DIAGRAMMES

ZIANI NOUACER

Caractères et sous-groupes des groupes de Suzuki

Diagrammes, tome 8 (1982), exp. n° 3, p. ZN1-ZN29

<http://www.numdam.org/item?id=DIA_1982__8__A3_0>

Diagrammes, Volume 8, Paris 1982.

CARACTERES ET SOUS-GROUPES DES GROUPES DE SUZUKI

par

Ziani Nouacer

Cet article rassemble les résultats exposés par moi-même au Séminaire Broué-Enguehard, en 1980, à l'Université Paris 6, et dont le thème était "Les groupes finis de type de Lie". Il était sans doute utile de rassembler dans un seul texte les résultats les plus marquants concernant les groupes de Suzuki, jusqu'ici assez épars dans la littérature , et ceci devrait inciter le lecteur à consulter aussi les textes originaux de Ito, Feit et Suzuki , cités en référence à la fin de l'introduction.

INTRODUCTION.

Les travaux sur les groupes de Suzuki ont joué un grand rôle dans la classification des groupes finis (simples). Le premier grand résultat fut démontré en 1957 par Suzuki; voici l'énoncé:

Soit G un groupe fini d'ordre pair. Si le centralisateur de toute involution de G est abélien, alors le groupe G vérifie l'une des trois propriétés suivantes:

(i) Les 2-sous-groupes de Sylow de G sont cycliques.

(ii) Le groupe G possède un seul 2-sous-groupe de Sylow, qui sera par suite normal dans G.

(iii) Le groupe G est le produit direct d'un groupe abélien

d'ordre impair et du groupe $SL(2,2^n)$ pour un certain entier n, groupe des matrices 2x2 de déterminant 1 sur le corps à 2^n éléments.

Avant d'énoncer le deuxième grand résultat de classification qui justifie l'intérêt porté aux groupes de Suzuki, on rappellera deux définitions nécessaires à la formulation de cet énoncé.

DEFINITION d'un groupe de FROBENIUS.

Un groupe H est dit groupe de Frobenius de noyau S lorsque S est un sous-groupe propre de H, normal dans H, vérifiant la propriété suivante:

pour tout élément u de S différent de l'élément neutre 1, on a l'inclusion $C_H(u) \subset S$, $C_H(u)$ désignant le centralisateur de u dans H.

On montre alors trivialement que S est unique, qu'il existe un sous-groupe M de H tel que H soit le produit semi-direct de S par M, soit $H = S \rtimes M$. De plus, le sous-groupe M vérifie : $(uMu^{-1}) \cap M = \{1\}$ pour tout u appartenant à H mais non à M.

Tout sous-groupe conjugué à M est appelé sous-groupe de Frobénius de H.

DEFINITION d'un groupe de ZASSENHAUSS.

Un groupe fini G opérant sur un ensemble E est dit groupe de Zassenhauss si G est doublement transitif sur E et si le fixateur d'un point de E est un groupe de Frobénius.

On peut maintenant énoncer le deuxième grand résultat de classification sous la forme suivante :

Si G est un groupe de Zassenhauss, et si le noyau du fixateur d'un point est un 2-groupe abélien, alors le groupe G est un groupe de Suzuki.

Ce résultat a fait espérer, dans les années 60 et au début des années 70, que le problème de la classification des groupes finis se ramènerait à l'étude de la multiple-transitivité de leurs actions sur des ensembles bien choisis ...

En tout cas, le fait que les groupes de Suzuki soient des groupes de Zassenhauss interviendra d'une manière essentielle, comme nous le verrons dans ce qui suit, dans l'obtention des caractères de ces groupes.

REFERENCES originales sur le sujet.

N.ITO, Notes polycopiées du cours professé à l'Université de l'Illinois, 1968-1969.

W.FEIT A characterization of the simple groups $SL(2,2^a)$, Amer.Journal of Math., Vol. 82, 1960, pp 281-300.

M.SUZUKI On characterizations of linear groups, I , II, Trans.Amer.Math.Soc.,Vol. 92,1959, pp 191-219.

M.SUZUKI On characterizations of linear groups, III, Nagoya Math. J. 21, pp 159-183.

M.SUZUKI On a class of doubly transitive groups, Ann.of Math. , Vol. 75, 1962, pp 105-145.

On pourra consulter aussi les références citées en finale.

