe du premier type d'ordre 8 étant $\mathfrak{Z}8$ cyclique).

4.3. *Si $\mathfrak{G}'$ est du premier type, il est cyclique. En d'autres termes, un groupe du premier type, non cyclique, n'est le dérivé d'aucun autre groupe.*

Ce corollaire du théorème précédent s'établit immédiatement. Si $\mathfrak{G}'$ est du premier type, $\mathfrak{G}' \supset \mathfrak{G}'' \supset E$, $\mathfrak{G}'/\mathfrak{G}''$ cyclique, $\mathfrak{G}''$ cyclique; $\mathfrak{G}'' = E$ d'après le lemme 3.5 et $\mathfrak{G}'$ est cyclique.

---

[12]) [5] p. 327, [4] Satz 122.
[13]) [3] p. 127.

4.4. Zassenhaus[11]) utilise ces considérations pour construire tous les groupes à sous-groupes de Sylow cycliques au moyen de deux éléments : l'un engendrant le groupe des commutateurs, l'autre appartenant à une classe modulo le groupe des commutateurs qui engendre le groupe-quotient. Il s'assure ensuite que les générateurs et relations définissent bien un groupe ayant les propriétés voulues en faisant appel au théorème de Hölder relatif aux groupes finis ayant un sous-groupe invariant cyclique d'ordre m à groupe-quotient cyclique d'ordre n.

Un tel groupe est défini par :

$$A^m = E \qquad B^n = A^t \qquad BAB^{-1} = A^r \tag{1}$$

avec les conditions numériques

$$\text{a)}\ \ m, n > 0 \qquad g = mn \qquad \text{b)}\ \ r^n \equiv 1\,(m) \qquad \text{c)}\ \ t(r-1) \equiv 0\,(m)\ .$$

Or ce théorème est une application particulière de la théorie de l'extension de Schreier[14]) qui pose et résout le problème suivant :

On donne deux groupes abstraits $\mathfrak{N}$ et $\mathfrak{F}$; trouver tous les groupes $\mathfrak{G}$ admettant $\mathfrak{N}$ comme sous-groupe invariant de telle manière que le groupe-quotient $\mathfrak{G}/\mathfrak{N}$ soit isomorphe à $\mathfrak{F}$.

$\mathfrak{G}$ est une extension de $\mathfrak{N}$ par $\mathfrak{F}$. Dans le cas qui nous occupe, il s'agit d'une extension par un groupe $\mathfrak{F} = \mathfrak{G}/\mathfrak{G}'$ cyclique, je parlerai d'extensions cycliques. Comme $\mathfrak{N} = \mathfrak{G}'$ est aussi cyclique, nous retrouvons le cas particulier de Hölder. Plus loin, pour les groupes du deuxième type, j'aurai à déterminer des extensions par un groupe abélien, je parlerai d'extensions abéliennes.

4.5. Tout groupe $\mathfrak{G}$ du premier type et d'ordre g est donné par[11]) :

$$A^m = E \qquad B^n = E \qquad BAB^{-1} = A^r \tag{2}$$

avec les conditions numériques

$$\text{a)}\ \ m > 0\,, \quad mn = g \qquad \text{b)}\ \ \big((r-1)n, m\big) = 1 \qquad \text{c)}\ \ r^n \equiv 1\,(m)$$

et réciproquement.

Le groupe des commutateurs $\mathfrak{G}'$ est cyclique engendré par $BAB^{-1}A^{-1} = A^{r-1}$; comme $r-1$ est premier à m en vertu de b), c'est $\{A\}$. On vérifie que le groupe-quotient $\mathfrak{G}/\mathfrak{G}'$ est cyclique engendré par B. La condition accessoire n premier à m assure que tout sous-groupe de Sylow admet un conjugué dans $\{A\}$ ou $\{B\}$; il est donc cyclique. Ceci élimine les groupes analogues à $D4$, signalé à la fin de 4.2. La condition c) est une

[14]) Exposée aux §§ 6 à 8 du chap. III de Zassenhaus [3].

conséquence des relations (2) : $BAB^{-1} = A^r$ entraîne $B^\nu AB^{-\nu} = A^{r^\nu}$; comme $B^n = E$, r^n doit être $\equiv 1$ (modulo m).

4.6. Tirons quelques conséquences des conditions numériques b) et c). Toute racine de la congruence $r^n \equiv 1\,(m)$ est première au module : $(r, m) = 1$. De plus, n est multiple de l'exposant d auquel appartient la racine r (d est l'exposant de la plus petite puissance de r congrue à 1 modulo m, c'est l'ordre de r dans $\mathfrak{G}m$ (3.1)). La condition $(r, m) = 1$ jointe à $(r - 1, m) = 1\,(b)$, prouve que m doit être impair. *Le groupe des commutateurs d'un groupe du premier type est cyclique d'ordre impair.*

Les seules valeurs admissibles pour r sont telles que r, $r - 1$ et l'ordre de r dans $\mathfrak{G}m$ soient premiers à m.

On peut se demander, m et n étant fixés, s'il existe plusieurs groupes (1) de structures différentes. Dans la théorie de l'extension cyclique, c'est le groupe des automorphismes de $\mathfrak{N}$ qui joue le rôle important. Or ici, $\mathfrak{N} = \mathfrak{G}' = \{A\}$ est le groupe cyclique d'ordre m impair. Son groupe des automorphismes est précisément $\mathfrak{G}m$, le groupe multiplicatif des classes de restes modulo m premières au module. La condition donnée dans la théorie de l'extension cyclique, pour l'isomorphisme sur $\mathfrak{N}$ de deux extensions, se traduit ici par le fait qu'on obtient toutes les extensions isomorphes en remplaçant r par r^ν où $(\nu, n) = 1$. D'ailleurs, dans cette hypothèse, B^ν engendre le groupe $\{B\}$ et $B^\nu AB^{-\nu} = A^{r^\nu}$; la correspondance $A \to A$, $B \to B^\nu$ réalise l'isomorphisme.

§ 5. Groupes du deuxième type

Rappelons qu'un groupe fini $\mathfrak{G}$ est dit du deuxième type si ses p-sous-groupes de Sylow sont cycliques pour $p \neq 2$, quaternioniques pour $p = 2$ (1.3). L'ordre d'un tel groupe est divisible par une puissance de 2 supérieure ou égale à la troisième, donc au minimum par 8.

Quelques indications relatives à ces groupes se trouvent dans deux travaux de Burnside [6], [7].

5.1. Les groupes du deuxième type se subdivisent en groupes résolubles et groupes non résolubles.

Soit $\mathfrak{G}$ un groupe du deuxième type d'ordre $g = 2^\alpha p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $\alpha \geqslant 3$, $\mathfrak{Q}2^\alpha$ l'un de ses 2-sous-groupes de Sylow. $\mathfrak{Q}2^\alpha$, n'étant pas abélien, ne saurait être contenu dans le centre de son normalisateur, et l'on ne peut par suite établir l'existence d'un sous-groupe invariant d'ordre $p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ par la méthode indiquée en 4.1. En fait, $\mathfrak{G}$ peut ne pas être résoluble, comme le prouve l'exemple du groupe binaire de l'icosaèdre $\mathfrak{J}^*$ défini en

6.4. Ce groupe est du deuxième type et coïncide avec son groupe des commutateurs : $\mathfrak{J}^{*\prime} = \mathfrak{J}^*$.

5.2. Le groupe-quotient $\mathfrak{G}/\mathfrak{G}'$, d'un groupe du deuxième type par son groupe des commutateurs est soit abélien de type $(2, 2, u)$, soit cyclique d'ordre $2u$ ou u, u étant impair. Il peut se réduire à l'identité, son ordre étant alors $u = 1$.

Démonstration : $\mathfrak{G}'$ étant sous-groupe de $\mathfrak{G}$, est du premier ou du deuxième type. S'il est du premier type, il est cyclique d'après 4.3. Dans tous les cas, il contient le groupe des commutateurs du sous-groupe $\mathfrak{Q}2^\alpha$, c'est-à-dire le groupe cyclique $\{A^2\}$ d'ordre $2^{\alpha-2}$. L'intersection $\mathfrak{G}' \cap \mathfrak{Q}2^\alpha$ est un sous-groupe invariant de $\mathfrak{Q}2^\alpha$ contenant $\{A^2\}$. D'après 3.2 ce ne peut être que l'un des groupes suivants : $\{A^2\}$ lui-même, d'ordre $2^{\alpha-2}$; $\{A\}$, cyclique d'ordre $2^{\alpha-1}$; $\{A^2, B\}$ ou $\{A^2, BA\}$, quaternioniques d'ordre $2^{\alpha-1}$; $\mathfrak{Q}2^\alpha$ d'ordre 2^α.

Les p-sous-groupes de Sylow de $\mathfrak{G}/\mathfrak{G}'$, sont donnés par le lemme 3.3. Pour $p = 2$, ils sont isomorphes soit au groupe rectangle $D2$, soit au groupe cyclique d'ordre 2, $\mathfrak{Z}2$, ou enfin inexistants si $\mathfrak{G}/\mathfrak{G}'$ est d'ordre impair. Pour $p \neq 2$, ils sont cycliques.

Le groupe abélien $\mathfrak{G}/\mathfrak{G}'$ est donc soit $D2 \times \mathfrak{Z}u = \mathfrak{Z}2 \times \mathfrak{Z}2u$ (groupe abélien de type $(2, 2, u)$), soit $\mathfrak{Z}2u$, soit $\mathfrak{Z}u$ (u impair). Il se réduit à $E = \mathfrak{Z}1$ si $\mathfrak{G} = \mathfrak{G}'$.

Remarques : Si $\mathfrak{G}/\mathfrak{G}'$ est abélien de type $(2, 2, u)$, $\mathfrak{G}'$ est du premier type, donc cyclique.

Si $\mathfrak{G}' \cap \mathfrak{Q}2^\alpha = \{A\}$, $\mathfrak{G}'$ est également du premier type, donc cyclique, le groupe quotient $\mathfrak{G}/\mathfrak{G}'$ étant aussi cyclique. Ce cas ne peut en fait pas se présenter, ce qu'on vérifie en partant du théorème de Hölder (4.4).

Si $\mathfrak{G}'$ est du deuxième type, $\mathfrak{G}/\mathfrak{G}'$ est cyclique.

5.3. Si dans la série des groupes dérivés (3.4) d'un groupe $\mathfrak{G}$ du deuxième type, trois groupes dérivés consécutifs sont du deuxième type, les deux derniers sont identiques.

C'est une conséquence du lemme 3.5. Trois groupes dérivés consécutifs définissent deux groupes-quotient successifs, cycliques en vertu de 5.2, le second se réduit à l'identité.

5.4. Il en résulte la classification suivante des groupes $\mathfrak{G}$ du deuxième type :

Résolubles :

a) $\mathfrak{G} \supset \mathfrak{G}' \supset E$ b) $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset E$ c) $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset \mathfrak{G}''' \supset E$.

Le groupe précédant E est cyclique, les autres du deuxième type. *Un groupe du deuxième type résoluble est métabélien de rang 2, 3 ou 4.*

Non résolubles :

d) $\mathfrak{G} = \mathfrak{G}'$ e) $\mathfrak{G} \supset \mathfrak{G}' = \mathfrak{G}''$ f) $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' = \mathfrak{G}'''$.

Voici un exemple, le plus simple possible, pour chacune de ces six catégories :

a) $\mathfrak{Q}2^\alpha$, premier groupe dérivé $\{A^2\}$ cyclique d'ordre $2^{\alpha-2}$, groupe-quotient $D2$,

b) le groupe tétraédrique binaire $\mathfrak{T}^*$ (6.2), suite des groupes dérivés : $\mathfrak{T}^* \supset \mathfrak{Q}8 \supset \{A^2\} \supset E$,

c) le groupe octaédrique binaire $\mathfrak{O}^*$ (6.3), suite des groupes dérivés : $\mathfrak{O}^* \supset \mathfrak{T}^* \supset \mathfrak{Q}8 \supset \{A^2\} \supset E$,

d) le groupe icosaédrique binaire $\mathfrak{J}^*$ (6.4) : $\mathfrak{J}^{*\prime} = \mathfrak{J}^*$,

e) le produit direct $\mathfrak{J}^* \times \mathfrak{Z}m$ $(m, 120) = 1$,

f) le produit direct de $\mathfrak{J}^*$ par un groupe du premier type, non cyclique, d'ordre premier à 120 (un tel groupe existe, voir 8.3).

Je vais déterminer tous les groupes du deuxième type métabéliens de rang 2 (a), puis indiquer la possibilité théorique de construire ceux de rangs 3 (b) et 4 (c) (comme exemples, je retrouverai $\mathfrak{T}^*$ et $\mathfrak{O}^*$). Les groupes du deuxième type parfaits ($\mathfrak{G} = \mathfrak{G}'$, classe d) échappent à mes méthodes ; on pourrait en déduire ceux des classes (e) et (f).

5.5. La condition nécessaire et suffisante, pour qu'un groupe $\mathfrak{G}$ du deuxième type soit métabélien de rang 2, est qu'il contienne un sous-groupe invariant $\mathfrak{N}$ dont l'ordre soit la partie impaire de l'ordre de $\mathfrak{G}$.

La condition est suffisante : si $\mathfrak{G}$ du deuxième type d'ordre $2^\alpha p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $\alpha \geqslant 3$, contient un sous-groupe invariant $\mathfrak{N}$ d'ordre $p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, le groupe-quotient $\mathfrak{G}/\mathfrak{N}$ est isomorphe à l'un des sous-groupes de Sylow $\mathfrak{Q}2^\alpha$. Au sous-groupe invariant $\{A^2\}$ de $\mathfrak{Q}2^\alpha$ (son groupe des commutateurs) correspond un sous-groupe invariant $\mathfrak{M}$ de $\mathfrak{G}$ contenant $\mathfrak{G}'$ en vertu de l'isomorphisme $\mathfrak{G}/\mathfrak{M} \cong \mathfrak{G}/\mathfrak{N}/\mathfrak{M}/\mathfrak{N} \cong \mathfrak{Q}2^\alpha/\{A^2\} \cong D2$ abélien. $\mathfrak{M}$ est d'ordre $2^{\alpha-2} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Or l'ordre de $\mathfrak{G}'$ est divisible au moins par $2^{\alpha-2}$ (5.2); cet ordre est donc exactement divisible par $2^{\alpha-2}$. L'intersection $\mathfrak{G}' \cap \mathfrak{Q}2^\alpha$ est $\{A^2\}$, les 2-sous-groupes de Sylow de $\mathfrak{G}'$ sont cycliques, $\mathfrak{G}'$ est du premier type, donc cyclique (4.3), $\mathfrak{G} \supset \mathfrak{G}' \supset E$.

La condition est nécessaire : si $\mathfrak{G} \supset \mathfrak{G}' \supset E$ est la suite des dérivés d'un groupe $\mathfrak{G}$ du deuxième type, $\mathfrak{G}'$ est cyclique et $\mathfrak{G}/\mathfrak{G}'$ abélien de type $(2, 2, u)$ (5.2). $\mathfrak{G}/\mathfrak{G}'$ est engendré par a, b, c, avec $a^2 = b^2 = c^u = e$, les éléments a et b correspondant aux classes renfermant les générateurs A et B d'un des 2-sous-groupes de Sylow $\mathfrak{Q}2^\alpha$ de $\mathfrak{G}$. Ce groupe abélien a trois sous-groupes d'ordre $2u$: $\{a, c\}$, $\{b, c\}$, $\{ab, c\}$ (invariants puisque sous-groupes d'un groupe abélien).

L'un des sous-groupes invariants de $\mathfrak{G}$, celui correspondant à $\{a, c\}$, a ses 2-sous-groupes de Sylow cycliques (l'un est $\{A\}$). Il est du premier type, d'ordre $2^{\alpha-1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, et contient un sous-groupe caractéristique d'ordre $p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ (4.1), qui est le sous-groupe invariant $\mathfrak{N}$ de $\mathfrak{G}$.

Remarque : Ce sous-groupe invariant $\mathfrak{N}$ est même caractéristique, ainsi que tous les sous-groupes d'ordre $p_i^{\alpha_i}\ldots p_k^{\alpha_k}$ $(i = 2, \ldots, k)$ pour les mêmes raisons qu'en 4.1.

5.6. Rappelons un théorème de Burnside[15] :

Un groupe d'ordre $2^\alpha n$, où n est impair, non divisible par 3, et qui contient des éléments d'ordre $2^{\alpha-1}$, admet un sous-groupe invariant d'ordre n.

