CLAUDE CHEVALLEY

Le groupe de Janko

Séminaire N. Bourbaki, 1968, exp. nº 331, p. 293-307

<http://www.numdam.org/item?id=SB_1966-1968__10__293_0>

Séminaire BOURBAKI
20e Année, 1967/68, n° 331 Novembre 1967

LE GROUPE DE JANKO

par Claude CHEVALLEY

I. Définition

On sait que tout groupe simple (non cyclique) est d'ordre pair. Ce fait suffirait déjà à indiquer l'importance dans la recherche des groupes simples de l'étude des éléments d'ordres puissances de 2. Cette importance a été confirmée par les travaux de SUZUKI et de BRAUER (cf. notamment [2]). Janko ([4]) s'est proposé de caractériser les groupes finis G qui possèdent les propriétés suivantes :

1) Les 2-groupes de SYLOV de G sont abéliens ;

2) G contient une involution ι dont le centralisateur est isomorphe au produit du groupe $\langle\iota\rangle$ engendré par ι et du groupe $\mathfrak{A}_5$ des permutations paires de $\{1,2,3,4,5\}$;

3) G n'admet aucun sous-groupe d'indice 2 .

Il obtient (entre autres) les résultats suivants :

Il existe au moins un groupe G qui possède les propriétés 1), 2), 3) ; tous les groupes possédant ces propriétés sont isomorphes entre eux et sont simples ; ils ne sont isomorphes à aucun des groupes simples précédemment construits ; ils peuvent se plonger dans le groupe (de type G_2) des automorphismes d'une algèbre de CAYLEY sur le corps premier de caractéristique 11.

De plus, il détermine explicitement l'ordre, les classes d'éléments conjugués, les caractères irréductibles, les groupes de SYLOW et leurs normalisateurs, les sous-groupes maximaux $\neq G$ d'un groupe G possédant ces propriétés ; il montre que G n'admet pas d'automorphismes extérieurs et que son multiplicateur de SCHUR est trivial.

On se propose dans ce qui suit de dégager les étapes essentielles de la démonstration ; il ne sera bien entendu pas possible d'entrer dans les détails. La théorie des caractères et celle des caractères modulaires jouent naturellement un rôle de premier plan. Mais, comme dans le mémoire de FEIT-THOMSON, il faut, avant de pouvoir l'appliquer, obtenir un certain nombre de résultats préliminaires par l'étude directe des conditions imposées.

II - Résultats préalables à l'utilisation des caractères.

1) 2-groupes de SYLOW et leurs normalisateurs.

Soit S un groupe de SYLOW contenant une involution ι dont le centralisateur est de la forme $\langle \iota, A \rangle$, où A est isomorphe à $\mathfrak{A}_5$ (le symbole $\langle \ldots, \ldots \rangle$ signifiera "groupe engendré par"). Comme S est abélien, il est contenu dans $\langle \iota, A \rangle$. Or on voit tout de suite que les 2-groupes de SYLOW de A sont de type $(2,2)$; il en résulte que S est de type $(2,2,2)$. De plus, le centralisateur de S est contenu dans $\langle \iota, A \rangle$ et les 2-groupes de SYLOW de A sont leurs propres centralisateurs ; S est donc son propre centralisateur. Si N est son normalisateur, N/S est représenté fidèlement comme groupe d'automorphismes de S et est d'ordre impair. Or $\mathrm{Aut}\, S$ est isomorphe à $GL(3, \mathbb{Z}/2\,\mathbb{Z})$ qui est d'ordre $8 \times 3 \times 7$; l'ordre de N/S divise 21. Par ailleurs, dans A, le normalisateur d'un 2-groupe de SYLOW contient un élément d'ordre 3 ; l'ordre de N/S est donc $\equiv 0 \pmod 3$, et, ou bien N/S est d'ordre 21 ou bien N est contenu dans $\langle \iota, A \rangle$. Le second cas est impossible. En effet, $N \cap A$ serait alors un sous-groupe d'indice 2 de N ; or, S étant abélien, il est 2-normal (i.e. le centre de S est contenu dans le centre de tout 2-groupe de SYLOW qui le contient), et il résulterait alors du deuxième théorème de Grün (cf [3], p. 215) que G aurait un sous-groupe d'indice 2. On en conclut que N/S est d'ordre 21. Donc N contient une opération σ d'ordre 7 qui permute transitivement tous les éléments $\neq 1$ de S ainsi que tous les sous-groupes d'ordre 4 de S. Donc :

Toutes les involutions de G sont conjuguées ; tous les sous-groupes d'ordre 4 de G sont conjugués.