1. PRELIMINAIRES.

A. Résultats classiques souvent utilisés dans ce qui suit.

PROPOSITION 1. (cf. (E.B.))

Soit E un ensemble sur lequel G opère transitivement et soit X le caractère de la représentation linéaire associée. Le rang de l'opération de G sur E est égal à $(X,X)_G$. En particulier G est deux fois transitif sur E si et seulement si $(X,X)_G = 2$, et l'on a alors $X = 1_G + \lambda$, où λ est un caractère irréductible de G.

DEFINITION. Soit π un ensemble de nombres premiers et soient G un groupe fini et H un sous-groupe de G. On dit que H contrôle la fusion des π-sous-groupes nilpotents de G (ou que H est un sous-groupe de π-nil-contrôle de G) si les deux conditions suivantes sont satisfaites:

(1) H contient un conjugué de tout π-sous-groupe nilpotent de G,

(2) Si P est un π-sous-groupe nilpotent de H et si $x \in G$ est tel que $P^x = xPx^{-1} \subset H$, il existe $y \in H$ et $z \in C_G(P)$ tels que $x = zy$.

DEFINITION. Pour tout groupe fini G et tout ensemble de nombres premiers π , on note $ZF(G,\pi)$ (resp. $R(G,\pi)$) l'espace vectoriel des fonctions centrales sur G qui prennent même valeur sur un élément s que sur sa π-composante s_π (resp. le $\underline{Z}$-module des caractères généralisés de G qui appartiennent à $ZF(G,\pi)$).

Le $\underline{Z}$-module des caractères généralisés de G sera noté R(G). L'ensemble des caractères irréductibles de G sera noté Irr(G).

PROPOSITION 2. (cf. (E.B.))

Si H est un sous-groupe de π-nil-contrôle de G, les applications Res_H^G , restriction d'un caractère de G à H, et Pro_H^G , prolongement d'un caractère de H à G, induisent des isométries

inverses l'une de l'autre entre $R(G,\pi)$ et $R(H,\pi)$.

PROPOSITION 3. (cf. (E.B.))

Si H est un groupe de Frobénius et si $H = S \rtimes M$, alors on a les égalités suivantes:

(1) $\mathrm{Irr}(H) = \{\mathrm{Pro}_M^H X \mid X \in \mathrm{Irr}(M)\} \cup \{\mathrm{Ind}_S^H Y \mid Y \in (\mathrm{Irr}(S)-\{1_S\})\}$,

$$|\mathrm{Pro}_M^H \mathrm{Irr}(M)| = |\mathrm{Irr}(M)| \ , \ |\mathrm{Ind}_S^H(\mathrm{Irr}(S)-\{1_S\})| = (|\mathrm{Irr}(S)|-1)/|M|,$$

où Ind_S^H désigne l'induction de S à H.

(2) $R(H,\pi(S)) = \underline{Z}.1_H \oplus (\mathrm{Ind}_S^H(R(S)))^\circ$,

où $\pi(S) = \{p \text{ premier} \mid p \mid |S|\}$ et $(\mathrm{Ind}_S^H(R(S)))^\circ$ est le sous-groupe de $\mathrm{Ind}_S^H(R(S))$ formé des éléments de degré zéro (c'est-à-dire nuls sur l'élément neutre).

Remarque. Dans la suite, quand il n'y a pas d'ambiguité $\mathrm{Ind}_S^H X$ sera encore noté X^* .

THEOREME 1. (cf. (C.R.))

Soient G un groupe fini, L un sous-groupe de G et $S \subset L$ un sous-ensemble contenant l'élément neutre et vérifiant :

(1) si $S^x = S$ pour x dans G, alors x est dans L,

(2) $S \cap S^x = \{1\}$ pour x dans G non dans L.

Soient $\lambda_1,\lambda_2,\ldots,\lambda_n$ des caractères irréductibles de L, nuls sur le complémentaire de S dans L, de même degré ($n \geq 2$), alors il existe n caractères $X_1,X_2,\ldots,X_n$ irréductibles, distincts, de G tels que $\mathrm{Pro}_L^G \lambda_i - \mathrm{Pro}_L^G \lambda_j = \epsilon(X_i - X_j)$, où $\epsilon = \pm 1$.

B. Définition des groupes de Suzuki.

Soient $n \geq 1$, $q = 2^{2n+1}$, $r = 2^n$, $\mathbb{F}_q$ le corps à q éléments.