Ce théorème, joint au précédent, nous montre que les groupes du deuxième type dont l'ordre n'est pas divisible par 3 appartiennent à la catégorie a) dans la classification 5.4. Les cinq autres catégories ne renferment que des groupes dont l'ordre est divisible par 24 et présentent ainsi un caractère exceptionnel.

5.7. Je passe à la détermination de tous les groupes du deuxième type métabéliens de rang 2 :

$\mathfrak{G} \supset \mathfrak{G}' \supset E$, $\mathfrak{G}'$ cyclique d'ordre pair (divisible par $2^{\alpha-2}$, $\alpha \geqslant 3$), $\mathfrak{G}/\mathfrak{G}'$ abélien $(2, 2, u)$, u impair.

Il s'agit : 1) de former les extensions[16] d'un groupe cyclique $\{A\}$ par le groupe abélien $(2, 2, u) = \mathfrak{Z}2 \times \mathfrak{Z}2u$; 2) de telle sorte que le groupe des commutateurs soit $\{A\}$ et 3) que les sous-groupes de Sylow aient la structure voulue.

Voici ce que donne la théorie de l'extension abélienne dans ce cas très particulier :

$$\left.\begin{array}{lll} A^m = E & S_1^2 = A^{s_1} & S_2^{2u} = A^{s_2} \\ S_1 S_2 S_1^{-1} S_2^{-1} = (S_1, S_2) = A^r & S_1 A S_1^{-1} = A^{t_1} & S_2 A S_2^{-1} = A^{t_2} \end{array}\right\} \quad (1)$$

avec les conditions numériques :

$$\begin{array}{ll} \text{a) } t_1^2 \equiv 1\,(m) & \text{c) } s_2(t_1 - 1) \equiv r(1 + t_2 + t_2^2 + \cdots + t_2^{2u-1})\ (m) \\ \text{b) } t_2^{2u} \equiv 1\,(m) & \text{d) } s_1(t_2 - 1) \equiv -r(1 + t_1)\ (m) \end{array}$$

Retrouvons tout d'abord $\mathfrak{Q}2^\alpha$; son groupe des commutateurs étant cyclique d'ordre $2^{\alpha-2}$, c'est la valeur à choisir pour m ; on trouve :

---

[15]) [5] p. 330.

[16]) Voir 4.4 et plus particulièrement [3] p. 97.

$$\left.\begin{array}{lll} A^{2^{\alpha-2}} = E & S_1^2 = A & S_2^2 = A^{2^{\alpha-3}} \\ (S_1, S_2) = A & S_1 A S_1^{-1} = A & S_2 A S_2^{-1} = A^{-1} \end{array}\right\} \quad (2)$$

S_1 et S_2 suffisent à engendrer le groupe :

$$S_1^{2^{\alpha-1}} = E \qquad S_2^2 = S_1^{2^{\alpha-2}} \qquad S_2 S_1 S_2^{-1} = S_1^{-1}$$

ce sont les relations connues.

Pour le *cas général*, où le groupe des commutateurs est cyclique d'ordre $2^{\alpha-2}n$ (n impair), on obtient :

$$\left.\begin{array}{lll} A^{2^{\alpha-2}n} = E & S_1^2 = A^n & S_2^{2u} = A^{2^{\alpha-3}n} \\ (S_1, S_2) = A^r & S_1 A S_1^{-1} = A^{t_1} & S_2 A S_2^{-1} = A^{t_2} \end{array}\right\} \quad (3)$$

avec les conditions numériques :

$$\alpha \geqslant 3, \quad (u, n) = 1, \quad u \text{ et } n \text{ impairs}$$

$$\begin{array}{lll} t_1^2 \equiv 1\,(2^{\alpha-2}n) & t_2^{2u} \equiv 1\,(2^{\alpha-2}n) & (r, t_1 - 1, t_2 - 1) = 1 \\ t_1 \equiv 1\,(2^{\alpha-2}) & t_2 \equiv -1\,(2^{\alpha-2}) & r \equiv n\,(2^{\alpha-2}) \end{array}$$

$$r(1 + t_1) \equiv 0 \ (n) \qquad r(1 + t_2 + \cdots + t_2^{u-1}) \equiv 0 \ (n)$$

Ce groupe est d'ordre $g = 2^\alpha n u$. Il admet trois sous-groupes invariants d'indice $2u$, engendrés par A joint respectivement à S_1, S_2, $S_1 S_2^u$, en accord avec le fait que $\mathfrak{G}/\mathfrak{G}'$ abélien $(2, 2, u)$ a trois sous-groupes d'indice $2u$ (d'ordre 2). L'un, $\{A, S_1\}$, est du premier type ; les deux autres sont du premier type si $\alpha = 3$, mais du deuxième si $\alpha > 3$. Le sous-groupe invariant $\mathfrak{N}$ du premier type d'ordre nu (5.5) est engendré par $A^{2^{\alpha-2}}$ et S_2^4. Il importe de remarquer que des valeurs différentes de t_1, t_2, et r peuvent correspondre à des groupes isomorphes. Il en est ainsi, en particulier, quand on change t_2 en $t_1 t_2$ et r en $r t_1$, comme le montre l'automorphisme réalisé en conservant A et S_1, mais en substituant à S_2 l'élément générateur $S_1 S_2$.

Comme premier exemple, je forme tous les groupes du deuxième type dont le groupe des commutateurs est cyclique d'ordre 2. Ici $\alpha = 3$, $n = 1$; j'obtiens $t_1 = t_2 = r = 1$ et, en modifiant un peu les relations :

$$A^4 = E \qquad B^{2u} = A^2 \qquad BAB^{-1} = A^{-1} \ . \qquad (4)$$

Ce groupe est isomorphe au produit direct $\mathfrak{Q}8 \times \mathfrak{Z}u$ (u impair).

Un groupe du deuxième type d'ordre 24, dont le groupe des commutateurs est cyclique d'ordre 2, est isomorphe au produit direct $\mathfrak{Q}8 \times \mathfrak{Z}3$. Si le groupe des commutateurs est cyclique d'ordre 6, les formules (3) donnent un seul type :

$$A^{12} = E \qquad B^2 = A^6 \qquad BAB^{-1} = A^{-1}$$

qui est isomorphe au groupe diédrique binaire D_6^* (6.1). Ces deux groupes, joints au groupe binaire du tétraèdre (5.8), métabélien de rang 3, sont les seuls d'ordre 24 et du deuxième type. Si l'on y ajoute $\mathfrak{Z}24$ et le groupe :

$$A^3 = E \qquad B^8 = E \qquad BAB^{-1} = A^{-1}$$

qui sont du premier type, on voit que sur les 15 types[17]) de groupes d'ordre 24, 5 seulement ont leurs sous-groupes abéliens tous cycliques. Tous les 5 admettent des représentations sans points fixes.

Les groupes du deuxième type d'ordre 48 sont au nombre de quatre. Les formules (3) permettent de trouver ceux dont le groupe des commutateurs est cyclique. Pour $\mathfrak{G}'$ cyclique d'ordre 4, on obtient un seul type : $\mathfrak{Q}16 \times \mathfrak{Z}3$; $\mathfrak{G}'$ cyclique d'ordre 12, par contre, donne deux structures non isomorphes

$$A^{24} = E \qquad B^2 = A^{12} \qquad BAB^{-1} = A^{-1}$$

c'est le groupe diédrique binaire D_{12}^* (6.1) ; en outre

$$\left.\begin{array}{lll} A^{12} = E & S_1^2 = A^3 & S_2^2 = A^6 \\ (S_1, S_2) = A^3 & S_1 A S_1^{-1} = A^5 & S_2 A S_2^{-1} = A^{-1} \end{array}\right\} \qquad (5)$$

Il existe de plus un groupe d'ordre 48 du deuxième type, métabélien de rang 4 ; c'est le groupe binaire de l'octaèdre (5.9).

J'envisage encore les groupes définis par les relations (3) où $t_1 = 1$. Le sous-groupe invariant $\{A, S_1\}$ est alors cyclique et $S_1 A$, S_2 suffisent à engendrer le groupe. En modifiant les notations, les relations deviennent :

$$A^{2^{\alpha-1}n} = E \qquad B^{2u} = A^{2^{\alpha-2}n} \qquad BAB^{-1} = A^r \qquad (6)$$

avec les conditions numériques :

$$\alpha \geqslant 3\,, \qquad (u, n) = 1\,, \qquad u \text{ et } n \text{ impairs}$$

$$r^{2u} \equiv 1\,(2^{\alpha-1}n) \qquad r \equiv -1\,(2^{\alpha-1}) \qquad (r-1, 2^{\alpha-1}n) = 2\ .$$

---

[17]) [5] p. 157.

$\mathfrak{G}$ admet un sous-groupe invariant cyclique $\{A\}$ à groupe-quotient cyclique $\mathfrak{Z}2u$; le type des relations obtenues est bien celui prévu par le théorème de Hölder (4.4).

Voici la *classification* que j'établis désormais pour les groupes du deuxième type :

(α) $\mathfrak{G}'$ cyclique, contenu dans un sous-groupe invariant cyclique d'ordre double de celui de $\mathfrak{G}'$; ils sont définis par les relations (6).

(β) $\mathfrak{G}'$ cyclique, contenu dans un sous-groupe invariant du premier type, non cyclique, d'ordre double de celui de $\mathfrak{G}'$; ils sont définis par les relations (3) où $t_1 \neq 1$. Exemple : le groupe défini par les relations (5).

(γ) Tous les autres, c'est-à-dire les groupes métabéliens de rangs 3 et 4 et tous les groupes non résolubles.

D'après 5.4, (α) et (β) épuisent la catégorie a), (γ) est formé des cinq autres.

5.8. Un groupe du deuxième type, métabélien de rang 3 admet la suite des groupes dérivés $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset E$. $\mathfrak{G}'$ est du deuxième type, métabélien de rang 2, et appartient aux classes (α) ou (β). $\mathfrak{G}/\mathfrak{G}'$ est cyclique d'ordre u ou $2u$, u impair (5.2).

La théorie de l'extension cyclique[18]) permettrait de les obtenir tous. A titre d'exemple, je choisis pour $\mathfrak{G}'$ le groupe métabélien de rang 2 le plus simple, $\mathfrak{Q}8$.

Une extension cyclique d'ordre n est caractérisée par $\mathfrak{N}$ (ici $\mathfrak{Q}8$), un automorphisme σ de $\mathfrak{N}$ et par $N \in \mathfrak{N}$, invariant par σ, $N^\sigma = N$, et induisant dans $\mathfrak{N}$ l'automorphisme $N\,\mathfrak{N}\,N^{-1}$ identique à σ^n.

$\mathfrak{Q}8$, défini par $A^4 = E \quad B^2 = A^2 \quad BAB^{-1} = A^{-1}$, a 24 automorphismes (3.2). L'automorphisme d'ordre 3 défini par $A^\sigma = B$, $B^\sigma = BA$ conduit au groupe :

$$\left.\begin{array}{lll} A^4 = E & B^2 = A^2 & BAB^{-1} = A^{-1} \\ S^{3n'} = E & SAS^{-1} = B & SBS^{-1} = BA \end{array}\right\} \qquad (7)$$

qui est du deuxième type si n' est impair. Son ordre est $24n'$; pour $n' = 1$, c'est le groupe binaire du tétraèdre $\mathfrak{T}^*$ (6.2) d'ordre 24, contenant $\mathfrak{Q}8$ comme sous-groupe invariant (groupe des commutateurs) et quatre sous-groupes d'ordre 3. Sa série des dérivés est : $\mathfrak{T}^* \supset \mathfrak{Q}8 \supset \{A^2\} \supset E$. Si $n' \neq 1$ est premier à 24, (7) représente le produit direct $\mathfrak{T}^* \times \mathfrak{Z}n'$.

Pour $\mathfrak{Q}2^\alpha$, avec $\alpha > 3$, on trouve des extensions du deuxième type (par exemple $\mathfrak{Q}2^{\alpha+1}$), mais aucune ne conduit à un groupe métabélien de

---

[18]) [3] p. 94.

rang 3. En voici la raison : aucun automorphisme de $\mathfrak{Q}2^\alpha$, $\alpha > 3$, ne change $A^{2^{\alpha-3}}$ en B (3.2). Dans une extension cyclique, ces deux éléments ne peuvent être conjugués et il résulte d'un théorème de Burnside[15]) déjà cité que le groupe correspondant admet un sous-groupe invariant dont l'ordre est la partie impaire de l'ordre de $\mathfrak{G}$. Si $\mathfrak{G}$ est du deuxième type, il est métabélien de rang 2 (5.5).

5.9. Les groupes du deuxième type métabéliens de rang 4 pourraient s'obtenir à partir des groupes métabéliens de rang 3 par une nouvelle extension cyclique.

Un seul exemple fera comprendre la méthode. Partant du groupe binaire du tétraèdre $\mathfrak{T}^*$, donné par les relations (7) où $n' = 1$, j'envisage l'automorphisme : $A^\sigma = A$, $B^\sigma = BA^3$, $S^\sigma = S^2BA^2$. Cet automorphisme est d'ordre 4, il engendre entre autres l'extension suivante :

$$\left.\begin{array}{llll} & A^4 = E & B^2 = A^2 & BAB^{-1} = A^{-1} \\ & S^3 = E & SAS^{-1} = B & SBS^{-1} = BA \\ T^2 = A & TAT^{-1} = A & TBT^{-1} = BA^3 & TST^{-1} = S^2BA^2 \end{array}\right\} \quad (8)$$

Ce groupe, que je désigne par $\mathfrak{O}^*$ est d'ordre 48 et du deuxième type ; il a trois sous-groupe d'ordre 16 (l'un est engendré par A, B et T : $T^8 = E$ $B^2 = T^4$ $BTB^{-1} = T^{-1}$) isomorphes à $\mathfrak{Q}16$ et 4 sous-groupes d'ordre 3 (évidemment cycliques). Son groupe des commutateurs est d'ordre 24 et isomorphe à $\mathfrak{T}^*$. La série des groupes dérivés est :

$$\mathfrak{O}^* \supset \mathfrak{T}^* \supset \mathfrak{Q}8 \supset \{A^2\} \supset E \ .$$

J'ai pu montrer son isomorphisme avec le groupe binaire de l'octaèdre (6.3).

Cet exemple met en défaut l'affirmation de Burnside[19]) selon laquelle un groupe du deuxième type d'ordre $2^\alpha p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $\alpha > 3$, contient des sous-groupes caractéristiques de tous les ordres $p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \ldots p_k^{\alpha_k}$ ($i = 2, 3, \ldots, k$). Ce n'est le cas, en vertu de 5.5, que pour les classes (α) et (β), soit pour les groupes du deuxième type métabéliens de rang 2.

5.10. Voici un théorème qui limite le nombre des types contenus dans la classe (γ) (5.7) :

Le groupe des commutateurs $\mathfrak{G}'$ d'un groupe $\mathfrak{G}$ du deuxième type, métabélien de rang 3, a ses 2-sous-groupes de Sylow isomorphes à $\mathfrak{Q}8$.

---

[19]) [6] p. 50.

Démonstration: $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}'' \supset E$; $\mathfrak{G}'$ est métabélien de rang 2 et admet un sous-groupe caractéristique $\mathfrak{N}$ dont l'ordre est la partie impaire de l'ordre de $\mathfrak{G}$. (Remarque à la fin de 5.5.) $\mathfrak{N}$ est sous-groupe invariant de $\mathfrak{G}$: $(\mathfrak{G}/\mathfrak{N})' \cong \mathfrak{G}'\mathfrak{N}/\mathfrak{N} \cong \mathfrak{G}'/\mathfrak{N} \cong \mathfrak{Q}2^\alpha$, 2-sous-groupe de Sylow de $\mathfrak{G}'$. Ceci est impossible si $\alpha > 3$, car dans le cas contraire $\mathfrak{Q}2^\alpha$ admettrait une extension cyclique $\mathfrak{G}/\mathfrak{N}$, groupe du deuxième type, métabélien de rang 3 (5.8).

Une hypothèse, que je n'ai pu démontrer, me paraît justifiée:

Si $\mathfrak{G}'$ est du deuxième type, ses 2-sous-groupes de Sylow sont isomorphes à $\mathfrak{Q}8$.

Cette proposition (analogue à: $\mathfrak{G}'$ du premier type entraîne $\mathfrak{G}'$ cyclique) concernerait toute la classe (γ). Un groupe de cette classe aurait en particulier ses 2-sous-groupes de Sylow d'ordre au plus égal à 16. De plus, il me semble qu'un groupe $\mathfrak{G}$ de la classe (γ) doit contenir des sous-groupes d'ordre 24 isomorphes à $\mathfrak{T}^*$. Cela est en tout cas exact pour $\mathfrak{O}^*$ et $\mathfrak{J}^*$.