Le groupe S admet un sous-groupe T d'ordre 4 contenu dans A. On a $\mathcal{Z}_A(T) = T$ et $\mathfrak{N}_A(T)/T$ est d'ordre 3. Soit ι' un élément $\neq 1$ de T ; on a $\mathcal{Z}_G(T) \subset \mathcal{Z}_G(\iota') = \langle \iota' \rangle A'$, où A' est isomorphe à $\mathfrak{A}_5$ (car toutes les involutions de G sont conjuguées), A' contient une involution $\iota'' \neq \iota'$ de T, et $\mathcal{C}_{A'}(\iota'')$ est d'ordre 4. Il en résulte que $\mathcal{C}_G(T)$ est d'ordre 8, d'où $\mathcal{C}_G(T) = S$. Le groupe $\mathcal{N}_G(T)/\mathcal{C}_G(T)$ est représenté fidèlement comme groupe d'automorphismes de T, et ce groupe est d'ordre impair comme il résulte de ce qu'un 2-groupe de SYLOW de G est d'ordre 8. Or Aut T est d'ordre 6 et $\mathcal{N}_A(T)/T$ d'ordre 3 ; il en résulte que $\mathcal{N}_G(T)/\mathcal{C}_G(T)$ est d'ordre 3.

Lemme 1. Si L est un sous-groupe d'ordre 3 de $\mathcal{N}_G(T)$, $\mathcal{N}_G(L)$ contient un sous-groupe T' d'ordre 4 qui contient un élément d'ordre 2 de $\mathcal{C}_G(L)$ ainsi qu'un élément qui transforme les éléments de L en leurs inverses.

Cela résulte de ce que $L \subset A$.

Lemme 2. Le groupe S ne normalise aucun sous-groupe d'ordre impair $\neq 1$ de G.

Soit M un sous-groupe d'ordre impair de G normalisé par S. Soit α un élément $\neq 1$ de S ; on a $\mathcal{C}_G(\alpha) = \langle \alpha, A_\alpha \rangle$, où A_α est un groupe isomorphe à $\mathfrak{A}_5$. Le groupe $M \cap \mathcal{C}_G(\alpha)$, étant d'ordre impair, est dans A_α et est normalisé par le 2-groupe de SYLOW $S \cap A_\alpha$ de A_α. On en déduit facilement que $M \cap \mathcal{C}_G(\alpha) = \{1\}$. Or un automorphisme d'ordre 1 ou 2 d'un groupe M d'ordre impair qui n'a aucun élément fixe $\neq 1$ transforme tout élément de M en son inverse ; on a donc $\alpha m \alpha^{-1} = m^{-1}$ pour tout $\alpha \neq 1$ de S et tout $m \in M$. Il en résulte tout de suite que $M = \{1\}$.

2) Le normalisateur d'un sous-groupe d'ordre 5.

Utilisant les notations de 1), le groupe A contient un groupe V d'ordre 5 et une involution qui transforme les éléments de V en leurs inverses. Il en résulte que V est normalisé par un sous-groupe T d'ordre 4 de S contenant l'involution ι qui centralise V. Nous désignerons par M un élément maximal de l'ensemble des sous-groupes d'ordres impairs de G qui sont normalisés par T ; on a donc $M \neq \{1\}$.

Nous appellerons involution de CARTAN d'un groupe H un automorphisme involutif θ de H qui possède la propriété suivante : si J est l'ensemble des $x \in H$ tels que $\theta(x) = x^{-1}$, l'application $x \mapsto x^2$ induit une bijection de J sur J. On voit alors facilement que, si K est le groupe des points fixes de θ, l'application $(x,y) \mapsto xy$ de $K \times J$ dans H est bijective (on reconnait la situation que l'on rencontre dans la théorie des sous-groupes compacts maximaux des groupes de Lie, d'où le nom d'involution de Cartan). Si H est un groupe fini d'ordre impair, l'application $x \mapsto x^2$ de H dans H est bijective ; on voit alors facilement que tout automorphisme involutif de H est une involution de CARTAN. Nous admettrons le lemme suivant (dû à R. BRAUER et généralisé par WIELANDT ([5]) :

Lemme 3. *Soient* H *un groupe,* Θ *un sous-groupe abélien de type* $(2,2)$ *de* Aut H, θ_1, θ_2 *et* $\theta_3 = \theta_1\theta_2$ *les éléments* $\neq 1$ de Θ, K_h *le groupe des points fixes de* θ_h. *Supposons que* $\theta_1, \theta_2, \theta_3$ *soient des involutions de CARTAN et que* $K_1 \cap K_2 \cap K_3 = \{1\}$. *Alors, si* $h' \neq h$, θ_h *transforme les éléments de* $K_{h'}$ *en leurs inverses ; l'application* $(x_1,x_2,x_3) \mapsto x_1x_2x_3$ *est une bijection de* $K_1 \times K_2 \times K_3$ *sur* A.

Soient $\iota_1, \iota_2, \iota_3$ les éléments $\neq 1$ de T. Comme $\mathcal{L}_G(T)$ est d'ordre 8, on a $\mathcal{L}_G(T) \cap M = \{1\}$, et T est représenté fidèlement comme groupe d'automorphismes de M ; comme M est d'ordre impair, les éléments $\iota_h (1 \leq h \leq 3)$ définissent des involutions de CARTAN de M. Nous posons $M_h = M \cap \mathcal{L}_G(\iota_h)$ $(1 \leq h \leq 3)$; M_h est un sous-groupe d'ordre impair de $\mathcal{L}_G(\iota_h)$, donc isomorphe à un sous-groupe d'ordre impair de $\mathfrak{A}_5$; il en résulte aussitôt que l'ordre p_h de M_h est 1, 3 ou 5.