Soit θ l'automorphisme de $\mathbb{F}_q$ défini par : $\alpha^\theta = \alpha^{2^n} = \alpha^r$. Pour tout élément (α,β) de $\mathbb{F}_q^2$, on notera $S(\alpha,\beta)$ la matrice 4 x 4 triangulaire suivante:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha^\theta & 1 & 0 & 0 \\ \beta & \alpha & 1 & 0 \\ (\alpha,\beta)_1 & (\alpha,\beta)_2 & \alpha^\theta & 1 \end{pmatrix}$$

où $(\alpha,\beta)_1 = \alpha^{2\theta+1} + \alpha^\theta\beta + \beta^{2\theta}$ et $(\alpha,\beta)_2 = \alpha^{\theta+1} + \beta$.

On vérifie aisément la relation :

$$S(\alpha,\beta)\, S(\gamma,\delta) = S(\alpha+\gamma,\ \alpha\gamma^\theta + \beta + \delta).$$

L'ensemble de ces matrices est un groupe qu'on notera S. Il est d'ordre q^2 et non abélien, car $\alpha\gamma^\theta \neq \gamma\alpha^\theta$, si $\alpha \neq \gamma$.

Soit maintenant, pour tout $\mu \neq 0$, $M(\mu)$ la matrice diagonale :

$$\begin{pmatrix} \mu^\theta & 0 & 0 & 0 \\ 0 & \mu^{1-\theta} & 0 & 0 \\ 0 & 0 & \mu^{\theta-1} & 0 \\ 0 & 0 & 0 & \mu^{-\theta} \end{pmatrix}$$

L'ensemble de ces matrices forment un groupe cyclique M d'ordre $q-1$, isomorphe au groupe multiplicatif $\mathbb{F}_q^*$.

De plus, en utilisant la relation : $2\theta^2 = \mathrm{Id.}$, on vérifie que:

$$M(\mu)^{-1}\, S(\alpha,\beta)\, M(\mu) = S(\mu^{2-2\theta}\alpha\ ,\ \mu\beta\ ).$$

Ainsi le groupe M normalise S et l'ensemble H = S.M est un groupe,

le groupe produit semi-direct S XI M .

De plus $S(\alpha,\beta)$ est égal à son conjugué par $M(\mu)$ si et seulement si $\mu = 1$ ou $\alpha = \beta = 0$ $(S(\alpha,\beta) = Id)$.
Par suite, H est un groupe de Frobénius de noyau S. Soit maintenant σ la matrice d'ordre 2 suivante :

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Le groupe de Suzuki sur le corps à q éléments sera le groupe S(q) engendré par H et σ : $\langle H,\sigma\rangle$.
On vérifie aisément les relations suivantes :

- $\sigma M(\mu)\sigma = M(\mu)^{-1}$,
- $S(q) = H \cup H\sigma H$,
- $H \cap (\sigma H\sigma) = M$, desquelles on déduit :

$S(q) = H \cup (H\sigma H) = H \cup H\sigma S$ et $H \cap H\sigma S = \emptyset$.

Par suite, $\mathrm{Card}(S(q)) = q^2(q-1) + q^2(q-1)q^2 = q^2(q-1)(q^2+1)$.

En faisant opérer S(q) sur les classes à gauche modulo H, on voit aisément que S(q) est doublement transitif, que H est le fixateur de la classe H et M le fixateur des classes H et $H\sigma$.
Par suite S(q) est un groupe de Zassenhauss de degré q^2+1 .
De ce résultat, on déduit que S(q) est simple .

RESUME DES RESULTATS EXPOSES, ICI, SUR LES GROUPES DE SUZUKI.

.) $\mathrm{Card}(G) = (q^2+1)q^2(q-1)$, $q = 2^{2n+1}$, $r = 2^n$, où $G = S(q)$.

.) G a q+3 classes de conjugaisons, toutes fortement réelles, sauf les 2 classes de conjugaisons des éléments d'ordre 4 qui ne sont pas réelles.

.) G admet une partition en sous-groupes:

$$G = \left(\bigcup_{x\in G} S^{*x}\right) \cup \left(\bigcup_{x\in G} M^{*x}\right) \cup \left(\bigcup_{x\in G} A_1^{*x}\right) \cup \left(\bigcup_{x\in G} A_2^{*x}\right) \cup \{1\}.$$

S est un 2-groupe de Sylow. M est cyclique d'ordre q-1 .