§ 6. Les groupes polyédriques binaires

Ces groupes peuvent être représentés comme groupes de translations de Clifford (rotations sans points fixes d'une nature particulière) de la sphère à trois dimensions S^3 (voir 10.5).

En vertu du théorème 2.5, ils sont du premier ou du deuxième type. C'est ce que je me propose de vérifier directement ici, en précisant lesquels appartiennent au premier type et lesquels au deuxième.

La dénomination „groupes binaires" vient de ce que l'on peut les engendrer par des substitutions binaires (unitaires). Ils renferment un sous-groupe invariant d'ordre 2, le groupe-quotient correspondant étant un groupe polyédrique ordinaire[20]).

6.1. Les *groupes diédriques binaires* D_m^* (ordre $4m$) sont définis par:

$$A^m = B^2 = C^2 = P \qquad CBA = E \qquad P^2 = E\ .$$

Sous cette forme, on voit que le groupe-quotient par le sous-groupe invariant $\{P\}$, d'ordre 2, est le groupe diédrique ordinaire $Dm : A^m = B^2 = C^2 = E\ \ CBA = E$, d'ordre $2m$. A et B suffisent à engendrer le groupe, car $C^{-1} = BA$:

$$A^{2m} = E \qquad B^2 = A^m \qquad BAB^{-1} = A^{-1} \tag{1}$$

où la dernière relation s'obtient en transformant $C^2 = A^m$.

---

[20]) J'utilise ici les notations de Threlfall et Seifert [2] p. 26.

Supposons tout d'abord m pair: $m = 2^{\alpha-2}n$, n impair, $\alpha \geqslant 3$. Les relations deviennent :

$$A^{2^{\alpha-1}n} = E \qquad B^2 = A^{2^{\alpha-2}n} \qquad BAB^{-1} = A^{-1} \ . \tag{2}$$

C'est un groupe du deuxième type d'ordre $4m = 2^\alpha n$ appartenant à la classe (α) comme le montrent les relations (6) de (5.7). Son groupe des commutateurs est $\{A^2\}$ cyclique d'ordre $2^{\alpha-2}n = m$. Pour $n = 1$, c'est-à-dire lorsque m est une puissance de 2, c'est le groupe quaternionique $\mathfrak{Q}\,2^\alpha$. Ainsi $\mathfrak{Q}\,8$, par exemple, n'est autre que le groupe rectangle binaire D_2^*.

Supposons maintenant m impair. Opérons dans (1) la substitution d'éléments générateurs $A^2 = X$, $BA = Y$; on obtient :

$$X^m = E \qquad Y^4 = E \qquad YXY^{-1} = X^{-1} \ . \tag{3}$$

On s'assure de l'isomorphisme en exprimant A et B au moyen de X et Y : $A = X^{\frac{1-m}{2}} Y^2$, $B = Y^{-1} X^{\frac{m-1}{2}}$, et en montrant que les relations (3) entraînent (1), ou plus simplement encore en remarquant que (3) représente un groupe du premier type d'ordre $4m$ d'après les relations (2) de 4.5. Le groupe des commutateurs est $\{X\}$, cyclique, d'ordre m impair.

Les groupes D_m^* étant rangés suivant les valeurs croissantes de m (2, 3,...), *sont alternativement du deuxième et du premier type.*

Remarque: Les groupes diédriques ordinaires Dm, qui peuvent être définis par : $A^m = E$ $B^2 = E$ $BAB^{-1} = A^{-1}$ sont du premier type pour m impair. Ils n'admettent aucune représentation sans points fixes, car ils contiennent plus d'un élément d'ordre 2 (11.2). Pour m pair, ils ne sont ni du premier type, ni du deuxième type, leurs 2-sous-groupes de Sylow étant diédriques.

6.2. Le *groupe binaire du tétraèdre* $\mathfrak{T}^*$ (ordre 24) est défini par :

$$A^3 = B^2 = C^3 = P \qquad CBA = E \qquad P^2 = E \ .$$

On peut éliminer B en résolvant $CBA = E$: $B = C^{-1}A^{-1}$, $B^{-1} = AC$ $B^{-2} = B^2 = ACAC = A^3 = C^3$. Les relations deviennent :

$$A^6 = E \qquad C^3 = A^3 \qquad CAC^{-1} = A^{-1}C \ . \tag{4}$$

En posant : $AC = X$, $CA = Y$, $A^2 = Z$, on trouve :

$$\left.\begin{array}{lll} X^4 = E & Y^2 = X^2 & YXY^{-1} = X^{-1} \\ Z^3 = E & ZXZ^{-1} = Y & ZYZ^{-1} = YX \end{array}\right\} \qquad (5)$$

et réciproquement, $Z^2X^2 = A$ et $ZX^3 = C$ conduisent aux anciennes relations. Or (5) est le *groupe du deuxième type, métabélien de rang 3*, trouvé en 5.8.

6.3. Le *groupe binaire de l'octaèdre* $\mathfrak{O}^*$ (ordre 48) est défini par :

$$A^4 = B^2 = C^3 = P \qquad CBA = E \qquad P^2 = E \ .$$

On peut éliminer B et obtenir :

$$A^8 = E \qquad C^3 = A^4 \qquad CAC^{-1} = A^{-1}C \ . \qquad (6)$$

Ce groupe est isomorphe au *groupe du deuxième type, métabélien de rang 4*, construit en 5.9.

6.4. Le *groupe binaire de l'icosaèdre* $\mathfrak{J}^*$ (ordre 120) est défini par :

$$A^5 = B^2 = C^3 = P \qquad CBA = E \qquad P^2 = E \ .$$

On peut également éliminer B :

$$A^{10} = E \qquad C^3 = A^5 \qquad CAC^{-1} = A^{-1}C \ . \qquad (7)$$

Ce groupe, identique à son groupe des commutateurs, $\mathfrak{J}^{*\prime} = \mathfrak{J}^*$, n'est pas à portée de mes méthodes (parce que du *deuxième type, non résoluble*).

Il n'est pas identique au groupe symétrique $\mathfrak{S}_5$ d'ordre 120, qui possède un sous-groupe invariant d'ordre 60, le groupe simple $\mathfrak{A}_5$. Constatons cependant ce fait curieux : les deux groupes ont des séries de composition de même longueur et des groupes-quotient isomorphes à l'ordre près :

$$\mathfrak{J}^* \supset \mathfrak{Z}_2 \supset E \qquad \mathfrak{S}_5 \supset \mathfrak{A}_5 \supset E$$

les groupes-quotient étant respectivement : $\mathfrak{A}_5$, $\mathfrak{Z}_2$ et $\mathfrak{Z}_2$, $\mathfrak{A}_5$. Autre fait intéressant : les éléments de $\mathfrak{J}^*$ se répartissent en 9 classes d'éléments conjugués, alors que ceux de $\mathfrak{O}^*$ se répartissent en 8 classes et ceux de $\mathfrak{T}^*$ en 7.

Chapitre III

Conditions suffisantes pour l'existence de représentations sans points fixes. Théorèmes fondamentaux

§ 7. Représentations irréductibles. Groupes cycliques et quaternioniques

7.1. Les éléments d'un groupe abstrait $\mathfrak{G}$ fini, d'ordre g, se répartissant en N classes d'éléments conjugués, $\mathfrak{G}$ admet N représentations irréductibles, unitaires, non équivalentes, de degrés d_i $(i = 1, 2, \ldots, N)$ diviseurs de g, caractérisées par leurs caractères χ_i[21]. Je désigne par C_i les classes et par c_i le nombre des éléments qu'elles renferment : $\sum_{i=1}^{N} c_i = g$.

Le *critère d'irréductibilité* d'une représentation de caractère χ est $\sum \chi(S)\,\overline{\chi}(S) = g$, la somme étant étendue à tous les éléments $S \in \mathfrak{G}$.

Les caractères des N représentations irréductibles non équivalentes vérifient les *relations d'orthogonalité :*

$$\sum_S \chi_i(S)\,\overline{\chi}_j(S) = \left\{ \begin{array}{lll} 0 & \text{si} & i \neq j \\ g & \text{si} & i = j \end{array} \right\} \tag{1}$$

$$\sum_{j=1}^{N} \chi_j(S)\,\overline{\chi}_j(T) = \left\{ \begin{array}{lll} 0 & \text{si} & S \text{ et } T \text{ non conjugués} \\ \dfrac{g}{c_i} & \text{si} & S \text{ et } T \text{ conjugués dans } \mathfrak{G} \end{array} \right\} \tag{2}$$

S et T appartenant à la classe C_i, $\dfrac{g}{c_i}$ est l'ordre du normalisateur d'un élément de cette classe. En particulier, si $S = T = E$, l'élément unité de $\mathfrak{G}$, les deuxièmes relations d'orthogonalité donnent :

$$\sum_{i=1}^{N} d_i^2 = g \ , \tag{3}$$

la somme des carrés des degrés des représentations irréductibles est égale à l'ordre du groupe.

La condition nécessaire et suffisante pour l'*équivalence de deux représentations linéaires*, réductibles ou non, d'un même groupe $\mathfrak{G}$, est l'*identité des caractères*.

---

[21]) Voir note 4.

7.2. Les représentations irréductibles, unitaires, de $\mathfrak{G}$ sont de trois sortes : 1. équivalentes à une représentation réelle ; 2. équivalentes à l'imaginaire conjuguée, mais à aucune représentation réelle ; 3. non équivalentes à l'imaginaire conjuguée[22]).

Cette classification peut s'opérer d'après les valeurs des caractères par la relation

$$\sum_S \chi(S^2) = cg \tag{4}$$

où c vaut $+1$, -1, 0 suivant que la représentation envisagée appartient à la première, à la deuxième ou à la troisième catégorie.

Une représentation quelconque de $\mathfrak{G}$ est somme de représentations irréductibles. Pour qu'elle soit équivalente à une représentation réelle, il faut et il suffit que les représentations de la deuxième catégorie qu'elle peut contenir apparaissent un nombre pair de fois, celles de la troisième catégorie aussi souvent que l'imaginaire conjuguée.

A ce propos, je rappelle la correspondance qu'on peut établir entre $\mathfrak{U}^k(n)$ et $\mathfrak{U}^r(2n)$: la forme d'Hermite, à n variables, $z_1\bar{z}_1 + \cdots + z_n\bar{z}_n$ où $z_s = x_s + iy_s$ (x_s, y_s réels), peut s'écrire : $x_1^2 + y_1^2 + \cdots + x_n^2 + y_n^2$, forme quadratique à $2n$ variables. De plus, $\mathfrak{U}$ désignant une matrice unitaire $U + iV$ (U et V matrices réelles), de degré n, on a la relation

$$T\begin{pmatrix} \mathfrak{U} & 0 \\ 0 & \bar{\mathfrak{U}} \end{pmatrix} T^{-1} = \begin{pmatrix} U & -V \\ V & U \end{pmatrix} \quad \text{où} \quad T = \frac{1}{\sqrt{2}}\begin{pmatrix} E & -iE \\ -iE & E \end{pmatrix} \tag{5}$$

T étant unitaire et la matrice du second membre orthogonale de degré $2n$.

Cette loi de composition sera utilisée pour les représentations irréductibles des deuxième et troisième catégories. Elle permet d'obtenir les représentations orthogonales (réelles)[23]), irréductibles dans $\mathfrak{U}^r(n)$. Toute représentation orthogonale de $\mathfrak{G}$ est une somme de représentations irréductibles unitaires qui peuvent appartenir aux trois catégories, à condition que celles de la deuxième et de la troisième soient amplifiées au sens que je viens d'indiquer.

7.3. Le cas d'un *groupe cyclique*, engendré par A, d'ordre g, est particulièrement simple.

Les $N = g$ représentations irréductibles sont toutes de degré 1 et s'obtiennent en faisant correspondre à A la matrice (ε^k) $k = 1, 2, \ldots, g$ où ε est une racine primitive $g^{\text{ième}}$ de l'unité (2.4).

---

[22]) Pour tout le 7.2 voir [8].

[23]) Voir note 5.

Celles correspondant à k premier à g sont *sans points fixes ;* leur nombre est $\varphi(g)$ (définition en 3.1). Ce sont les seules qui soient *fidèles ;* de plus elles appartiennent à la troisième catégorie (7.2), c'est-à-dire qu'elles ne sont *pas équivalentes à l'imaginaire conjuguée,* sauf dans le cas $g = 2$.

Les représentations orthogonales, sans points fixes, irréductibles dans le domaine réel, non équivalentes, d'un groupe cyclique d'ordre g ($\neq 2$) sont de degré 2 et en nombre égal à $\frac{1}{2}\varphi(g)$. Il n'y en a qu'une, formée de $+1$ et de -1, de degré 1, pour le groupe cyclique d'ordre 2.

Le groupe cyclique d'ordre g ($\neq 2$) admet des représentations orthogonales, sans points fixes, pour tous les degrés $2k$ et pour ceux-là seuls. Le nombre des représentations non équivalentes pour le degré $2k$ est égal au nombre des combinaisons k à k avec répétitions, des $\frac{1}{2}\varphi(g)$ représentations irréductibles de degré 2. Le groupe d'ordre 2, par contre, admet pour tout degré l'unique représentation orthogonale sans points fixes formée de E et $-E$.

Je retrouve les théorèmes connus :

Toute sphère de dimension impaire admet des groupes cycliques de rotations sans points fixes, de degrés quelconques.

Une sphère de dimension paire n'admet pas d'autres groupes cycliques de rotations sans points fixes que $\mathfrak{Z}2$ et le groupe se réduisant à l'identité.

Comme formes spatiales sphériques (11.1), j'obtiens ici : l'espace sphérique S^n et l'espace elliptique P^n (non orientable) pour les dimensions n paires ; je montre plus loin que ce sont les seules. Pour les dimensions impaires, des formes orientables : l'espace sphérique, l'espace elliptique, une infinité de formes sphériques à groupe fondamental cyclique (les espaces lenticulaires pour la dimension trois). Ces dernières sont elliptiques ou non, suivant qu'elles admettent ou non l'espace elliptique comme espace de recouvrement, c'est-à-dire suivant que g est pair ou impair[24]).

7.4. Pour les *groupes quaternioniques* $\mathfrak{Q}2^\alpha$ ($\alpha \geqslant 3$), j'ai donné en 3.2 la répartition en classes d'éléments conjugués : $N = 2^{\alpha-2} + 3$.

C'est le nombre des représentations irréductibles unitaires. L'ordre du groupe rendu abélien, $\mathfrak{Q}/\mathfrak{Q}'$, étant 4, il existe quatre représentations irréductibles de degré 1 ($A \to (\pm 1)$, $B \to (\pm 1)$). La formule (3) de 7.1 prouve que les $2^{\alpha-2} - 1$ autres sont de degré 2 : $4 \cdot 1 + (2^{\alpha-2} - 1) \cdot 4 = 2^\alpha = g$. On les obtient en posant :

$$A = \begin{pmatrix} \lambda^r & 0 \\ 0 & \lambda^{-r} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

[24]) [1] p. 321.

où λ est une racine primitive d'ordre $2^{\alpha-1}$ de l'unité et $r = 1, 2, \ldots, 2^{\alpha-2} - 1$. Les autres valeurs de r conduisent à des représentations équivalentes (même caractère) sauf $r = 2^{\alpha-2}$ et $r = 2^{\alpha-1}$ qui donnent des représentations réductibles.

Remarques : 1. Les caractères sont tous réels ; c'est une conséquence du fait que S et S^{-1} sont dans la même classe quel que soit $S \in \mathfrak{Q}$, car $\chi(S^{-1}) = \bar{\chi}(S)$, ici $\chi(S^{-1}) = \chi(S)$ d'où $\chi(S) = \bar{\chi}(S)$ réel.

2. Les caractères de B (et BA) sont nuls dans toutes les représentations irréductibles de degré 2, en accord avec le fait que la somme $\chi_j(B)\,\bar{\chi}_j(B)$ étendue aux caractères de degré 1 donne déjà 4, ordre du normalisateur de B (formules (2) en 7.1).

Les représentations irréductibles sans points fixes sont à rechercher parmi les représentations fidèles. Or celles-ci s'obtiennent en donnant à r les $\frac{1}{2}\varphi(2^{\alpha-1}) = 2^{\alpha-3}$ valeurs $(1, 3, \ldots, 2^{\alpha-2} - 1)$ premières à $2^{\alpha-1}$ et inférieures à $2^{\alpha-2}$.