Lemme 4. *Soient* p *un nombre premier* $\neq 2$ *et* P *un* p-*sous-groupe* $\neq \{1\}$ *de* G *normalisé par* T. *Si* $\mathcal{N}_G(P) \cap \mathcal{N}_G(T)$ *est d'ordre* $\not\equiv 0$ (*mod.* 3), *les éléments d'ordres impairs de* $\mathcal{N}_G(P)$ *forment un sous-groupe distingué* M' *de* $\mathcal{N}_G(P)$ *et on a* $\mathcal{N}_G(P) = M'T$; *si on suppose de plus que* P *est un sous-groupe distingué de* M, *on a* $M' = M$. *La condition que l'ordre de* $\mathcal{N}_G(P) \cap \mathcal{N}_G(T)$ *soit* $\not\equiv 0$ (mod 3) *est satisfaite si les groupes* $P \cap \mathcal{L}_G(\iota_h)$ $(h = 1,2,3)$ *ne sont pas tous du même ordre.*

Si l'ordre de $\mathcal{N}_G(P) \cap \mathcal{N}_G(T)$ est $\equiv 0$ (mod 3), $\mathcal{N}_G(P)$ contient un élément λ d'ordre 3 de $\mathcal{N}_G(T)$; on sait que cet élément n'est pas dans $\mathcal{L}_G(T)$, de sorte que l'automorphisme intérieur Int λ permute transitivement $\iota_1, \iota_2, \iota_3$, donc aussi les groupes $P \cap \mathcal{L}_G(\iota_h)$ $(h = 1,2,3)$, ce qui démontre la dernière assertion. Supposons que l'ordre de $U = \mathcal{N}_G(P) \cap \mathcal{N}_G(T)$ soit $\not\equiv 0$ (mod 3) ;

comme $\mathcal{N}_G(T)/T$ est d'ordre 6, U/T est d'ordre 1 ou 2 ; s'il était d'ordre 2, U serait un 2-groupe de SYLOW de G, et normaliserait le groupe P d'ordre impair ; ce qui est impossible (lemme 2). Donc $U = T$ et T est le centre de son normalisateur dans $\mathcal{N}_G(P)$. Il en résulte que $\mathcal{N}_G(P)$ admet un sous-groupe distingué M' d'ordre impair tel que $\mathcal{N}_G(P) = M'T$ (th. de BURNSIDE, [3], p. 203) ; il est clair que M' est l'ensemble des éléments d'ordres impairs de $\mathcal{N}_G(P)$. Si P est un sous-groupe distingué de M, on a $M \subseteq \mathcal{N}_G(P)$, d'où $M \subset M'$; comme M' est normalisé par T, il résulte du caractère maximal de M que $M' = L$.

Lemme 5. <u>Si</u> $p_1 = p_2$, M_1 et M_2 <u>sont conjugués dans</u> G.

Les involutions de G étant conjuguées, il existe un élément $g \in G$ tel que $g\iota_2 g^{-1} = \iota_1$; M_1 et gM_2g^{-1} sont des sous-groupes de même ordre impair de $\mathcal{L}_G(\iota_1)$. Comme deux sous-groupes de même ordre impair de $\mathfrak{A}_5$ sont conjugués, il en résulte que M_1 et gM_2g^{-1} sont conjugués dans $\mathcal{L}_G(\iota_1)$.

Lemme 6. <u>Il est impossible que l'on ait</u> $p_1 = p_2 > 1$, $p_3 \neq p_1$.

Supposons le contraire, et soit alors P un p_1-groupe de SYLOW de M, donc d'ordre p_1^2 et par suite abélien. Montrons que P est distingué dans M. Sinon, P serait le centre de son normalisateur dans M ; M admettrait donc un sous-groupe distingué Q tel que $Q \cap P = \{1\}$, $M = PQ$, et Q serait d'ordre p_3 ; mais un groupe d'ordre 3 (resp. 5) n'admet aucun automorphisme d'ordre 5 (resp. 3) ; Q serait donc dans le centre de M et M serait abélien, d'où contradiction. Le groupe P, étant le seul p_1-groupe de SYLOW de M, est normalisé par T ; lui appliquant le lemme 3, on voit que $P = M_1M_2$. Comme P est abélien, ses éléments sont transformés en leurs inverses par ι_3, d'où $P \cap \mathcal{L}_G(\iota_3) = \{1\}$; il résulte alors du lemme 4 que $\mathcal{N}_G(P) = MT$. En particulier, $\mathcal{N}_G(P)/P$ est d'ordre premier à p_1, ce qui implique que P_1 est un p_1-groupe de SYLOW de G. Les groupes M_1, M_2, qui sont distingués dans P et conjugués dans G, sont conjugués dans $\mathcal{N}_G(P) = MT$ ([3], p. 203), donc dans M puisqu'ils sont normalisés par T. Or on a $M = M_3P$; il existe donc un élément x_3 de M_3 tel que l'on ait, pour tout $x_1 \in M_1$, $x_2 = x_3x_1x_3^{-1} \in M_2$. Transformant par ι_1, on a

$x_2^{-1} = x_3^{-1}x_1x_3$, d'où $x_3x_2x_3^{-1} = x_1^{-1}$ et x_3^4 commute aux éléments de M_1 ; comme x_3 est d'ordre impair, il commute aux éléments de M_1, d'où contradiction (car $M_1 \neq M_2$).