A_i est cyclique d'ordre $q+(-1)^{i+1}(2r+1)$.

S, M, A_1, A_2 sont des sous-groupes de Hall de G .

$N_G(S) = S \rtimes M = H$ est le fixateur de la classe H .

$N_G(M) = M \rtimes \langle\sigma\rangle$, où σ est une involution.

$N_G(A_i) = A_i \rtimes \langle\sigma_i\rangle$, où σ_i est élément d'ordre 4.

$N_G(S)$, $N_G(M)$, $N_G(A_i)$ sont des groupes de Frobénius.

.) Les q+3 caractères irréductibles de G sont:

(1) le caractère principal 1_G ,

(2) le caractère doublement transitif X_0 ,

(3) $\frac{q-2}{2}$ caractères de degré q^2+1 induits de caractères linéaires de H,

(4) 2 caractères de degré r(q-1) dont les restrictions à H sont les 2 caractères non réels et non linéaires de H.

(5) $\frac{q+2r}{4}$ caractères de degré (q-2r+1) et $\frac{q-2r}{4}$ caractères de degré (q+2r+1)(q-1) . Ils sont construits à partir des caractères de A_1 et A_2 respectivement.

Nous avons préféré le symbole Card pour désigner le cardinal d'un ensemble, pensant que cela faciliterait la lecture du texte.

2. CLASSES DE CONJUGAISON ET SOUS-GROUPES.

Commençons par rappeler un résultat général sur les groupes de Zassenhaus, les notations étant celles des préliminaires :

THEOREME 2.1 Soit G un groupe de Zassenhaus simple, et M le fixateur de deux points. Supposons que Card(M) soit impair. Les résultats ci-dessous s'en suivent:

1) M est cyclique et $N_G(M)$ est diédral.

2) Les involutions de G sont toutes conjuguées, et leur nombre m est égal à Card(M)x(Card(S) + 1).

3) Le nombre de classes de G fortement réelles, ne rencontrant pas S, est au moins égal à Card(M).

DEMONSTRATION. Nous renvoyons le lecteur à (E.B.) .

REMARQUE. Si G = S(q) , le point (1) est trivial ; de plus, dans ce cas, le nombre m est égal à $(q-1)(q^2+1)$.

Dans les groupes de Suziki, en ce qui concerne les classes de conjugaison non réelles, on peut préciser ceci :

THEOREME 2.2 Dans S(q) il y a exactement deux classes d'éléments d'ordre 4, et ces classes ne sont pas réelles. En d'autres termes, il n'y a pas de groupe de quaternions dans les 2-Sylow de G .

DEMONSTRATION. Soit f un élément d'ordre 4 ; comme S est un 2-Sylow, on peut supposer que f appartient à S. Posons alors f = S(a,b) (avec $a \neq 0$, car $f^2 \neq 1$). Soit g un élément de $C_G(f)$; comme S est le noyau du groupe de Frobenius H, $C_G(f)$ est contenu dans S. On peut donc poser g = S(c,d) . Les égalités suivantes sont équivalentes:

S(a,b)S(c,d) = S(c,d)S(a,b) et (1) $ca^{\theta} = a\,c^{\theta}$ (cf. 1)

Envisageons les deux cas suivants :

- $c = 0$. Alors l'égalité (1) est toujours vérifiée ; donc les q éléments $S(0,d)$ sont dans $C_G(f)$.

- $c \neq 0$. L'égalité (1) devient : $a^{\theta-1} = c^{\theta-1}$; en appliquant l'automorphisme 2θ , il vient : $a^{1-2\theta} = c^{1-2\theta}$, car $2\theta^2 = 1$. En multipliant les deux égalités précédentes terme à terme, on trouve : $a^{-\theta} = c^{-\theta}$, et par suite $a = c$. Les q éléments $S(a,d)$ appartiennent donc à $C_G(f)$, dont l'ordre est bien $2q$.

Comme $C_G(f) = C_S(f)$, le nombre de conjugués de f est :

$$(G:S)(S:C_S(f)) = ((q^2+1)q^2(q-1)).1/2q = 1/2.(q^2+1)q(q-1).$$

L'élément f n'est pas réel : s'il l'était, alors il existerait g dans G tel que : $g^{-1}fg = f^{-1}$; mais f^2 est une involution, et $g^{-1}f^2g = f^{-2} = f^2$; donc $g \in C_G(f^2) \subset S$; soit donc $S(c,d) = g$.