Les $2^{\alpha-3}$ représentations irréductibles, unitaires, fidèles, de degré 2, sont toutes sans points fixes.

Démonstration : Les valeurs propres de A sont des racines primitives d'ordre $2^{\alpha-1}$ de l'unité. La première puissance de A qui admet une valeur propre $+1$ est $A^{2^{\alpha-1}}$ qui vaut E. Celles de B sont i et $-i$ (équation caractéristique $\lambda^2 + 1 = 0$) et sont les mêmes pour tous les éléments de sa classe. Celles de BA enfin :

$$BA = \begin{pmatrix} 0 & \lambda^{-r} \\ -\lambda^r & 0 \end{pmatrix}$$

d'équation caractéristique $\lambda^2 + 1 = 0$, sont i et $-i$ comme pour tous les éléments de sa classe.

Ces $2^{\alpha-3}\left(= \dfrac{\varphi(g)}{4}\right)$ représentations irréductibles, unitaires, sans points fixes, appartiennent à la deuxième catégorie (7.2) c'est-à-dire qu'elles sont *équivalentes à l'imaginaire conjuguée* (évident puisque le caractère est réel) *mais à aucune représentation réelle.*

La formule (4) de 7.2 donne, en effet, tous calculs effectués :

$$\sum_S \chi(S^2) = -2^\alpha = -g\ .$$

Les représentations orthogonales, sans points fixes, irréductibles dans $\mathfrak{U}^r(n)$, non équivalentes, s'obtiennent par composition à partir des $2^{\alpha-3}$ représentations irréductibles, unitaires, sans points fixes, de degré 2. Elles ont le degré 4 et sont en nombre égal à $2^{\alpha-3}$.

Le groupe quaternionique $\mathfrak{Q}2^\alpha$, *d'ordre* 2^α, *admet des représentations orthogonales, sans points fixes* (en général réductibles, même dans le domaine réel), *pour tous les degrés* $4k$ *et pour ceux-là seuls.* Le nombre des représentations non équivalentes pour ce degré est égal au nombre de combinaisons k à k, avec répétitions, des $2^{\alpha-3}$ représentations orthogonales irréductibles.

Or tout groupe $\mathfrak{G}$ du deuxième type contient des 2-sous-groupes de Sylow quaternioniques. Soit $\mathfrak{Q}2^\alpha$ l'un d'eux ; toute représentation sans points fixes de $\mathfrak{G}$ induit une représentation sans points fixes de $\mathfrak{Q}2^\alpha$. Toute représentation orthogonale, sans points fixes, d'un groupe du deuxième type est de degré $4k$. Envisagée comme groupe de rotations, cette représentation transforme en elle-même la sphère S^{4k-1}, à $4k-1$ ou $4k'+3$ dimensions ; d'où le

Théorème I : *Seules les sphères* S^{4k+3}, *dont le nombre de dimensions est congru à 3* (*mod.* 4), *peuvent admettre des groupes de rotations sans points fixes du deuxième type.*

Les groupes quaternioniques $\mathfrak{Q}2^\alpha$ sont du deuxième type ; ils apparaissent effectivement comme groupes de rotations sans points fixes de toutes les sphères $S^3, S^7, S^{11}, \ldots$ Ils sont *relatifs à la dimension* 3 ; j'entends par là, que c'est la plus petite dimension pour laquelle ils apparaissent comme groupes de rotations sans points fixes.

Les formes sphériques (elliptiques) correspondantes sont, pour la dimension trois, des espaces prismatiques particuliers ($\mathfrak{Q}2^\alpha$ est en effet le groupe diédrique binaire $D^*_{2^{\alpha-1}}$ (6.1)).

D'autres exemples sont donnés plus loin (9.3).

§ 8. Groupes du premier type, non cycliques

Un groupe $\mathfrak{G}$ du premier type (sous-groupes de Sylow cycliques), d'ordre g, est défini par :

$$A^m = E \qquad B^n = E \qquad BAB^{-1} = A^r \tag{1}$$

où :

a) $m > 0,\ mn = g$ b) $\big((r-1)n, m\big) = 1$ c) $r^n \equiv 1\,(m)$.

Son groupe des commutateurs $\{A\}$ est cyclique d'ordre m impair (4.5 formules (2) et 4.6).

8.1. Soit tout d'abord m *premier* (impair). Nous pouvons choisir pour r l'un quelconque des $m-2$ restes premiers à m autres que 1

($\varphi(m) = \lambda(m) = m - 1$; pour $r = 1$, nous aurions le groupe cyclique d'ordre mn, déjà traité) ; $r - 1$ est, en effet, premier à m pour toutes ces valeurs.

Supposons, dans un premier cas, que la valeur choisie pour r *appartienne à l'exposant* $m - 1$; r engendre le groupe multiplicatif $\mathfrak{G}m$ (3.1) cyclique d'ordre $\varphi(m) = m - 1$. Il y a exactement $\varphi(m - 1)$ valeurs de r vérifiant cette condition, correspondant dans les cas précisés à la fin de 4.6 à des groupes isomorphes.

La condition c) $r^n \equiv 1(m)$ entraîne n multiple de $m - 1$: $n = (m - 1)n'$, n' premier à m.

La relation $BAB^{-1} = A^r$ donne par itération $B^\nu AB^{-\nu} = A^{r^\nu}$, si bien que B^{m-1} est permutable à A ; étant aussi permutable à B, cet élément est dans le centre. Le groupe admet un centre $\{B^{m-1}\}$ d'ordre n', $\neq E$ si $n' \neq 1$. De plus, r engendrant $\mathfrak{G}m$, l'élément A et ses puissances forment une seule classe d'éléments conjugués. Mon but étant la recherche des représentations irréductibles sans points fixes, je précise tout d'abord cette répartition en classes. Comme $BAB^{-1} = A^r$, $BA^{r^{m-2}}B^{-1} = A^{r^{m-1}} = A$ et $ABA^{-1} = BA^{r^{m-2}-1}$, on a $A^tBA^{-t} = BA^{t(r^{m-2}-1)}$; $r^{m-2} - 1$ étant premier à m, la classe de B renferme tous les éléments : B, BA, $BA^2, \ldots, BA^{m-1}$. Le résultat est analogue pour tous les éléments B^ν qui n'appartiennent pas au centre, d'où la répartition suivante en classes d'éléments conjugués, où les éléments d'une même classe sont dans la même colonne :

$$\begin{array}{lllll} E & A & B & B^2 & \cdots & B^{m-2} \\ & A^2 & BA & B^2A & \cdots & B^{m-2}A \\ & \vdots & \vdots & \vdots & & \vdots \\ & A^{m-1} & BA^{m-2} & B^2A^{m-2} & \cdots & B^{m-2}A^{m-2} \\ & & BA^{m-1} & B^2A^{m-1} & \cdots & B^{m-2}A^{m-1} \end{array} \qquad (2)$$

La répartition complète est formée de n' tableaux de structure identique à (2) (elle se réduit d'ailleurs à (2) si $n' = 1$) ; les $n' - 1$ autres tableaux s'obtiennent en multipliant (2) par les $n' - 1$ éléments $\neq E$ du centre $\{B^{m-1}\}$.

Voici ce que je me propose d'établir tout d'abord : quel que soit n', les représentations irréductibles de $\mathfrak{G}$ sont soit de degré 1, soit de degré $m - 1$. Je montre alors que, moyennant une restriction sur n', il existe des représentations irréductibles sans points fixes, toutes de degré $m - 1$, non équivalentes à des représentations réelles. Je procède par étapes :

a) L'ordre du groupe $\mathfrak{G}$ est $g = mn = m(m-1)n'$. Les classes d'éléments conjugués sont en nombre $N = mn'$. C'est le nombre des représentations irréductibles. Le groupe rendu abélien, $\mathfrak{G}/\mathfrak{G}' = \mathfrak{G}/\{A\}$ est cyclique d'ordre $n = (m-1)n'$; c'est le *nombre des représentations de degré 1*, qui s'obtiennent par la correspondance $A \to (1)$, $B \to (\beta^k)$ $k = 1, 2, \ldots, n$, où β désigne une racine primitive $n^{\text{ième}}$ de l'unité. Il reste n' représentations de degrés inconnus, supérieurs à 1.

b) Le caractère de B dans toute représentation de degré supérieur à 1 est nul. C'est une conséquence des relations d'orthogonalité (2) des caractères, rappelées en 7.1. La somme des $\chi_j(B)\,\overline{\chi}_j(B)$, étendue aux caractères de degré 1, donne déjà n, ordre du normalisateur de B.

Il en est de même pour toute puissance de B, non contenue dans le centre.

Un élément du centre est représenté (dans toute représentation irréductible) par αE[25]). C'est une conséquence immédiate du „lemme de Schur". Ici, B^{m-1} est représenté par αE, $B^{k(m-1)}$ par $\alpha^k E$, où α désigne une racine $n'^{\text{ième}}$ de l'unité (primitive ou non).

$\mathfrak{G}$ n'étant pas abélien, les matrices d'une représentation linéaire fidèle de $\mathfrak{G}$ ne peuvent avoir toutes la forme diagonale. Mais deux matrices correspondant à des éléments permutables de $\mathfrak{G}$ peuvent être mises simultanément sous forme diagonale ; les valeurs propres du produit sont alors le produit des valeurs propres. Ainsi les valeurs propres de $B^{m-1}A$ sont le produit par α de celles de A ; plus généralement, les valeurs propres de $B^{k(m-1)}A$ sont celles de A multipliées par α^k. Soit χ le caractère d'une représentation irréductible de degré $x > 1$; le *système des caractères* est :

$$\chi(E) = x, \chi(A), 0, \ldots, 0 \quad \text{pour le premier tableau,}$$
$$\chi(B^{m-1}) = \alpha x, \chi(B^{m-1}A) = \alpha\chi(A),\ 0, \ldots, 0 \quad \text{pour le deuxième,}$$
$$\chi(B^{k(m-1)}) = \alpha^k x, \chi(B^{k(m-1)}A) = \alpha^k\chi(A),\ 0, \ldots, 0 \quad \text{pour le } (k+1)^{\text{ième}}.$$

c) Utilisons alors le critère d'irréductibilité d'une représentation (7.1) : $\sum_S \chi(S)\,\overline{\chi}(S) = g$.

$$n'x^2 + n'(m-1)\,\chi(A)\,\overline{\chi}(A) = g = m(m-1)\,n'$$

ou

$$x^2 + (m-1)\,\chi(A)\,\overline{\chi}(A) = m(m-1)\ .$$

Cette égalité prouve que $\chi(A)\,\overline{\chi}(A)$ est rationnel. Or, $\chi(A)$ est un entier

[25]) [5] p. 266, [4] Satz 151.

algébrique (somme de racines de l'unité) ; $\chi(A)\,\overline{\chi}(A)$ est un entier rationnel, x est divisible par $m-1$. *Les n' représentations irréductibles de degré >1 sont toutes de degré $m-1$* ; c'est la seule valeur qui convienne, la somme des carrés des degrés des représentations irréductibles devant être égale à g (7.1) :

$$(m-1)\,n' \times 1 + n' \times (m-1)^2 = m(m-1)\,n' = g\ .$$

De plus, $\chi(A)\,\overline{\chi}(A) = 1$ dans toutes les représentations irréductibles (même pour le degré 1).

d) A et ses puissances $\neq E$ forment une seule classe d'éléments conjugués, les matrices correspondantes ont les mêmes valeurs propres. Dans toute représentation irréductible de degré $m-1$, ce sont λ, $\lambda^2, \ldots, \lambda^{m-1}$ où λ désigne une racine de l'unité d'ordre m. Elles sont toutes primitives, puisque m est premier. Le cas où elles seraient toutes égales à l'unité ne peut se produire à cause de $\chi(A)\,\overline{\chi}(A) = 1$. Je trouve ici $\chi(A) = -1$, en accord avec cette relation. *A, ni aucune de ses puissances $\neq E$, n'admet la valeur propre $+1$.* Je suis désormais en mesure de donner le *système complet des caractères* ; pour les n' représentations irréductibles de degré $m-1$ on obtient :

$$\begin{array}{rl} m-1,\ -1,\ 0, \ldots, 0 & \text{pour le premier tableau} \\ \alpha^k(m-1),\ -\alpha^k,\ 0, \ldots, 0 & \text{pour le } (k+1)^{\text{ième}} \end{array}$$

où α est à remplacer successivement par les n' racines $n'^{\text{ièmes}}$ de l'unité.

e) Je cherche alors à déterminer les valeurs propres de B dans une représentation irréductible de degré $m-1$.

Soient $\mu_1, \mu_2, \ldots, \mu_{m-1}$ ces valeurs propres, racines de l'unité d'ordre $n = (m-1)n'$. Comme celles de l'élément B^{m-1} du centre sont toutes égales, $\mu_1^{m-1} = \mu_2^{m-1} = \cdots = \mu_{m-1}^{m-1} = \mu^{m-1}$ et l'on peut poser : $\mu_i = \mu\,\varepsilon_i$ où $\varepsilon_i^{m-1} = 1$. Le caractère de B^k est nul pour $k = 1, 2, \ldots, m-2$: $\sum_{i=1}^{m-1} \mu^k\,\varepsilon_i^k = 0$. D'où $\sum_{i=1}^{m-1} \varepsilon_i^k = 0$ pour $k = 1, 2, \ldots, m-2$ et $\sum_{i=1}^{m-1} \varepsilon_i^{m-1} = m-1$. Les formules de Newton prouvent que les ε_i sont les $m-1$ racines de $\varepsilon^{m-1} = 1$.

Les valeurs propres de B, dans toute représentation irréductible de degré $m-1$, occupent sur le cercle unité les sommets d'un polygone régulier de $m-1$ côtés.

Soit μ une racine primitive de l'unité, d'ordre $n = (m-1)\,n'$. Les valeurs propres de B dans les n' représentations irréductibles de degré $m-1$ sont : $\mu^k, \mu^k\varepsilon, \ldots, \mu^k\varepsilon^{m-2}$, $k = 1, 2, \ldots, n'$, ε racine primitive $(m-1)^{\text{ième}}$ de l'unité. Choisissons en particulier pour ε la valeur $\mu^{n'}$, les valeurs propres de B sont : $\mu^k, \mu^{k+n'}, \mu^{k+2n'}, \ldots, \mu^{k+(m-2)n'}$.

f) A quelle condition les valeurs propres de B sont-elles toutes racines primitives d'ordre n de l'unité ?

Les $m-1$ entiers :

$$k, k+n', k+2n', \ldots, k+(m-2)\,n' \tag{3}$$

doivent être premiers à $n = (m-1)\,n'$.

La *condition nécessaire et suffisante*, pour qu'un choix de k remplissant cette exigence soit possible, est que *n' soit multiple des facteurs premiers de* $m-1$; si $m-1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, n' doit égaler $p_1 p_2 \ldots p_k n''$ (n'' restant premier à m, pour satisfaire la condition $(n, m) = 1$).

La condition est nécessaire : k peut toujours être choisi premier à $n = (m-1)\,n'$: il suffit de prendre au besoin $k = 1$. Soit p_i un des diviseurs premiers de $m-1$ et supposons qu'il ne divise pas n' : $(n', p_i) = 1$. Les p_i premiers entiers de la suite (3) : $k, k+n', \ldots, k+(p_i-1)\,n'$ sont deux à deux incongrus (mod. p_i) : car $k + sn' \equiv k + tn'(p_i)$ entraînerait $(s-t)\,n' \equiv 0\,(p_i)$ et $s \equiv t\,(p_i)$ puisque $(n', p_i) = 1$. L'un d'eux est congru à $0\,(p_i)$ et n'est pas premier à n, contrairement à l'hypothèse. Donc $p_i \,/\, n'$.

La condition est suffisante : soit $n' = p_1 p_2 \ldots p_k n''$ et choisissons k premier à n' : du même coup, k est premier à $m-1$. Les nombres de la suite (3) sont tous congrus à k (mod. n'), donc premiers à $n = (m-1)n'$.

On peut choisir pour k les $\varphi(n')$ valeurs inférieures et premières à n'. Pour les $\varphi(n')$ représentations irréductibles correspondantes, de degré $m-1$, B ni aucune de ses puissances $\neq E$ n'admet la valeur propre $+1$. Il en est de même pour tous les éléments d'une classe renfermant une puissance de B (qui ont en effet les mêmes valeurs propres). Il ne reste à considérer, d'après les tableaux (2), que les éléments tels que $B^{k(m-1)}A$. Or, d'après (b), les valeurs propres d'un tel élément sont celles de A multipliées par α^k. Toute valeur propre de A est racine $m^{\text{ième}}$ primitive de l'unité ; α^k est racine $n'^{\text{ième}}$ (primitive ou non) ; $(m, n') = 1$ rend impossible l'apparition d'une valeur propre $+1$.