Lemme 7. <u>Supposons que</u> M <u>soit d'ordre</u> 3, 5 <u>ou</u> 15 ; <u>il est alors cyclique</u>. <u>Si</u> p <u>est un facteur premier de son ordre et</u> P_p <u>son unique sous-groupe d'ordre</u> p, <u>on a</u> $\mathcal{N}_G(P_p) = \mathcal{N}_G(M) = MT$; <u>l'ordre de</u> G <u>est</u> $\not\equiv 0 \pmod{p^2}$. <u>Si</u> M <u>est d'ordre</u> 15, T <u>est engendré par deux involutions dont l'une commute aux éléments de</u> P_3 <u>et transforme ceux de</u> P_5 <u>en leurs inverses tandis que l'autre commute aux éléments de</u> P_5 <u>et transforme ceux de</u> P_3 <u>en leurs inverses</u>.

La première assertion résulte de ce que M est résoluble et de ce qu'un groupe d'ordre 3 (resp. 5) n'admet pas d'automorphisme d'ordre 5 (resp. 3). On peut choisir les notations de telle manière que $M_1 = P_p$ et $M = M_1M_2$ si M est d'ordre 15. Il est clair que les groupes $P_p \cap \mathcal{L}_G(\iota_h)$ (h = 1,2,3) ne sont pas tous de même ordre, et de même pour les groupes $M \cap \mathcal{L}_G(\iota_h)$. On a donc $\mathcal{N}_G(P_p) = \mathcal{N}_G(M) = MT$ (lemme 4). L'ordre du groupe $\mathcal{N}_G(P_p)/P_p$ étant $\not\equiv 0 \pmod{p}$, P_p est un p-groupe de SYLOW de G et l'ordre de G est $\not\equiv 0 \pmod{p^2}$. La dernière assertion résulte du lemme 3.

Lemme 8. <u>Supposons que</u> M <u>soit d'ordre</u> p^3, p <u>premier</u>. <u>On a alors</u> p = 3. Nous omettrons la démonstration de ce lemme.

3) <u>Simplicité du groupe</u> G.

Soit H un sous-groupe distingué de G.

1) Supposons d'abord H d'ordre impair. Si ι est une involution de G, on a $H \cap \mathcal{L}(i) = \{1\}$, car $\mathcal{L}(\iota)$ n'admet aucun sous-groupe distingué d'ordre impair $\neq \{1\}$. Donc ι induit un automorphisme sans élément fixe $\neq 1$ de H, un tel automorphisme transforme tout élément de H en son inverse.

Si ι_1, ι_2 sont des involutions distinctes de G qui commutent entre elles, $\iota_1\iota_2$ est une involution et commute aux éléments de H ; ces derniers sont donc leurs propres inverses, d'où $H = \{1\}$.

2) Supposons G/H d'ordre impair. Comme $\mathcal{L}_G(\iota)$ n'a pas de sous-groupe distingué $\neq \mathcal{L}_G(\iota)$ d'indice impair, on a $\mathcal{L}_G(\iota) \subset H$. Soit H' l'intersection des sous-groupes distingués d'indice 2 de H ; H' est donc distingué dans G . Un 2-groupe de SYLOW S de G est contenu dans H. Si $S \cap H' = \{1\}$, H' est d'ordre impair, d'où $H' = \{1\}$; H est alors un 2-groupe, d'où $H = S$; or S n'est pas distingué dans G (car il ne l'est pas dans le centralisateur de l'une de ses involutions). On a donc $S \cap H' \neq \{1\}$; comme toutes les involutions de G sont conjuguées, on a $S \subset H'$ et H/H' est d'ordre impair ; comme c'est un 2-groupe, on a $H' = H$. Le groupe H possède donc les propriétés 1), 2), 3) du groupe G. Il en résulte que les involutions de G, qui sont dans H, sont conjuguées dans H ; si ι est l'une d'elles, on a $G = H\mathcal{L}_G(\iota) = H$ puisque $\mathcal{L}_G(\iota) \subset H$.

3) Considérons maintenant le cas général . Si $H \neq \{1\}$, $H \neq G$, H et G/H seraient d'ordres pairs ; si S est un 2-groupe de SYLOW de G, on aurait $H \cap S \neq \{1\}$, $H \cap S \neq S$; or c'est impossible, toutes les involutions de G étant conjuguées ; G est donc simple.

II - Application de la théorie des caractères.

1) La méthode de SUZUKI.

Si G est un groupe fini, nous noterons Φ_G l'espace vectoriel des fonctions centrales sur G (à valeurs dans $\mathbb{C}$). Cet espace est muni d'une structure hilbertienne dont le produit scalaire est donné par la formule

$$(f|g)_G = [G]^{-1} \sum_{s\in G} f(s)\bar{g}(s) \ .$$

Les caractères irréductibles de G forment une base orthonormée de Φ_G.

Si H est un sous-groupe de G et $f \in \Phi_H$, on appelle fonction induite par f sur G, et on désigne par f^G, la fonction définie par la formule

$$f^G(s) = [H]^{-1} \sum_{t\in G} \widetilde{f}(tst^{-1})$$

où $\widetilde{f}$ est la fonction qui prolonge f et qui est nulle en dehors de H. Si χ est un caractère irréductible de H, χ^G est un caractère (en général non irréductible) de G. Pour toute fonction centrale F sur G, on a

$$(F|f^G)_G = (F_{/H}|f)_H \ ,$$

où F_H est la restriction de F à H.

La méthode de SUZUKI pour étudier les relations entre G et H consiste en l'utilisation de certains sous-espaces Ψ de Φ_H tels que la restriction à Ψ de l'application $f \to f^G$ soit isométrique. Appelons ensemble de SUZUKI (pour G et H) une partie Σ de H qui possède les propriétés suivantes : Σ est réunion de classes d'éléments conjugués ; si $s\in\Sigma$, tout élément t de G tel que $tst^{-1}\in\Sigma$ est dans H. Soit Σ un ensemble de SUZUKI, et soit Ψ l'espace des fonctions centrales sur H nulles en dehors de Σ. On voit tout de suite que la condition $f \in \Psi$ entraîne $(f^G)_{/\Sigma} = f_{/\Sigma}$; il en résulte que l'on a alors $(f^G|f'^G)_G = (f|f')_H$ pour tout $f' \in \Psi$. L'orthogonal $\Psi^\perp$ de Ψ se compose des fonctions centrales nulles sur Σ. Soient $(f_1,\ldots,f_p)$ et $(f_{p+1},\ldots,f_{p+q})$ des bases de Ψ et $\Psi^\perp$; désignant par $\mu_1,\ldots,\mu_n$ les caractères irréductibles de G, soit

$$f_i^G = \sum_{j=1}^n b_{ji}\, \mu_j \ ;$$

on a alors

(1) $\sum_{j=1}^{n} b_{ji}\, \bar{b}_{ji'} = (f_i | f_{i'})_H$.

De plus, si $(\mu_j)_{/H} = \sum_{k=1}^{p} c_{kj}\, f_k + \sum_{k=1}^{q} c_{kj}^{1}\, f_{p+k}$, on a

(2) $\sum_{k=1}^{p} c_{kj}(f_k | f_\ell)_H = ((\mu_j)_{/H} | f_\ell)_H = (\mu_j | f_L^G) = \bar{b}_{j\ell}$ $(1 \leq \ \leq p)$.

En pratique, on sera en général dans le cas où on peut prendre pour $f_1,\dots,f_p$ des caractères généralisés (i.e. des combinaisons linéaires à coefficients entiers des caractères irréductibles de H) ; les b_{ji} seront alors des entiers sur les valeurs desquels les relations (1) donneront des renseignements d'autant plus précis que les nombres $|(f_i | f_{i'})_H|$ sont petits. Une fois ces nombres connus, les relations (2) permettent de déterminer les c_{kj} , i.e. les restrictions des μ_j à Σ .

En liaison avec cette méthode, on utilise généralement (notamment en vue de la détermination de l'ordre de G) une autre formule que nous allons maintenant décrire. Nous identifierons une partie du groupe G à la somme de ses éléments dans l'algèbre de groupe $\mathbb{Z}[G]$. Soit I l'ensemble des involutions ; on a alors dans $\mathbb{Z}[G]$ une formule de la forme $I^2 = \sum c(K)K$, la somme étant étendue aux classes d'éléments conjugués de G . Si d_j est le degré de μ_j , on voit (en utilisant le fait qu'une représentation de caractère μ_j définit un homomorphisme de $\mathbb{Z}[G]$ qui applique les éléments du centre sur des scalaires) que l'on a $d_j^{-1}(\mu_j(I))^2 = \sum_K c(K)\mu_j(K)$ (μ_j étant étendue de manière évidente en une fonction centrale sur $\mathbb{Z}[G]$). Appliquant les secondes relations d'orthogonalité et observant que $\mu_j(K) = \bar{\mu}_j(K)$ si $c(K) \neq 0$, on obtient la formule

$$c(K) = [G]^{-1} \sum_j d_j^{-1}(\mu_j(I))^2\, \mu_j(s) \qquad \text{si } s \in K .$$

Soit maintenant Σ un ensemble de SUZUKI pour H et G tel que la condition $s \in \Sigma$ entraîne $s^{-1} \in \Sigma$, et soit J la somme des involutions de H ; soit $J^2 = \Sigma_L\, c'(L)L$, la somme étant étendue aux classes d'éléments conjugués de H . Si l'une de ces classes L est contenue dans Σ et si

K est la classe de G qui contient L, on a $c(K) = c(L)$ comme il résulte de ce que les involutions j de H ou de G qui interviennent dans une représentation $s = jj'$ de s comme produit d'involutions sont celles qui transforment s en s^{-1}. Soient $\lambda_1, \ldots, \lambda_m$ les caractères irréductibles de H et d_i^1 le degré de λ_i ; les fonctions $[G]^{-1} \sum_j d_j^{-1} (\mu_j(I))^2 (\mu_j)_{/H}$ et $[H]^{-1} \sum_i d_i^{1-1} (\lambda_i(J))^2 \lambda_i$

coïncident donc sur $\sum$. Il en résulte que, si f est une fonction centrale sur H nulle en dehors de $\sum$ et si $f = \sum_i a_i \lambda_i$, $f^G = \sum_j b_j \mu_j$, on a

$$\boxed{[G]^{-1} \sum_j d_j^{-1}(\mu_j(I))^2 b_j = [H]^{-1}\sum_i d_i^{1-1}(\mu_i(J))^2 a_i} \quad .$$

C'est cette formule que nous appellerons la formule de SUZUKI.