La condition nécessaire et suffisante d'existence de représentations sans points fixes d'un groupe $\mathfrak{G}$ du type considéré est que n' soit multiple des facteurs premiers de $m-1$.

$\mathfrak{G}$ admet n' représentations irréductibles de degré $m-1$, parmi lesquelles $\varphi(n')$ sont alors sans points fixes.

Remarques: 1. Le centre de $\mathfrak{G}$ est alors $\neq E$.

2. Le nombre $\varphi(n')$ des représentations irréductibles sans points fixes est égal à $\dfrac{\varphi(g)}{(m-1)^2}$. Car $g = m(m-1)n'$; $(m,(m-1)\,n') = 1$ entraîne $\varphi(g) = \varphi(m)\,\varphi[(m-1)\,n']$; $\varphi(m) = m-1$ et $\varphi[(m-1)\,n'] = (m-1)\,\varphi(n')$ à cause de n' multiple des facteurs premiers de $m-1$; $\varphi(g) = (m-1)^2\,\varphi(n')$, d'où l'égalité en question.

3. Toutes les représentations irréductibles fidèles de $\mathfrak{G}$ sont sans points fixes; ce sont justement les $\varphi(n')$ représentations irréductibles sans points fixes trouvées ci-dessus.

g) A quelle catégorie appartiennent les $\varphi(n')$ représentations irréductibles sans points fixes, de degré $m-1$? Les caractères de ces $\varphi(n')$ représentations s'obtiennent en donnant à α, à la fin de (d), les $\varphi(n')$ valeurs, racines $n'^{\text{ièmes}}$ primitives de l'unité. J'applique la formule (4) de 7.2; on trouve:

$$\sum_S \chi(S^2) = m(m-1)\,(\alpha + \alpha^3 + \alpha^5 + \cdots + \alpha^{2n'-1})\ .$$

Deux cas sont à distinguer suivant que n', qui est pair (multiple des facteurs premiers de $m-1$, où m est premier), est supérieur ou égal à 2:

$n' > 2$ entraîne $\sum_S \chi(S^2) = 0$ et les $\varphi(n')$ représentations irréductibles sans points fixes appartiennent à la troisième catégorie (non équivalentes à l'imaginaire conjuguée).

Pour $n' = 2$, α vaut -1, et $\sum_S \chi(S^2) = -m(m-1)\,2 = -g$; l'unique représentation sans points fixes de degré $m-1$ appartient à la deuxième catégorie, c'est-à-dire qu'elle est équivalente à l'imaginaire conjuguée, mais à aucune représentation réelle. Dans ce cas, $m-1$ ne doit admettre que le facteur premier 2: $m-1 = 2^s$, $m = 2^s + 1$ est un nombre premier de Fermat (3, 5, 17,...).

Les représentations orthogonales, sans points fixes, irréductibles dans $\mathfrak{U}^r(n)$, *sont dans les deux cas de degré* $2(m-1)$ *et en nombre (non équivalentes) égal à* $\frac{1}{2}\varphi(n')$ *si* $n' > 2$ *et* 1 *si* $n' = 2$.

8.2. Passons au cas, où m étant toujours *premier*, l'*ordre de* r dans $\mathfrak{G}m$ est, non pas $m-1$, mais un *diviseur* d *de* $\varphi(m) = m-1$:

$$A^m = E \qquad B^n = E \qquad BAB^{-1} = A^r$$

comme r^d est la plus petite puissance de r congrue à 1 modulo m, $r^n \equiv 1$ (m) entraîne n multiple de d: $n = dn'$ (avec n' premier à m, en vertu de $(m, n) = 1$). $B^\nu A^\mu B^{-\nu} = A^{\mu r^\nu}$ montre que la classe de A^μ renferme les d éléments: $A^\mu, A^{\mu r}, \ldots, A^{\mu r^{d-1}}$, les exposants étant incongrus modulo m car les $r^\alpha - 1$ sont premiers à m pour $0 < \alpha < d$. Les puissances de A, $\neq E$, se répartissent en $\dfrac{m-1}{d}$ classes de d éléments. $A^\mu B^\nu A^{-\mu} = B^\nu A^{\mu(r^{d-\nu}-1)}$ montre, d'une part que B^d est dans le centre, d'autre part que la classe d'un élément B^ν n'appartenant pas au centre renferme les m éléments $B^\nu, B^\nu A, \ldots, B^\nu A^{m-1}$ (conséquence de $r^{d-\nu} - 1$ premier à m).

La répartition en classes d'éléments conjugués est formée de n' tableaux:

$$\begin{array}{cccccccc}
E & A & \ldots & A^\mu & B & B^2 & \ldots & B^{d-1} \\
 & A^r & \ldots & A^{\mu r} & BA & B^2A & \ldots & B^{d-1}A \\
 & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
 & \underbrace{A^{r^{d-1}} \quad \ldots \quad A^{\mu r^{d-1}}}_{\frac{m-1}{d}} & & & \vdots & \vdots & & \vdots \\
 & & & & BA^{m-1} & B^2A^{m-1} & \ldots & B^{d-1}A^{m-1}
\end{array} \tag{4}$$

les $n' - 1$ autres ont la même structure et s'obtiennent en multipliant les éléments de (4) par les $n' - 1$ éléments $\neq E$ du centre $\{B^d\}$.

Je me propose d'établir que les représentations irréductibles ont soit le degré 1, soit le degré d (quel que soit n'). La condition nécessaire et suffisante pour qu'il existe des représentations irréductibles sans points fixes est que n' soit multiple des facteurs premiers de d. Il existe alors

$$\frac{m-1}{d}\varphi(n') = \frac{\varphi(g)}{d^2}$$

représentations irréductibles sans points fixes, non équivalentes à des représentations réelles.

Je suis le même plan qu'en 8.1:

L'ordre de $\mathfrak{G}$ est $g = mn = mdn'$; les classes d'éléments conjugués sont en nombre $N = \left(\dfrac{m-1}{d} + d\right) n'$. $\mathfrak{G}/\mathfrak{G}'$ est cyclique d'ordre $n = dn'$; c'est le nombre des représentations irréductibles de degré 1. Il reste $\dfrac{m-1}{d} n'$ représentations de degrés inconnus, supérieurs à 1.

Soit χ le caractère d'une représentation de degré $x > 1$. Les raisonne-

ments de 8.1 b) s'appliquent ici et permettent d'affirmer que $\chi(B^\nu) = 0$ pour tout élément B^ν n'appartenant pas au centre $\{B^d\}$; de plus, $\chi(B^{kd}) = \alpha^k x$, $\chi(B^{kd}A^\mu) = \alpha^k \chi(A^\mu)$ où α désigne une racine $n'^{\text{ième}}$, primitive ou non, de l'unité.

Le critère d'irréductibilité de χ (7.1) permet d'écrire : $\sum_S \chi(S)\,\bar{\chi}(S) = g$

$$n'x^2 + n'd \sum \chi(A^\mu)\,\bar{\chi}(A^\mu) = g = m\,dn'$$

la somme étant étendue aux $\dfrac{m-1}{d}$ classes en lesquelles se répartissent les puissances de A autres que E. On en tire : $x^2 + d \sum \chi(A^\mu)\,\bar{\chi}(A^\mu) = md$ qui prouve que x est multiple de d (car $\sum \chi(A^\mu)\,\bar{\chi}(A^\mu)$ entier algébrique, rationnel, est entier rationnel). Comme $\sum_i d_i^2 = g$ (7.1) et que : $dn' \times 1 + \dfrac{m-1}{d} n' \times d^2 = m\,dn' = g$, j'obtiens le résultat : *les* $\dfrac{m-1}{d} n'$ *représentations irréductibles de degré* > 1 *ont toutes le degré* d.

Autre conséquence : $\sum \chi(A^\mu)\,\bar{\chi}(A^\mu) = m - d$. Les valeurs propres de A ne sauraient, dans une représentation irréductible de degré d, être toutes égales à l'unité (la somme prendrait en effet la valeur $(m-1)\,d$). Soit $\lambda \neq 1$ une valeur propre de A, racine $m^{\text{ième}}$ de l'unité (primitive puisque m premier). En se reportant au tableau (4), on voit que les d valeurs propres de A sont : $\lambda, \lambda^r, \ldots, \lambda^{r^{d-1}}$. Ce sont toutes des racines primitives : A, *ni aucune de ses puissances* $\neq E$, *n'admet la valeur propre* $+1$. On obtient $\dfrac{m-1}{d}$ caractères différents en remplaçant λ par λ^μ où μ est un représentant d'une classe de $\mathfrak{G}m$ suivant $\{r\}$; l'ordre de $\mathfrak{G}m/\{r\}$ est précisément $\dfrac{m-1}{d}$.

Quant aux valeurs propres de B, de ses puissances et des $B^{kd}A^\mu$, on les obtient par les mêmes raisonnements qu'en 8.1 e) et f).

Dans toute représentation irréductible de degré d, *les valeurs propres de* B *occupent sur le cercle unité les sommets d'un polygone régulier de* d *côtés.* Les n' caractères distincts obtenus ici, joints aux $\dfrac{m-1}{d}$ caractères relatifs à A, donnent les $\dfrac{m-1}{d} n'$ représentations irréductibles, non équivalentes, de degré d.

La condition nécessaire et suffisante pour que les valeurs propres de B *puissent être toutes primitives, est que* n' *soit multiple des facteurs premiers de* d (même raisonnement qu'en 8.1 f)).

Dans ce cas, aucun élément $\neq E$ n'admet la valeur propre $+1$.

Moyennant cette condition, $\mathfrak{G}$ *admet* $\frac{m-1}{d}\varphi(n')$ *représentations irréductibles (unitaires), sans points fixes, toutes de degré* d. Ce nombre n'est autre que $\frac{\varphi(g)}{d^2}$ (voir fin de 8.1 f); c'est aussi celui des représentations irréductibles fidèles.

Pour trouver les représentations orthogonales, sans points fixes, irréductibles dans $\mathfrak{U}^r(n)$, il faut déterminer à quelle catégorie appartiennent ces $\frac{\varphi(g)}{d^2}$ représentations irréductibles, sans points fixes, unitaires. En appliquant le critère (4) de 7.2, on obtient :

$$\sum_S \chi(S^2) = \begin{cases} 0 & \text{si } d \text{ impair} \\ md(\alpha + \alpha^3 + \cdots + \alpha^{2n'-1}) & \text{si } d \text{ pair} \end{cases}$$

où α désigne une racine $n'^{\text{ième}}$ primitive de l'unité.

Quand d est pair, deux cas se présentent :

$$n' \text{ (qui doit être pair) supérieur à } 2 : \sum_S \chi(S^2) = 0$$

$$n' = 2 : \sum_S \chi(S^2) = -md2 = -g \ .$$

Dans ce dernier cas, d est une puissance de 2.

En définitive, $\mathfrak{G}$ admet $\frac{\varphi(g)}{d^2}$ représentations irréductibles, sans points fixes, non équivalentes à l'imaginaire conjuguée (troisième catégorie), ou équivalentes à l'imaginaire conjuguée, mais à aucune représentation réelle (deuxième catégorie). Les représentations orthogonales, sans points fixes, irréductibles dans $\mathfrak{U}^r(n)$, ont toutes le degré $2d$. Elles sont en nombre égal à $\frac{1}{2}\frac{\varphi(g)}{d^2}$ dans le premier cas, $\frac{\varphi(g)}{d^2} = \frac{m-1}{d}$ dans le second (où $n' = 2$).

8.3. Existe-t-il un entier m, tel que le groupe $\mathfrak{G}m$ (groupe multiplicatif des classes de congruences modulo m, premières au module) contienne un élément d'ordre d donné?

La réponse est affirmative ; il y a même une infinité d'entiers répondant à la question. Il me suffit ici, d'établir l'existence d'une infinité d'entiers m, premiers impairs, tels que $\varphi(m) = \lambda(m) = m - 1$ soit divisible par d. Or, tous les nombres premiers (en nombre infini, d'après Dirichlet) de la progression arithmétique $1 + kd$ répondent à la question. Soit m l'un

d'eux, r un reste modulo m d'ordre d dans $\mathfrak{G}m$. *Le groupe* $\mathfrak{G}$ *du premier type, d'ordre* $g = mdn'$ *défini par:*

$$A^m = E \qquad B^{dn'} = E \qquad BAB^{-1} = A^r$$

où n', *premier à* m, *est multiple des facteurs premiers de* d, *admet* $\frac{\varphi(g)}{d^2}$ *représentations irréductibles (unitaires), sans points fixes, de degré* d. Les représentations orthogonales correspondantes, irréductibles dans $\mathfrak{U}^r(n)$, sans points fixes, non équivalentes, sont de degré $2d$ et en nombre égal à : $\frac{1}{2}\frac{\varphi(g)}{d^2}$ si $n' \neq 2, \frac{\varphi(g)}{d^2} = \frac{m-1}{d}$ si $n' = 2$.

$\mathfrak{G}$ admet des représentations orthogonales, sans points fixes, pour tous les degrés $2kd$ et pour ceux-là seuls. Je dirai de $\mathfrak{G}$ qu'il est *relatif* à la dimension $2d - 1$; il n'apparaît pas comme groupe de rotations sans points fixes d'une sphère de dimension inférieure. Le nombre de représentations orthogonales, sans points fixes, non équivalentes, pour le degré $2kd$ est égal au nombre de combinaisons k à k, avec répétitions, des $\frac{1}{2}\frac{\varphi(g)}{d^2}\left(\frac{\varphi(g)}{d^2} \text{ si } n' = 2\right)$ représentations orthogonales irréductibles.

J'obtiens le :

Théorème II : *Toute sphère de dimension impaire (supérieure à 1) admet une infinité de groupes finis de rotations sans points fixes, non abéliens, ne se présentant pas pour des dimensions inférieures.*

Pour illustrer ce théorème, je vais construire quelques exemples. Mais auparavant, je fais une remarque qui sera précisée après l'étude complète des groupes du premier type (il s'agit ici de groupes du premier type dont le groupe des commutateurs est d'ordre premier). Si d est pair ($\equiv 0$ modulo 2), $\mathfrak{G}$ est relatif à la dimension $2d - 1 \equiv -1$ ou $+3$ modulo 4 ; quel que soit k, $2kd - 1 \equiv +3(4)$. $\mathfrak{G}$ n'apparaît que pour des sphères S^{2kd-1} dont la dimension est $\equiv 3(4)$. Si d est impair ($\equiv 1$ modulo 2), $\mathfrak{G}$ est relatif à la dimension $2d - 1 \equiv +1$ modulo 4 ; mais $2kd - 1 \equiv -1$ ou $+1$ suivant que k est pair ou impair. $\mathfrak{G}$, relatif à une sphère de dimension $\equiv 1(4)$, apparaît aussi pour des sphères dont la dimension est alternativement $\equiv 1$ ou $\equiv 3(4)$.

Voici le *groupe de rotations sans points fixes de* S^5, *non cyclique, d'ordre minimum.* $2d - 1 = 5$ donne $d = 3$; le plus petit nombre premier de la progression arithmétique $1 + 3k$ est $m = 7$; $\mathfrak{G}7 \cong \mathfrak{Z}6$, on peut

choisir pour r les valeurs 2 ou 4, seuls restes d'ordre 3 dans $\mathfrak{G}7$ (groupes isomorphes si n' impair, voir fin de 4.6) $n = 3n'$; n' doit être multiple de 3 pour qu'il existe des représentations sans points fixes : $n' = 3n''$ (n'' premier à 7), $n = 9n''$. Pour $n'' = 1$:

$$A^7 = E \qquad B^9 = E \qquad BAB^{-1} = A^2$$

Ce groupe est d'ordre 63 ; il admet $\frac{\varphi(g)}{d^2} = 4$ représentations irréductibles, unitaires, de degré 3, sans points fixes, non équivalentes à l'imaginaire conjuguée, données par :

$$A = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda^2 & 0 \\ 0 & 0 & \lambda^4 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha & 0 & 0 \end{pmatrix}$$

où λ désigne une racine primitive d'ordre 7 de l'unité (les diverses valeurs de λ ne conduisent qu'à deux caractères distincts), α une racine primitive d'ordre 3 (deux possibilités). Les représentations orthogonales irréductibles sont au nombre de deux (non équivalentes), de degré 6. S^5 admet deux groupes de rotations non équivalents de ce type. Ce groupe se présente également pour $S^{11}, S^{17}, \ldots, S^{6k-1}, \ldots$; pour S^{11}, par exemple, on obtient $\frac{2 \cdot 3}{1 \cdot 2} = 3$ représentations orthogonales non équivalentes.