2) Application au groupe de JANKO.

Soit G un groupe possédant les propriétés 1), 2), 3) énoncées au début, et soit H le centralisateur d'une involution ι. Soient R l'ensemble des éléments 2-réguliers de H et $\sum = \iota R$; $\sum$ est alors un ensemble de SUZUKI pour H et G. Cet ensemble est en effet stable par les automorphismes intérieurs de H ; si r, r' sont des éléments 2-réguliers de H et si g est un élément de G tel que $g(\iota r)g^{-1} = \iota r'$, r et r' sont de même ordre m, on a $(\iota r)^m = (\iota r')^m = \iota$ et $g\iota g^{-1} = \iota$, d'où $g \in H$. On construit facilement une base $(\phi_1, \ldots, \phi_4)$ de l'espace des fonctions centrales sur H nulles en dehors de $\sum$. En décomposant en caractères irréductibles les caractères généralisés ϕ_i^G $(1 \leq i \leq 4)$, on obtient 10 caractères irréductibles distincts μ_i $(0 \leq i \leq 9)$ (avec $\mu_o = 1$) qui interviennent dans les ϕ_i^G avec des coefficients égaux à ± 1 (liés d'ailleurs par un certain nombre de relations). Utilisant la formule (2), on peut exprimer en fonction de ces coefficients les valeurs des μ_i en les éléments de $\sum$.

Soit maintenant N le normalisateur d'un sous-groupe V d'ordre 5 de H. On sait que N est d'ordre 20 ou 60, et il est facile de calculer les caractères irréductibles de N. On applique alors la méthode de SUZUKI au groupe N.

Si N est d'ordre 20, soit V^* l'ensemble des éléments $\neq 1$ de V, et soit

$\Sigma' = V^* \cup \iota V^*$. Alors Σ' est un ensemble de SUZUKI pour N et G comme il résulte tout de suite de ce que V est engendré par tout élément de V^* et aussi par le carré de tout élément de ιV^*. L'espace des fonctions centrales sur N nulles en dehors de V^* a une base de 4 éléments $\Psi_1,\ldots,\Psi_4$. Les Ψ_i^G s'écrivent comme combinaisons linéaires à coefficients égaux à ± 1 de μ_0 et de 7 caractères irréductibles $\xi_1,\ldots,\xi_7$, dont on peut calculer les valeurs sur Σ'. Cependant, comme Σ' ne contient aucune involution, ces valeurs ne permettent pas encore d'écrire le premier membre des formules de SUZUKI pour les Ψ_i (car cela exige la connaissance des valeurs des ξ_i sur une involution). Mais l'ensemble Σ' a en commun l'ensemble ιV^* avec l'ensemble Σ précédemment introduit, ce qui permet de comparer les valeurs en un élément $s \in \iota V^*$ des ξ_i et des μ_j. On sait que tout caractère irréductible ξ distinct de μ_0 et des ξ_i est nul en s ; comme 7 des caractères μ_i prennent des valeurs $\neq 0$ en s, il en résulte que $\{\xi_1,\ldots,\xi_7\} \subset \{\mu_1,\ldots,\mu_9\}$.

De plus, la comparaison des valeurs en s des ξ_i et des μ_j, jointe au fait qu'on a certaines relations entre les degrés des ξ_j dues à ce que l'on a $\Psi_i^G(1) = 0$ $(1 \leq i \leq 4)$, permet d'obtenir assez de renseignements sur la manière dont les ξ_i se répartissent parmi les μ_j pour calculer les nombres $\xi_i(\iota)$. On peut alors appliquer la formule de SUZUKI à l'une, convenablement choisie, des fonctions Ψ_i ; on obtient ainsi une relation qui fait intervenir l'ordre de G et deux entiers m,ζ dont l'un est > 0 et l'autre ± 1. Sachant que l'ordre de G est de la forme $2^3.5.7.r$, où r est premier à 10, on constate par des raisonnements d'arithmétique élémentaire que la relation obtenue conduit à une impossibilité. L'ordre de N est donc 60. Ici encore, on peut calculer sans difficulté les caractères irréductibles de N. Si Σ' est maintenant l'ensemble des éléments de N dont les ordres sont soit impairs soit égaux à 6 ou à 10, Σ' est un ensemble de SUZUKI. On procède alors exactement comme dans le cas précédent, et on trouve cette fois une relation qui permet de déterminer complètement l'ordre $[G]$ de G :

$$[G] = 2^3.3.5.7.11.19 \quad .$$

De plus, on détermine en même temps les degrés de deux des représentations ξ_i. Appliquant maintenant la formule de SUZUKI aux caractères généralisés ψ_1, ψ_2, ψ_3 du centralisateur de ι, on parvient à déterminer les degrés de toutes les représentations μ_i ; on trouve qu'il y en a une de degré 1, deux de degré 76, trois de degré 77, trois de degré 133, une de degré 209.

3) Normalisateurs des groupes de SYLOW.

Si p est un nombre premier, soit S_p un p-groupe de SYLOW de G. Si $p = 2$, on sait déjà que $\mathcal{N}_G(S_p)/S_p$ est d'ordre 21. On voit facilement que ce groupe n'est pas abélien ; il admet donc un sous-groupe distingué d'indice 7. (car un groupe d'ordre 3 n'admet pas d'automorphisme d'ordre 7). On en déduit que, si T est un sous-groupe d'ordre 7 de $\mathcal{N}_G(S_p)$, il est impossible que T soit son propre normalisateur dans $\mathcal{N}_G(S_p)$, ce qui montre que $\left[\mathcal{N}_G(S_7)\right] \equiv 0 \pmod 3$. Par ailleurs, $\mathcal{N}_G(S_7) \not\equiv 0 \pmod 5$ car un élément d'ordre 5 qui normaliserait S_7 le centraliserait, et on sait que $\left[\mathcal{N}_G(S_5)\right] = 60$. On a aussi $\left[\mathcal{N}_G(S_7)\right] \not\equiv 0$ (mod 4) car un groupe d'ordre 4 ne normalise aucun groupe d'ordre 7. Sachant que l'indice de $\mathcal{N}_G(S_7)$ dans G est $\equiv 1 \pmod 7$, on trouve alors que la seule possibilité est $\left[\mathcal{N}_G(S_7)\right] = 42$; le groupe $\mathcal{N}_G(S_7)/S_7$ est cyclique d'ordre 6.

On a, comme dans le cas précédent, $\left[\mathcal{N}_G(S_{11})\right] \not\equiv 0 \pmod 4$. Comme S_{11} n'a ni automorphisme d'ordre 3 ni automorphisme d'ordre 7, $\left[\mathcal{N}_G(S_{11})\right]$ n'est divisible ni par 4 ni par 5 ni par 11. Comme l'indice de $\mathcal{N}_G(S_{11})$ est $\equiv 1 \pmod{11}$, on trouve qu'il en résulte que $\left[\mathcal{N}_G(S_{11})\right] = 11 \times 10$; $\mathcal{N}_G(S_{11})/S_{11}$ est cyclique d'ordre 10.

On voit par la même méthode que $\left[\mathcal{N}_G(S_{19})\right] = 19 \times 6$; $\mathcal{N}_G(S_{19})/S_{19}$ est cyclique d'ordre 6.

Les résultats précédents permettent de déterminer les classes d'éléments conjugués. Il y en a 15 qui se répartissent ainsi : la classe de 1 ; pour $n = 2,3,6,7$, une classe d'éléments d'ordre n ; pour $n = 5, 10, 15$, 2 classes d'éléments d'ordre n ; pour $n = 19$, 3 classes d'éléments d'ordre n.

4) Détermination de tous les caractères.

On a déjà déterminé 10 caractères $\mu_0,\ldots,\mu_9$ de G ainsi que leurs valeurs en les éléments qui centralisent des involutions. Comme il y a 15 classes d'éléments conjugués, il reste 5 caractères $\mu_{10},\ldots,\mu_{14}$ à déterminer. Il faut pour cela utiliser la théorie des caractères modulaires.

Le groupe G comporte 5 classes 2-régulières de défaut 0 (les classes d'éléments d'ordres 7, 11, 19) ; il admet 5 caractères irréductibles de 2-défaut 0, donc de degrés $\equiv 0 \pmod 8$. Comme aucun des degrés de $\mu_0,\ldots,\mu_9$ n'est $\equiv 0 \pmod 8$, ceux de $\mu_{10},\ldots,\mu_{14}$ le sont. Par ailleurs, si p est un diviseur premier $\neq 2$ de l'ordre de G, l'ordre de G est $\not\equiv 0 \pmod{p^2}$, de sorte que les caractères de p-défaut 1 sont exactement ceux dont les degrés sont $\not\equiv 0 \pmod p$. Or le nombre de ces caractères est égal au nombre de classes d'éléments conjugués de $\mathfrak{N}(S_p)$ ([1], th. 8). On en déduit que, parmi les degrés de $\mu_{10},\ldots,\mu_{14}$, il y en a 3 qui sont $\equiv 0 \pmod 3$, 3 qui sont $\equiv 0 \pmod 5$, 2 qui sont $\equiv 0 \pmod 7$, aucun qui soit $\equiv 0 \pmod{11}$ ou $\pmod{19}$.

Ces renseignements, joints au fait que la somme des carrés des degrés de $\mu_0,\ldots,\mu_{14}$ est $[G]$, suffisent à déterminer les degrés de $\mu_{10},\ldots,\mu_{14}$, que l'on trouve être 56, 56, 120, 120, 120.