Pour n'' quelconque (mais premier à 7), on obtient une infinité de groupes différents, d'ordres $63n''$, de rotations sans points fixes de S^5. Si n'' est pair, il faut considérer en outre les groupes : $A^7 = E$, $B^{9n''} = E$, $BAB^{-1} = A^4$, d'ordres $63n''$, non isomorphes aux précédents.

Comme *deuxième exemple*, je forme le groupe suivant :

$$A^{29} = E \qquad B^{49} = E \qquad BAB^{-1} = A^{16}$$

Son ordre est $g = 29 \cdot 49 = 1421$; on vérifie que $16^7 \equiv 1$ (modulo 29). Ce groupe admet $\frac{\varphi(g)}{d^2} = 24$ représentations irréductibles (unitaires), sans points fixes, de degré 7, non équivalentes à l'imaginaire conjuguée. *Il est relatif à la dimension* 13. C'est l'exemple annoncé en 5.4, d'un groupe du premier type d'ordre premier à 120, admettant en outre des représentations sans points fixes.

J'indique encore le *groupe du premier type (non cyclique) d'ordre le plus petit, admettant des représentations sans points fixes.* C'est :

$$A^3 = E \qquad B^4 = E \qquad BAB^{-1} = A^{-1}$$

d'ordre 12, isomorphe au groupe binaire D_3^* (6.1). Il est relatif à S^3 et admet $\frac{\varphi(g)}{d^2} = 1$ représentation irréductible, sans points fixes, de degré 2, à caractère réel, donc équivalente à l'imaginaire conjuguée mais à aucune représentation réelle. C'est avec $\mathfrak{Z}12$ le seul du premier type de cet ordre (il y a 5 groupes d'ordre 12).

Remarque : Les groupes de rotations sans points fixes relatifs à S^{2d-1} sont en nombre infini pour deux raisons : l'ordre du groupe des commutateurs $\mathfrak{G}'$ peut être choisi d'une infinité de façons et il en est de même pour l'ordre de $\mathfrak{G}/\mathfrak{G}'$.

8.4. Pour achever l'étude des groupes du premier type, il reste à considérer le cas où l'*ordre m de $\mathfrak{G}'$ est un nombre impair composé.*

Il faut choisir r de telle sorte que r, $r - 1$ et l'ordre d de r dans $\mathfrak{G}m$ (3.1) soient premiers à m (ce choix est possible quel que soit m impair ; on prendra au besoin $r = -1$ d'ordre 2). d est diviseur de $\lambda(m)$, l'exposant de $\mathfrak{G}m$. L'indice n du groupe des commutateurs doit être multiple de d, égal à dn' avec $(n', m) = 1$. Le groupe $\mathfrak{G}$ est défini par :

$$A^m = E \qquad B^{dn'} = E \qquad BAB^{-1} = A^r \ . \tag{5}$$

Son ordre est $g = m\,dn'$. La répartition de ses éléments en classes d'éléments conjugués est plus compliquée que pour m premier (8.1 et 8.2). Soit m_i un diviseur quelconque de m, r_i le reste de r modulo m_i, d_i l'ordre de r_i dans $\mathfrak{G}m_i$ (pour $m_i = 1$, je pose par convention $d_i = 1$). Je vais établir le théorème :

$\mathfrak{G}$ admet $\frac{\varphi(m_i)\,dn'}{d_i^2}$ représentations irréductibles (unitaires) de degré d_i, où A^{m_i} et ses puissances sont, seules parmi les puissances de A, représentées par la matrice E. Le nombre total des représentations irréductibles de $\mathfrak{G}$ est égal à : $\sum \frac{\varphi(m_i)\,dn'}{d_i^2}$, la somme étant étendue à tous les diviseurs m_i de m (y compris 1 et m). C'est le nombre N des classes d'éléments conjugués.

Ce théorème est vrai pour m premier, ainsi qu'il résulte de 8.2, les repré-

sentations irréductibles étant $\frac{m-1}{d} n'$ de degré d et dn' de degré 1, au total :

$$\frac{m-1}{d} n' + dn' \ .$$

Je procède par *induction complète sur le nombre des facteurs premiers de* m, en supposant le théorème établi pour tous les groupes du type considéré où l'ordre du groupe des commutateurs est un diviseur m_i $(<m)$ de m. Le sous-groupe $\{A^{m_i}\}$, d'ordre $\frac{m}{m_i}$ du groupe cyclique $\mathfrak{G}'$ d'ordre m est caractéristique, donc sous-groupe invariant de $\mathfrak{G}$. Le groupe-quotient $\mathfrak{G}/\{A^{m_i}\}$ est d'ordre $m_i\, dn'$ et donné par :

$$A^{m_i} = E \qquad B^{dn'} = E \qquad BAB^{-1} = A^{r_i} \ . \tag{6}$$

Ses représentations irréductibles induisent des représentations de $\mathfrak{G}$ également irréductibles $\left(\sum_S \chi(S)\,\overline{\chi}(S) = \frac{m}{m_i} m_i\, dn' = m\, dn' = g\right)$ dans lesquelles A^{m_i} et ses puissances sont représentés par la matrice E. J'applique l'hypothèse d'induction à $\mathfrak{G}/\{A^{m_i}\}$ $(m_i<m)$; le nombre des représentations irréductibles correspondantes de $\mathfrak{G}$ où aucune puissance de A avant la $m_i^{\text{ième}}$ n'est représentée par E est $\frac{\varphi(m_i)\, dn'}{d_i^2}$. La formule (3) de 7.1 donne alors :

$$\sum_{i=1}^{N} d_i^2 = \sum \varphi(m_i)\, dn' + \sum x_k^2 = g = m\, dn' \tag{7}$$

la première somme étant étendue à tous les diviseurs de m inférieurs à m, la deuxième aux représentations (en nombre et de degrés inconnus) où aucune puissance de A, $\neq E$, n'est représentée par la matrice unité. Or $\sum_{m_i/m} \varphi(m_i) = m$; la relation (7) s'écrit : $[m - \varphi(m)]\, dn' + \sum x_k^2 = m\, dn'$ ou $\sum x_k^2 = \varphi(m)\, dn'$.

On montre d'autre part comme en 8.2 que les $\varphi(m)$ puissances de A d'exposants premiers à m se répartissent en $\frac{\varphi(m)}{d}$ classes contenant chacune d éléments $(A, A^r, \ldots, A^{r^{d-1}}$ par exemple). Le nombre des représentations inconnues est supérieur ou égal à $\frac{\varphi(m)}{d} n'$, leurs degrés divisibles par d (avec λ, A admet $\lambda^r, \lambda^{r^2}, \ldots, \lambda^{r^{d-1}}$ comme valeurs propres). La seule possibilité en accord avec $\sum x_k^2 = \varphi(m)\, dn'$ est : $\frac{\varphi(m)}{d} n'$

représentations irréductibles de degré d. Comme ce nombre est égal à $\frac{\varphi(m)\, dn'}{d^2}$, le théorème est établi.

$\mathfrak{G}$ admet $\frac{\varphi(m)}{d}\, n'$ représentations irréductibles de degré d où aucune puissance de A, $\neq E$, n'admet la valeur propre $+1$. Les valeurs propres de A sont en effet racines $m^{\text{ièmes}}$ primitives de l'unité, sinon une puissance de A, $\neq E$, serait représentée par la matrice unité.

Je vais montrer que les puissances de B non contenues dans le centre $\{B^d\}$ ont le caractère nul dans toutes ces représentations.

Si $m = p^\alpha$ (p premier impair), $\mathfrak{G}m$ est cyclique d'ordre $\varphi(m) = p^{\alpha-1}(p-1)$. La condition r, $r-1$ et d premiers à m entraîne d diviseur de $p-1$. $\mathfrak{G}m$ a un seul sous-groupe d'ordre $p-1$ (cyclique donc isomorphe à $\mathfrak{G}p$) ; on l'obtient en élevant les éléments de $\mathfrak{G}m$ à la puissance $p^{\alpha-1}$ (d'où l'homomorphisme $\mathfrak{G}m \to \mathfrak{G}p$). Soit $m_i = p^\beta$ $0<\beta<\alpha$ un diviseur de m ; r_i, reste de r modulo m_i, est d'ordre d dans $\mathfrak{G}m_i$ (conséquence de l'homomorphisme $\mathfrak{G}m_i \to \mathfrak{G}p$). Un groupe $\mathfrak{G}$ donné par les formules (5), où $m = p^\alpha$, admet des représentations irréductibles de degré 1 et de degré d. La répartition de ses éléments en classes d'éléments conjugués est la même que pour m premier (voir tableau (4) en 8.2). Toutes les puissances de B, non contenues dans le centre, ont le caractère nul dans les représentations de degré supérieur à 1.

Si m contient des facteurs premiers différents, $\mathfrak{G}m$ n'est plus cyclique et le groupe $\mathfrak{G}$ donné par les formules (5) admet des représentations irréductibles de degrés divers. Soit d_i $(1<d_i<d)$ le degré d'une de ces représentations irréductibles et m_i le plus grand diviseur de m tel que l'ordre de r_i dans $\mathfrak{G}m_i$ soit égal à d_i. Le groupe $\mathfrak{G}/\{A^{m_i}\}$, donné par les relations (6), admet pour centre $\{B^{d_i}\}$. L'élément B^{kd_i} est seul dans sa classe, les $B^{kd_i}A^\mu$ $(\mu = 1, 2, \ldots, m_i - 1)$ se répartissent en classes d'éléments conjugués de la même manière que les A^μ. Dans $\mathfrak{G}$, les m éléments $B^{kd_i}A^\mu\left(\mu = 1, 2, \ldots, m\,;\ k \text{ fixe premier à } \frac{d}{d_i}\right)$ se répartissent dans les mêmes classes, le nombre d'éléments dans chaque classe étant multiplié par $\frac{m}{m_i}$. C'est ainsi que la classe de B^{kd_i} contient les $\frac{m}{m_i}$ éléments : $B^{kd_i}, B^{kd_i}A^{m_i}, \ldots, B^{kd_i}A^{\left(\frac{m}{m_i}-1\right)m_i}$; la classe qui contient $B^{kd_i}A^\mu$ contient aussi : $B^{kd_i}A^{\mu+m_i}, \ldots, B^{kd_i}A^{\mu+\left(\frac{m}{m_i}-1\right)m_i}$.

J'en déduis deux conséquences importantes. Tout d'abord, le normalisateur dans $\mathfrak{G}$ de B^{kd_i} est d'ordre $m_i dn'$. Or, B^{kd_i} étant dans le centre

de $\mathfrak{G}/\{A^{m_i}\}$, la somme des $\chi_j(B^{kd_i})\,\bar{\chi}_j(B^{kd_i})$ étendue aux représentations irréductibles de $\mathfrak{G}/\{A^{m_i}\}$ (qui induisent des représentations irréductibles de $\mathfrak{G}$) donne l'ordre $m_i d n'$ de ce groupe. Il résulte de la relation d'orthogonalité (2) de 7.1 que B^{kd_i} a le caractère nul dans toutes les autres représentations irréductibles de $\mathfrak{G}$. *En particulier, dans les* $\frac{\varphi(m)}{d}\,n'$ *représentations irréductibles qui nous intéressent (voir plus haut), toute puissance de B non située dans le centre a un caractère nul. Il en est de même pour les $B^\nu A^\mu$ à condition que B^ν n'appartienne pas au centre.*

D'autre part, dans la suite $B^{kd_i}A^\mu$, $B^{kd_i}A^{\mu+m_i}, \ldots, B^{kd_i}A^{\mu+\left(\frac{m}{m_i}-1\right)m_i}$ d'éléments appartenant à la même classe, il en est un où l'exposant de A est multiple de $\frac{m}{m_i}$. Ces exposants sont en effet en nombre $\frac{m}{m_i}$ et deux à deux incongrus $\left(\text{modulo } \frac{m}{m_i}\right)$; l'un est $\equiv 0\left(\frac{m}{m_i}\right)$. Or, $BAB^{-1} = A^r$ entraîne $B^{kd_i}A^{\frac{m}{m_i}}B^{-kd_i} = A^{\frac{m}{m_i}r^{kd_i}} = A^{\frac{m}{m_i}}$ en vertu de $r^{d_i} \equiv 1\,(m_i)$; B^{kd_i} est permutable avec $A^{\frac{m}{m_i}}$. *Toute classe de $\mathfrak{G}$ qui renferme un $B^\nu A^\mu$, renferme un $B^\nu A^{\mu'}$, où B^ν est permutable avec $A^{\mu'}$.*

Les raisonnements de 8.1 e) f) g) sont dès lors applicables. Le caractère de toute puissance de B non contenue dans le centre étant nul, *les valeurs propres de B se répartissent aux sommets d'un polygone régulier de d côtés. La condition nécessaire et suffisante pour qu'elles puissent être toutes primitives est que n' soit multiple des facteurs premiers de d.* Il existe alors

$$\frac{\varphi(m)}{d}\,\varphi(n') = \frac{\varphi(g)}{d^2}$$

représentations irréductibles de degré d où aucune puissance de A ou de B, $\neq E$, n'admet la valeur propre $+1$; la deuxième remarque prouve que la valeur propre $+1$ ne peut intervenir dans aucune classe $\neq E$ ($B^\nu A^{\mu'}$ a pour valeurs propres le produit des valeurs propres de B^ν et $A^{\mu'}$ qui sont d'ordres différents, les ordres de A et B étant premiers entre eux). Ces $\frac{\varphi(g)}{d^2}$ représentations irréductibles sont sans points fixes. De plus, et ceci est essentiel, l'application du critère $\sum_S \chi(S^2) = cg$ (7.2), montre qu'elles appartiennent à la troisième catégorie (non équivalentes à l'imaginaire conjuguée) si $n' > 2$ et à la deuxième (équivalentes à l'imaginaire conjuguée mais à aucune représentation réelle) si $n' = 2$. Résumons ces résultats dans les deux théorèmes suivants :

Théorème III : *La condition nécessaire et suffisante d'existence de représentations sans points fixes d'un groupe $\mathfrak{G}$ fini, du premier type, non cyclique, d'ordre $g = m\,dn'$, défini par :*

$$A^m = E \qquad B^{dn'} = E \qquad BAB^{-1} = A^r$$

où n', r, $r-1$, d (ordre de r dans $\mathfrak{G}m$) sont premiers à m, est que n' soit multiple des facteurs premiers de d[26]).

Théorème III* : *Si un groupe $\mathfrak{G}$ fini, du premier type, non cyclique, admet une représentation sans points fixes :*

a) *toutes ses représentations irréductibles fidèles sont sans points fixes ;*

b) *elles ont toutes le même degré d, diviseur de l'ordre g du groupe ;*

c) *leur nombre est égal à $\frac{\varphi(g)}{d^2}$;*

d) *elles ne sont pas équivalentes à des représentations réelles et sont ou ne sont pas équivalentes à l'imaginaire conjuguée selon que $n' = 2$ ou $n' > 2$.*

Les représentations orthogonales de $\mathfrak{G}$, irréductibles dans $\mathfrak{U}^r(n)$, sans points fixes, sont de degré $2d$ et en nombre (non équivalentes) égal à $\frac{1}{2}\frac{\varphi(g)}{d^2}$ si $n' > 2$, $\frac{\varphi(g)}{d^2}$ si $n' = 2$. $\mathfrak{G}$ est relatif à la dimension $2d - 1$ et apparaît comme groupe de rotations sans points fixes pour toutes les dimensions $2kd - 1$.

Signalons en particulier cette conséquence : les seules formes spatiales sphériques de dimensions paires sont l'espace sphérique et l'espace elliptique (voir 7.3 et le théorème I en 7.4 pour les formes à groupe fondamental du deuxième type).

A titre d'exemple, le groupe $\mathfrak{G}$ défini par :

$$A^{35} = E \qquad B^{12n'} = E \qquad BAB^{-1} = A^2$$

d'ordre $g = 420n'$, admet : $12n'$ représentations irréductibles de degré 1, $3n'$ de degré 4, $8n'$ de degré 3, $2n'$ de degré 12. $2\varphi(n')$ des représentations de degré 12 sont fidèles. Si n' (premier à 35) est multiple de 6, ces représentations fidèles sont sans points fixes ; $n' = 6$, par exemple, conduit à un groupe d'ordre 2520 admettant 4 représentations irréductibles, sans points fixes, de degré 12, non équivalentes à l'imaginaire conjuguée. Ce groupe est relatif à la dimension 23 (2.12 − 1) et admet deux représentations orthogonales, sans points fixes, non équivalentes, irréductibles dans $\mathfrak{U}^r(24)$, de degré 24.

---

[26]) Cette condition est indiquée par Burnside [6], qui l'obtient par une tout autre méthode.

§ 9. Groupes du deuxième type, en particulier de la classe (α)

J'ai proposé, à la fin de 5.7, une répartition des groupes $\mathfrak{G}$ du deuxième type (groupes finis dont les p-sous-groupes de Sylow sont cycliques pour $p \neq 2$, quaternioniques pour $p = 2$) en trois classes : les deux premières (α) et (β) renfermant les groupes métabéliens de rang 2, la troisième (γ) les groupes métabéliens de rangs 3 et 4 et les groupes non résolubles. Je vais m'attacher surtout à la classe (α) et établir des théorèmes très analogues à ceux régissant les groupes du premier type.

9.1. Rappelons qu'un groupe $\mathfrak{G}$ du deuxième type est dit de la classe (α) si $\mathfrak{G}'$ cyclique est contenu dans un sous-groupe invariant cyclique d'ordre double. Il est donné par (relations (6) en 5.7) :

$$A^{2^{\alpha-1}n} = E \qquad B^{2u} = A^{2^{\alpha-2}} \qquad BAB^{-1} = A^r \tag{1}$$

avec les conditions numériques :

$$\alpha \geqslant 3\ , \quad (u, n) = 1, \quad u \text{ et } n \text{ impairs}$$

$$r^{2u} \equiv 1\,(2^{\alpha-1}n) \quad r \equiv -1\,(2^{\alpha-1}) \quad (r-1,\ 2^{\alpha-1}n) = 2$$

Son ordre est $g = 2^\alpha n u$. Le groupe des commutateurs $\mathfrak{G}' = \{A^2\}$ est cyclique d'ordre $2^{\alpha-2}n$, le groupe-quotient $\mathfrak{G}/\mathfrak{G}'$ abélien d'ordre $4u$ et de type $(2, 2, u)$. A^n et B^u engendrent l'un des 2-sous-groupes de Sylow, tous isomorphes à $\mathfrak{Q}2^\alpha$.

Je pose $2^{\alpha-1}n = m$, multiple de 4 à cause de $\alpha \geqslant 3$, et je désigne par d l'ordre de r dans $\mathfrak{G}m$ (3.1) : $r^d \equiv 1\,(m)$. Il résulte des conditions numériques qui accompagnent les relations (1) que d est pair, conséquence de $r \equiv -1\,(2^{\alpha-1})$, et que $2u$ est multiple de d ($r^{2u} \equiv 1$ modulo m). Comme u est impair, d est divisible par 2 et non par 4 : $d = 4k + 2$. De plus, $2u = du'$ avec u' impair et même premier à m. Les relations deviennent :

$$A^m = E \qquad B^{du'} = A^{\frac{m}{2}} \qquad BAB^{-1} = A^r \tag{2}$$

$m = 2^{\alpha-1}n$ (n impair, $\alpha \geqslant 3$) étant donné, il faut choisir r de telle sorte que r, $\dfrac{r-1}{2}$, $\dfrac{d}{2}$ soient premiers à m, et que r soit congru à -1 modulo $2^{\alpha-1}$. Alors d, l'ordre de r dans $\mathfrak{G}m$, est de la forme $4k + 2$. Un tel choix est possible quel que soit m (multiple de 4) ; on prendra au besoin $r = -1$ d'ordre 2. Il faut choisir en outre u' premier à m.

Sous cette forme, l'ordre de $\mathfrak{G}$ est $g = mdu'$. Remarquons que l'ordre de B est égal à $2du'$. Je désigne par m_i un diviseur quelconque de m, par r_i le reste de r (modulo m_i) par d_i l'ordre de r_i dans $\mathfrak{G}m_i$ (pour $m_i = 2$ ou 1, je pose $d_i = 1$). Des raisonnements très analogues à ceux exposés au § 8 pour les groupes du premier type conduisent au théorème :

Le groupe $\mathfrak{G}$ donné par les relations (2) *ci-dessus admet en tout*

$$\sum_{m_i/m} \frac{\varphi(m_i)\, du'}{d_i^2}$$

représentations irréductibles (*unitaires*) *de degrés d_i, diviseurs de d;*

$$\frac{\varphi(m)}{d}\, \varphi(u')$$

sont fidèles et de degré d.

La recherche des représentations sans points fixes aboutit aux deux théorèmes suivants :

Théorème IV : *La condition nécessaire et suffisante d'existence de représentations sans points fixes d'un groupe $\mathfrak{G}$ fini, du deuxième type et de la classe* (α), *d'ordre $g = m\, du'$, donné par les relations* (2) *ci-dessus, est que u'* (*premier à m*) *soit multiple des facteurs premiers impairs de d.*

Théorème IV* : *Si un groupe $\mathfrak{G}$ fini, du deuxième type et de la classe* (α), *admet une représentation sans points fixes :*

a) *toutes ses représentations irréductibles fidèles sont sans points fixes;*

b) *elles ont toutes le même degré d, diviseur de l'ordre g du groupe ;*

c) *leur nombre est égal à* $\dfrac{\varphi(g)}{d^2}$;

d) *elles ne sont pas équivalentes à des représentations réelles et sont ou ne sont pas équivalentes à l'imaginaire conjuguée selon que $u' = 1$ ou $u' > 1$.*

Précisons que $u' = 1$ n'est possible que si $d = 2$ et que ce cas se présente effectivement pour les groupes quaternioniques (7.4) et plus généralement pour ceux des groupes diédriques binaires qui sont du deuxième type (6.1).

Les représentations orthogonales irréductibles correspondantes ont toutes le degré $2d$ (de la forme $8k + 4$) et sont en nombre (non équivalentes) égal à $\frac{1}{2}\dfrac{\varphi(g)}{d^2}$ si $u' > 1$, $\dfrac{\varphi(g)}{d^2} = \dfrac{\varphi(g)}{4}$ si $u' = 1$.

9.2. Avant de construire un exemple relatif au théorème IV, je vais montrer qu'inversément, pour toute valeur $d = 4k + 2$ donnée, on peut trouver une infinité de groupes du type considéré, ce qui conduit au :

Théorème V : *Toute sphère S^{8k+3} dont le nombre de dimensions est congru à 3 (mod. 8), admet une infinité de groupes finis de rotations sans points fixes, du deuxième type et de la classe (α), ne se présentant pas pour des dimensions inférieures.*

Il existe une infinité d'entiers premiers n tels que $\varphi(n) = n - 1$ soit divisible par $d = 4k + 2$ (8.3). Choisissons pour m l'une quelconque des valeurs $2^{\alpha-1}n$ $(\alpha \geqslant 3)$. Si l'on peut trouver un r vérifiant les conditions qui accompagnent les relations (2) de 9.1, le théorème est établi.

L'ordre de $\mathfrak{G}m$ est $\varphi(2^{\alpha-1}n) = 2^{\alpha-2}(n-1)$. Réduisons ses éléments modulo $2^{\alpha-1}$; on réalise un homomorphisme de $\mathfrak{G}m$ sur $\mathfrak{G}2^{\alpha-1}$ (d'ordre $2^{\alpha-2}$). Le noyau $\mathfrak{N}$ de cet homomorphisme est le sous-groupe invariant de $\mathfrak{G}m$ formé des éléments $\equiv 1$ (modulo $2^{\alpha-1}$) ; son ordre est $n - 1$ et comme ses éléments sont incongrus deux à deux modulo n (ils sont tous congrus à l'un d'eux modulo $2^{\alpha-1}$ mais incongrus deux à deux modulo $2^{\alpha-1}n$), il est isomorphe au groupe cyclique $\mathfrak{G}n$ d'ordre $n - 1$.

Il faut choisir r parmi les éléments $\equiv -1$ (modulo $2^{\alpha-1}$). Or ceux-ci forment la classe $\mathfrak{C}$ de $\mathfrak{G}m/\mathfrak{N}$ qui contient -1 ; on les obtient en multipliant ceux de $\mathfrak{N}$ par -1. L'ordre d'un tel élément est celui de l'élément correspondant de $\mathfrak{N}$ si celui-ci est pair, son double s'il est impair. Or dans $\mathfrak{N}$ (cyclique d'ordre $n - 1$) existe un seul sous-groupe d'ordre d et par conséquent $\varphi(d)$ éléments d'ordre d et $\varphi\left(\frac{d}{2}\right) = \varphi(d)$ éléments d'ordre $\frac{d}{2}$ (impair). La classe $\mathfrak{C}$ renferme $2\varphi(d)$ éléments d'ordre d, qui tous peuvent être choisis pour r si $d \neq 2$, car le seul élément de $\mathfrak{C} \equiv 1(n)$, donc tel que $\frac{r-1}{2}$ ne soit pas premier à m $\left(\frac{r-1}{2} \equiv \frac{-2}{2} \equiv -1 \text{ modulo } 2^{\alpha-1} \text{ est premier à } 2^{\alpha-1}\right)$, est d'ordre 2. Si $d = 2$, la seule valeur admissible pour r est -1. C'est la valeur que l'on rencontre pour tous les groupes de ce type relatifs à S^3. Il existe dans tous les cas, des valeurs de r vérifiant les conditions imposées, le théorème est établi.

Remarques : 1. Les diverses valeurs de r peuvent conduire à des groupes isomorphes (voir fin de 4.6).

2. Les groupes qu'on peut ainsi construire sont en nombre infini pour deux raisons : l'ordre du groupe des commutateurs peut être choisi d'une infinité de façons, ainsi que l'ordre du groupe-quotient correspondant.

3. Le groupe $\mathfrak{G}m$ joue, comme pour $\mathfrak{G}$ du premier type, un rôle essentiel.

9.3. Je vais construire, à titre d'exemple, le *groupe de rotations sans points fixes, du deuxième type et de la classe* (α), *non relatif à* S^3, *d'ordre minimum.*

Il est *relatif à* S^{11} et correspond à $d = 6$; n vaut 7, 13, 19, 31,... Je choisis $n = 7$ et $m = 28$; les valeurs admissibles pour r sont 3, 11, 19, 23 (en nombre égal à $2\varphi(6) = 4$) : 3 et 19 ainsi que 11 et 23, conduisent à des groupes isomorphes si u' est premier à 5. J'obtiens entre autres le groupe défini par :

$$A^{28} = E \qquad B^{6u'} = A^{14} \qquad BAB^{-1} = A^3$$

d'ordre $g = 168u'$, admettant $\dfrac{\varphi(g)}{36}$ représentations irréductibles sans points fixes, de degré 6, si u' (premier à 28) est multiple de 3 (seul facteur premier impair de 6).

Pour $u' = 3$, $\mathfrak{G}$ est d'ordre 504 et admet 4 représentations unitaires, sans points fixes, de degré 6 ; d'où 2 représentations orthogonales sans points fixes, non équivalentes, irréductibles dans $\mathfrak{U}^r(12)$, de degré 12. $\mathfrak{G}$ apparaît pour $S^{11}, S^{23}, \ldots, S^{12k-1}, \ldots$. Ses 2-sous-groupes de Sylow sont isomorphes à $\mathfrak{Q}8$.

Voici des *groupes de rotations sans points fixes relatifs à* S^{11}, dont les 2-sous-groupes de Sylow sont isomorphes à $\mathfrak{Q}32$; $m = 16 \cdot 7 = 112$:

$$A^{112} = E \qquad B^{6u'} = A^{56} \qquad BAB^{-1} = A^r$$

r vaut 31, 47, 79 ou 95 (les deux premières valeurs et les deux dernières conduisent à des groupes isomorphes si u' est premier à 5). u', premier à 112, doit être multiple de 3 ; $u' = 3$ conduit à un groupe d'ordre $g = 2016$ admettant 16 représentations irréductibles de degré 6.

9.4. Il est très probable que des résultats analogues pourraient être obtenus pour les groupes du deuxième type des classes (β) et (γ).

Je me contente de signaler que les groupes binaires du tétraèdre, de l'octaèdre et de l'icosaèdre (§ 6), qui appartiennent à la classe (γ), admettent des représentations irréductibles (unitaires), sans points fixes, de degré 2. Comme groupes de rotations sans points fixes, ils sont relatifs à S^3. Ainsi $\mathfrak{T}^*$ admet 3 représentations irréductibles de degré 1, 1 de degré 3 (non fidèle) et 3 de degré 2 ; deux des représentations irréductibles de degré 2 sont sans points fixes. Fait remarquable, ce nombre est égal à $\dfrac{\varphi(g)}{d^2}$.

Chapitre IV
Applications

§ 10. Quelques corollaires des théorèmes fondamentaux

Je déduis des théorèmes I à V des conséquences relatives aux groupes finis de rotations sans points fixes de la sphère S^n à n dimensions. Pour les dimensions paires, j'ai retrouvé plus haut la propriété connue que seuls interviennent le groupe cyclique d'ordre 2 (groupe fondamental de l'espace elliptique, non orientable pour n pair) et le groupe se réduisant à l'identité (groupe fondamental de l'espace sphérique simplement connexe). Pour les dimensions n impaires, il importe de distinguer deux cas : $n \equiv 1$ et $n \equiv 3$ (modulo 4), c'est-à-dire les dimensions de la forme $4k + 1$ et $4k + 3$.

10.1. Les groupes du premier type sont étudiés complètement au § 8, au point de vue de leurs représentations sans points fixes. Les théorèmes I en 7.4, II en 8.3 et III en 8.4, permettent d'énoncer le :

Théorème VI : *Les groupes finis de rotations sans points fixes d'une sphère S^{4k+1} sont tous du premier type (cycliques ou non abéliens). Il s'en présente de nouveaux, en nombre infini, pour toute dimension $4k + 1$ et leur recherche se ramène à un problème purement arithmétique.*

10.2. Les sphères S^{4k+3} admettent une infinité de groupes finis de rotations sans points fixes, du premier et du deuxième type. Pour le premier type, il s'en présente de nouveaux, en nombre infini, pour toute dimension $4k + 3$; pour le deuxième type, j'ai montré en 9.2 (théorème V) que, pour toutes les dimensions $8k + 3$, apparaissent des groupes nouveaux de la classe (α) et j'ai donné la possibilité de les construire.

Un groupe $\mathfrak{G}$ du premier type (non cyclique), admettant des représentations irréductibles (unitaires), sans points fixes, de degré d, est relatif à la dimension $2d - 1$. Il admet des représentations (réductibles) comme groupe de rotations sans points fixes pour toutes les dimensions $2hd - 1$ et pour celles-là seules. Si d est pair, $2d - 1$ et $2hd - 1$ sont $\equiv 3$ (modulo 4) ; si d est impair, $2d - 1$ est $\equiv 1$ (modulo 4) et $2hd - 1$ est congru à 1 ou 3 suivant que h est impair ou pair.

Théorème VII : *Un groupe fini $\mathfrak{G}$ de rotations sans points fixes, du premier type, relatif à une sphère S^{4k+3} ne se présente pour aucune sphère S^{4k+1}. Dans les mêmes conditions, si le groupe $\mathfrak{G}$ est relatif à une sphère S^{4k+1}, il se présente alternativement pour des sphères S^{4k+1} et S^{4k+3}.*

En particulier, *aucun groupe* $\mathfrak{G}$, *non cyclique, de rotations sans points fixes de la sphère* S^3 *ne se présente pour une sphère* S^{4k+1} (voir 10.4). Si $\mathfrak{G}$ est du deuxième type c'est immédiat et si $\mathfrak{G}$ est du premier type, il est *relatif* à la dimension 3.

10.3. Un groupe de rotations sans points fixes d'ordre impair est du premier type, car l'ordre d'un groupe du deuxième type est divisible au moins par 8. S'il n'est pas cyclique, le degré de ses représentations orthogonales sans points fixes est divisible par un entier $d > 1$ impair, ce qui exclut les degrés 2^n.

Théorème VIII: *Les groupes d'ordre impair de rotations sans points fixes d'une sphère de dimension* $2^n - 1$ *sont tous cycliques. Par contre, toute sphère dont la dimension est un nombre impair qui n'est pas de la forme* $2^n - 1$ *admet une infinité de groupes d'ordre impair, non abéliens, de rotations sans points fixes.*

La première partie de ce théorème est la généralisation d'un théorème relatif à S^3 démontré par M. H. Hopf[27]).