Les caractères $\mu_{10},\ldots,\mu_{14}$, étant de 2-défaut 0, sont nuls sur l'ensemble des éléments 2-singuliers de G.

Les autres valeurs des caractères se déterminent en appliquant la méthode de SUZUKI aux sous-groupes $\mathfrak{N}_G(S_p)$ de G ($p = 3, 7, 11, 19$). Si $p = 3$, on prend comme ensemble de SUZUKI l'ensemble des éléments de $\mathfrak{N}_G(S_p)$ dont les ordres sont $\neq 1, 2$; (c'est un ensemble de SUZUKI parce que $\mathfrak{N}_G(S_3)$ est aussi le normalisateur de son unique sous-groupe d'ordre 5). Si $p = 7$ ou 11, on prend pour ensemble de SUZUKI l'ensemble des éléments $\neq 1$ de S_p. Si $p = 19$, on applique la théorie des caractères exceptionnels, qui peut être considérée comme un cas particulier de la méthode de SUZUKI.

5) Unicité du groupe G.

Elle se démontre en construisant une représentation de degré 7 sur un corps

K à 11 éléments. Pour ce faire, on utilise bien entendu la théorie des caractères 11-modulaires. Les représentations de degrés $\equiv 0 \pmod{11}$ donnent des représentations simples sur le corps K.

Les caractères ordinaires dont les degrés sont $\not\equiv 0 \pmod{11}$ et les caractères de BRAUER pour $p = 11$ peuvent, en vertu de résultats de BRAUER, s'arranger les premiers en une suite $(\theta_1,\ldots,\theta_{11})$, les seconds en une suite $(\rho_1,\ldots,\rho_{10})$ de telle manière que la restriction de θ_i à l'ensemble des éléments 11-réguliers soit ρ_1 si $i = 1$, ρ_{10} si $i = 11$, $\rho_{i-1} + \rho_i$ si $1 < i < 11$. On connaît l'ensemble $\{\theta_1,\ldots,\theta_{11}\}$; il reste à savoir comment ordonner cet ensemble de la manière indiquée par BRAUER. JANKO arrive par divers arguments à éliminer toutes les possibilités sauf une ; on peut alors calculer les degrés et les caractères modulaires des diverses représentations 11-modulaires de G ; l'une d'elles, soit ρ, est de degré 7. L'unicité du groupe G s'établit alors en construisant l'image $\rho(G)$ de ce groupe.

On voit facilement que ρ induit une représentation simple ρ_N du normalisateur N d'un 2-groupe de SYLOW S_2. Comme l'ordre de N est $\not\equiv 0 \pmod{11}$, ρ_N est obtenu par réduction $\pmod{11}$ à partir d'une représentation ordinaire simple de degré 7 de N, ce qui permet d'expliciter, pour une base convenable de l'espace de représentation, le groupe $\rho(N)$. Le goupe N contient des opérations σ_3, σ_7 telles que $\sigma_3\,\sigma_7\,\sigma_3^{-1} = \sigma_7^2$. Il résulte de ce que l'on sait sur la structure des normalisateurs des groupes d'ordre 7 qu'il existe une involution ι de G qui commute à σ_3 et qui transforme σ_7 en σ_7^{-1} ; il est clair que $\iota \in N$. Par ailleurs, σ_3 commute avec au moins une involution $\iota' \in S$. Or $\mathcal{C}_G(\sigma_3)$ est d'ordre 3, et, si ι est une de ses involutions, les autres sont les $\sigma_5^k\,\iota$, où σ_5 est un élément d'ordre 5 de $\mathcal{C}_G(\sigma_3)$; on en conclut que $(\iota'\iota)^5 = 1$. JANKO montre que les conditions auxquelles satisfait ι suffisent à déterminer la matrice $\rho(\iota)$. Or on voit facilement que G est engendré par S et ι ; ceci montre que G est isomorphe au groupe engendré par deux matrices à coefficients dans $\mathbb{Z}/11\mathbb{Z}$ que l'on peut écrire explicitement, ce qui achève la démonstration d'unicité.

6) <u>Plongement dans</u> G_2 .

L'existence d'un tel plongement est attribuée, dans le mémoire de JANKO , à W.A. COPPEL. Elle se démontre en donnant explicitement une matrice qui transforme les éléments de $\rho(N)$ (les notations étant celles de 5)) en matrices appartenant au groupe G_2 . On peut d'ailleurs aussi démontrer l'existence de ce plongement à partir de la connaissance des divers caractères 11-modulaires. On peut également montrer qu'il n'existe qu'une seule classe de plongements de G dans G_2 .

B I B L I O G R A P H I E

[1] R. BRAUER - On groups whose order contains a prime number to the first power, Amer. Journ. of Math., 64, 1942.

[2] R. BRAUER - FOWLER.- On groups of even order, Ann. of Math., 62, 1955.

[3] M. HALL - The theory of groups (Macmillan, New-York).

[4] JANKO - A new finite simple group with abelian Sylow 2-subgroups and its characterization, Journ. of Algebra, 3, 1966.

[5] WIELANDT - Beziehungen zwischen d. Fixpunktzahlen von automorphismengruppen einer endliche gruppe, Math. Zeit., 73, 1960.