10.4. Le groupe $\mathfrak{G}$ fini admettant des représentations réelles sans points fixes est du premier ou du deuxième type (2.5). S'il est du premier type, ses représentations réelles sans points fixes sont de degrés $2kd$, d étant le degré des représentations irréductibles (unitaires) sans points fixes (théorème III* 8.4). S'il est du deuxième type, ses représentations réelles sans points fixes sont de degrés multiples de 4 (théorème I 7.4).

On en déduit le théorème suivant, dû à M. H. Hopf[28]); il le démontre par voie topologique, comme cas particulier d'un théorème sur les groupes d'automorphismes sans points fixes des variétés admettant les mêmes groupes de Betti (ordinaires, c'est-à-dire relatifs à l'anneau des entiers rationnels) que la sphère S^n:

Théorème IX: *Si le groupe fini* $\mathfrak{G}$, *non cyclique, admet une représentation réelle sans points fixes de degré* $2d_1$, *il n'admet aucune représentation réelle sans points fixes de degré* $2d_2$ *où* d_2 *est premier à* d_1.

Ajoutons la remarque suivante:

Si $\mathfrak{G}$ *est du premier type ou du deuxième type et de la classe* (α), *les degrés des représentations réelles sans points fixes de* $\mathfrak{G}$ *sont les multiples du double* $2d$ *du degré* d *de ses représentations irréductibles (unitaires)* (théorèmes III* 8.4 et IV* 9.1).

---

[27]) [1] p. 325.
[28]) [9] 15.5 p. 76.

Le cas particulier $d_1 = 2$, signalé par M. Hopf, exprime qu'aucun groupe de rotations sans points fixes de S^3 ne se présente pour une sphère S^{4k+1} (rencontré en 10.2 comme conséquence du théorème VII).

10.5. Une rotation de S^{2d-1} est une *translation* au sens de Clifford si les valeurs propres de la matrice représentative (de degré $2d$) sont égales à l'une d'elles ou à l'imaginaire conjuguée; plus exactement, d d'entre elles doivent être égales à $\lambda = e^{i\alpha}$ et d à $\bar{\lambda} = e^{-i\alpha}$. Une telle translation est caractérisée géométriquement par le fait que tout vecteur réel subit une rotation d'amplitude α; elle est, par définition même, sans points fixes.

Existe-t-il des groupes finis formés uniquement de telles translations? La réponse est affirmative; les groupes quaternioniques admettent des représentations de cette nature, comme il résulte de 7.4.

Je vais établir la propriété suivante, conséquence d'un théorème topologique de M. E. Stiefel[29]):

Théorème X: *Il n'existe aucun groupe fini, non cyclique, de rotations d'une sphère S^{4k+1} dont les éléments soient tous des translations* (au sens de Clifford).

J'ajoute ce complément:

Les groupes de rotations du premier type (non cycliques) et du deuxième type classe (α), formés uniquement de translations, sont les groupes diédriques binaires (6.1); *ils sont relatifs à S^3.*

Démonstration: Soit $\mathfrak{G}$ un groupe fini, non cyclique, de translations et Γ l'une de ses composantes irréductibles (unitaire). Le degré de Γ est supérieur à 1 (sinon il y aurait des points fixes). Il résulte d'un théorème de Burnside[30]) que Γ renferme un élément au moins dont le caractère est nul. Soit B l'élément correspondant de $\mathfrak{G}$; ses valeurs propres dans Γ sont λ et $\bar{\lambda}$ (en nombre non nécessairement égal, il pourrait y avoir compensation avec la représentation complexe conjuguée). Or, le caractère devant être nul, ces valeurs propres ne peuvent être que i et $-i$ en nombre égal. Le degré de Γ est pair. De plus l'ordre de B est 4 (B^4 a des valeurs propres $+1$); l'ordre de $\mathfrak{G}$ est donc lui-même divisible par 4.

Pour la *première partie du théorème*, seuls interviennent les groupes $\mathfrak{G}$ du premier type (théorème VI 10.1); les représentations irréductibles (unitaires) sans points fixes de $\mathfrak{G}$ sont toutes de même degré d, celui de

---

[29]) *E. Stiefel*, Richtungsfelder und Fernparallelismus in n-dimensionalen Mannigfaltigkeiten, Comment. Math. Helvet. 8 (1935/36), Satz 27.

[30]) Proceedings of the London Math. Soc., New Series, Vol. I, p. 115.

Γ, donc pair. $\mathfrak{G}$ est relatif à une sphère S^{4k+3} et ne se présente pour aucune sphère S^{4k+1} (théorème VII 10.2).

Pour la *deuxième partie*, supposons tout d'abord $\mathfrak{G}$ du premier type; l'élément B, d'une classe qui engendre $\mathfrak{G}/\mathfrak{G}'$ a le caractère nul dans toute représentation irréductible sans points fixes (8.4). B est d'ordre 4 et $\mathfrak{G}$ du type défini par les relations (3) en 6.1. Pour un groupe $\mathfrak{G}$ du deuxième type et de la classe (α), il en est de même pour l'élément B, d'une classe engendrant $\mathfrak{G}/\{A\}$. B est d'ordre 4 et $\mathfrak{G}$ du type défini par les relations (2) en 6.1.

Les autres groupes polyédriques binaires (§ 6) admettent également des représentations comme groupes de translations (de degré 4). Ils appartiennent au deuxième type, classe (γ). Peut-être n'en existe-t-il pas d'autres, mais je n'ai pas encore pu le démontrer.

§ 11. Le point de vue topologique

11.1. Le problème de topologie à la solution duquel les résultats ci-dessus apportent une contribution est le problème spatial de Clifford-Klein, ainsi nommé par Killing[31]).

Il s'agit de déterminer les variétés V à n dimensions, connexes et sans frontière, métrisables par un ds^2 défini positif, à courbure riemannienne constante, et les géométries ainsi définies. De telles variétés sont localement applicables sur l'espace euclidien, hyperbolique ou sphérique. On exclut les variétés qui se déduisent de V en supprimant un ensemble fermé de points (la variété restant connexe) et en conservant la métrique, par l'exigence que sur toute géodésique passant par un point P quelconque de V on puisse reporter, dans les deux sens, tout segment positif a. C'est ainsi que le plan cartésien (homéomorphe à la sphère pointée) muni d'une métrique sphérique par projection stéréographique de la sphère, ne sera pas considéré comme définissant une géométrie différente de la géométrie sphérique. Dans ces conditions, V est dite variété de Clifford-Klein et la géométrie ainsi définie, forme spatiale de Clifford-Klein.

Le théorème fondamental, dû à Killing, et précisé par M. H. Hopf dans le travail cité[31]), exprime que la totalité des formes spatiales de Clifford-Klein peut s'obtenir en cherchant les groupes discontinus de déplacements de l'espace $\overline{V}$ euclidien, hyperbolique ou sphérique (au sens de la géométrie sur $\overline{V}$), sans points fixes, sauf pour le déplacement identique, et tels que l'ensemble des images d'un point de $\overline{V}$ par les opérations du groupe ne présente jamais de point d'accumulation sur $\overline{V}$. Un tel groupe

[31]) Voir à ce propos l'introduction et le § 1 du travail de M. H. Hopf [1].

$\mathfrak{G}$ définit une variété V, admettant $\overline{V}$ comme espace de recouvrement universel (simplement connexe), le groupe des transformations de recouvrement étant $\mathfrak{G}$, isomorphe au groupe fondamental ou groupe de connexion de V.

En particulier, la totalité des variétés de Clifford-Klein à courbure constante positive, ou *formes spatiales sphériques*, s'obtient en cherchant les groupes $\mathfrak{G}$ *finis* de déplacements isométriques (rotations), sans points fixes, de la sphère à n dimensions S^n.

Les groupes $\mathfrak{G}$ étudiés dans le présent travail donnent la totalité des groupes fondamentaux des formes spatiales sphériques.

Les théorèmes II 8.3 et V 9.2 prouvent l'existence de nouvelles formes sphériques pour toutes les dimensions impaires, en ce sens que le groupe fondamental $\mathfrak{G}$ n'est isomorphe à aucun des groupes fondamentaux des formes de dimensions inférieures (voir 11.4).

Il est à remarquer que ces formes spatiales sphériques peuvent se présenter comme espaces de recouvrement les unes des autres. Ainsi une forme de groupe fondamental $\mathfrak{G}$ du premier type admet un espace de recouvrement régulier, forme de groupe fondamental $\mathfrak{G}'$ cyclique (espace lenticulaire), le groupe des transformations de recouvrement étant $\mathfrak{G}/\mathfrak{G}'$ cyclique. Autre exemple : si $\mathfrak{G}$ est du deuxième type, métabélien de rang 2 (classes (α) et (β)), il admet un sous-groupe invariant $\mathfrak{N}$ du premier type, dont l'ordre est la partie impaire de l'ordre de $\mathfrak{G}$ (5.5). La forme correspondante admet un espace de recouvrement régulier à 2^α feuillets, forme de groupe fondamental $\mathfrak{N}$ du premier type, le groupe des transformations de recouvrement étant isomorphe à $\mathfrak{Q}\,2^\alpha$ et permutant transitivement les 2^α feuillets.

11.2. Un groupe fini $\mathfrak{G}$ de rotations sans points fixes de S^n, d'ordre pair, contient *un et un seul élément d'ordre 2*, $-E$ (conséquence de 7.3 et du fait que la représentation est fidèle). Le groupe $\mathfrak{P}$ formé de E et $-E$ est sous-groupe invariant de $\mathfrak{G}$. La forme spatiale sphérique correspondante, de groupe fondamental $\mathfrak{G}$ (11.1), admet P^n, l'espace elliptique, comme espace de recouvrement régulier (S^n étant l'espace de recouvrement universel, qui recouvre deux fois P^n). La forme est dite *elliptique* (si $\mathfrak{G}$ est d'ordre impair, la forme est sphérique mais non elliptique). Le groupe des transformations de recouvrement est isomorphe à $\mathfrak{G}/\mathfrak{P}$, groupe de déplacements (au sens de la métrique elliptique), sans points fixes, de P^n.

Ces groupes se déduisent sans peine des groupes de rotations sans points fixes de S^n. Si $\mathfrak{G}$ est cyclique (d'ordre pair), $\mathfrak{G}/\mathfrak{P}$ est aussi cyc-

lique. Pour $\mathfrak{G}$ du premier type (non cyclique), $\mathfrak{G}/\mathfrak{P}$ est également du premier type (ne vérifiant plus toujours la condition n' multiple des facteurs premiers de d). Mais pour $\mathfrak{G}$ du deuxième type, $\mathfrak{G}/\mathfrak{P}$ n'est plus du deuxième type, car ses 2-sous-groupes de Sylow sont diédriques (3.2).

Je vais préciser la structure de $\mathfrak{G}/\mathfrak{P}$ quand il est abélien. Si $\mathfrak{G}$ n'est pas abélien, $\mathfrak{P}$ doit être identique au groupe des commutateurs $\mathfrak{G}'\cdot\mathfrak{G}'$ d'ordre 2 entraîne $\mathfrak{G}$ du deuxième type ; j'ai montré en 5.7 que $\mathfrak{G}$ est alors isomorphe au produit direct $\mathfrak{Q}8\times\mathfrak{Z}u$ (u impair). $\mathfrak{G}/\mathfrak{P}$ est abélien de type $(2, 2, u)$.

Théorème XI : *Les groupes finis, abéliens, de déplacements elliptiques de P^n (l'espace elliptique), sans points fixes, sont cycliques ou de type $(2, 2, u)$, u impair.*

11.3. Les groupes de Betti $\mathfrak{B}_J^n$ d'une forme spatiale sphérique de dimension N sont entièrement déterminés par le groupe fondamental $\mathfrak{G}$, le domaine J des coefficients et le nombre N. $\mathfrak{G}$ étant fini, d'ordre g, les groupes de Betti (ordinaires, c'est-à-dire où J est l'anneau des entiers rationnels), sont également finis et l'ordre de chacun de leurs éléments est un diviseur de g[32]).

Je vais préciser ici la structure du premier groupe de Betti $\mathfrak{B}^1$ isomorphe à $\mathfrak{G}/\mathfrak{G}'$. Les propriétés des groupes $\mathfrak{G}$ du premier et du deuxième type (4.2 et 5.2), ainsi que les théorèmes III 8.4 et IV 9.1, permettent d'énoncer le :

Théorème XII : *Le groupe de Betti $\mathfrak{B}^1 \cong \mathfrak{G}/\mathfrak{G}'$ d'une forme spatiale sphérique de groupe fondamental $\mathfrak{G}$, est: soit le groupe nul, soit cyclique d'ordre quelconque m (un coefficient de torsion égal à m), soit abélien de type $(2, 2, u)$ u impair (coefficients de torsion 2 et $2u$). De plus, si $\mathfrak{G}$ est du premier type ou du deuxième et de la classe (α), relatif à la dimension $2d-1$, l'ordre de $\mathfrak{B}^1$ est divisible par $\prod_i p_i^{\alpha_i+1}$, où $d = \prod_i p_i^{\alpha_i}$ est la décomposition de d en facteurs premiers distincts.*

Signalons que même l'anneau d'homologie d'une forme spatiale sphérique est déterminé par son groupe fondamental. C'est ce qui résulte d'un travail récent de M. B. Eckmann[33]).

11.4. Un problème qui se présente naturellement est celui de la classification des formes spatiales sphériques.

---

[32]) Ainsi qu'il résulte du travail de M. H. Hopf [9].

[33]) *B. Eckmann*, Der Cohomologie-Ring einer beliebigen Gruppe, Comment. Math. Helvet. 18 (1945/46), 232—282.

On vérifie facilement l'affirmation suivante:

Pour que deux représentations réelles Γ_1 et Γ_2, sans points fixes, d'un même groupe $\mathfrak{G}$ définissent deux formes spatiales *isométriques*, il faut et il suffit qu'il existe un automorphisme α de $\mathfrak{G}$ tel que $\Gamma_2(x)$ soit équivalente à $\Gamma_1(\alpha x)$, x désignant un élément quelconque de $\mathfrak{G}$.

L'étude du groupe des automorphismes de $\mathfrak{G}$ permettrait en conséquence l'énumération des formes spatiales de groupe fondamental $\mathfrak{G}$ distinctes au point de vue *métrique*.

Mais examinons la question de l'équivalence *topologique:*

Que deux formes spatiales sphériques aient même groupe fondamental et même dimension est évidemment nécessaire pour leur homéomorphie, mais des exemples bien connus prouvent que ce n'est pas suffisant.

Il résulte d'un théorème de MM. W. Franz[34]) et G. de Rham[35]) que deux formes spatiales sphériques ne peuvent être homéomorphes „au sens combinatoire" sans être isométriques.

Si ce théorème se révélait valable pour l'homéomorphie au sens habituel, la classification topologique se réduirait à la précédente.

INDEX BIBLIOGRAPHIQUE

1] *H. Hopf*, Zum Clifford-Kleinschen Raumproblem, Math. Annalen 95 (1925), 313—339.

[2] *W. Threlfall* und *H. Seifert*, Topologische Untersuchung der Diskontinuitätsbereiche endlicher Bewegungsgruppen des dreidimensionalen sphärischen Raumes, Math. Annalen 104 (1930), 1—70; ib. 107 (1932), 543—586.

[3] *H. Zassenhaus*, Lehrbuch der Gruppentheorie, Hamburger mathematische Einzelschriften 21 (Leipzig und Berlin 1937).

[4] *A. Speiser*, Die Theorie der Gruppen von endlicher Ordnung, 3. Auflage (Berlin 1937).

[5] *W. Burnside*, Theory of Groups of finite Order, 2nd Edition (Cambridge 1911).

[6] *W. Burnside*, On finite groups in which all the Sylow subgroups are cyclical, The Messenger of Math. 35 (1905), 46—50.

[7] *W. Burnside*, On a general property of finite irreducible groups of linear substitutions, The Messenger of Math. 35 (1905), 51—55.

[8] *G. Frobenius und I. Schur*, Über die reellen Darstellungen der endlichen Gruppen, Berliner Sitzungsberichte (1906), 186—208.

[9] *H. Hopf*, Über die Bettischen Gruppen, die zu einer beliebigen Gruppe gehören, Comment. Math. Helvet. 17 (1944/45), 39—79.

(Reçu le 5 décembre 1946.)

---

[34]) *W. Frantz*, Über die Torsion einer Überdeckung, Journal für die r. u. angew. Math. 173 (1935), 245—254.

[35]) *G. de Rham*, Sur les nouveaux invariants topologiques de M. Reidemeister, Recueil mathématique de Moscou T. 1 (43) (1936), 737—743; voir aussi, Sur les complexes avec automorphismes, Comment. Math. Helvet. 12 (1939/40), 191—211.