On a : $f^{-1} = S(a,b+a^{\theta+1})$ et $g^{-1} = S(c,d+c^{\theta+1})$.

En effectuant $g^{-1}fg$, on obtient :

$$c\,a^{\theta} + a\,c^{\theta} = a^{\theta+1}$$

appliquons 2θ , il vient :

$$c^{2\theta} + a^{2\theta}\,c = a^{1+2\theta} , \quad \text{et en multipliant par } a^{-\theta} :$$

$$c^{2\theta}\,a^{-1-\theta} + a^{\theta}\,c^{\theta} = a^{1+\theta} , \text{ d'où } c^{2\theta}\,a^{1-\theta} = a\,c^{\theta} ,$$

ce qui entraîne $a = c$; alors g commuterait avec f , ce qui est absurde car $f^2 \neq 1$.

Le nombre d'éléments de G conjugués à des éléments de S^* est $(q^2+1)(q^2-1)$.

Le nombre d'éléments de G conjugués à des éléments de S^* qui ne sont pas des involutions est :

$$(q^2+1)(q^2-1) - (q^2+1)(q-1) = (q^2+1)q(q-1) .$$

Comme les éléments d'ordre 4 ne sont pas réels, il y a au moins deux classes de conjugaison d'éléments d'ordre 4, et comme chacune

d'elles contient $1/2.(q^2+1)q(q-1)$ éléments, il y a exactement deux classes d'éléments d'ordre 4. Fin de la démonstration.

REMARQUE. Les classes d'éléments d'ordre 4 dans G sont en bijection avec celles de H . En d'autres termes, le sous-groupe H contrôle la fusion des 2-éléments de G .

On peut maintenant calculer les classes de conjugaison de G:

THEOREME 2.3 Soit $T_i = \{ g \in G \mid g \text{ fixe } i \text{ points exactement} \}$, avec $i = 0,1,2$; $G = T_0 \cup T_1 \cup T_2 \cup \{1\}$. On a les résultats suivants :

(i) $\text{Card}(T_1) = (q^2+1)(q^2-1)$ et $T_1 = C(2) \cup C_1(4) \cup C_2(4)$ où $C(2)$ est la classe des involutions, et $C_1(4)$ et $C_2(4)$ sont les deux classes d'éléments d'ordre 4.

(ii) $\text{Card}(T_2) = 1/2.(q^2+1)q^2(q-2)$ et T_2 est formé de $\frac{q-2}{2}$ classes fortement réelles.

(iii) $\text{Card}(T_0) = 1/2.q^3(q-1)^2$ et T_0 est formé de $q/2$ classes fortement réelles.

DEMONSTRATION.

(i) n'est qu'une réécriture du théorème 2.1.

(ii) Soit $g \in T_2$; il existe x tel que $g^x \in M$ car G est 2 fois transitif. De plus $N_G(M)$ contrôle ultra-fortement la fusion dans M et $\text{Card}(N_G(M)) = 2(q-1)$.

Tout élément g de M^* a donc un nombre de conjugués dans G égal à $\frac{(q^2+1)q^2(q-1)}{2(q-1)} = 1/2.(q^2+1)q^2$. Par suite, on a :

$$\text{Card}(T_2) = 1/2.(q^2+1)q^2(q-2) = (G:N_G(M))\times\text{Card}(M^*).$$

Comme $N_G(M)$ est diédral, il y a dans $N_G(M)$ $1/2.(q-2)$ classes d'éléments de M^* fortement réelles. Chacune de ces classes donne une classe de G fortement réelle.

(iii) $\mathrm{Card}(T_0) = \mathrm{card}(S(q)) - (\mathrm{Card}(T_1) + \mathrm{Card}(T_2) + 1)$
$= 1/2.q^3(q-1)^2$.

Par le théorème (1), G contient (q-1) classes fortement réelles disjointes de T_1 ; comme T_2 en contient $\frac{q-2}{2}$, il y a au moins $(q-1) - \frac{q-2}{2} = \frac{q}{2}$ classes fortement réelles dans T_0 (cf. Théorème 2.1). Qu'il n'y ait dans T_0 que des classes fortement réelles, et que leur nombre soit exactement $\frac{q}{2}$ va résulter de tout ce qui suit jusqu'à la fin de la proposition 8.

Soient .) $C_1 = \{e\}$, $C_2 = C(2)$

.) $C_3, \ldots, C_{\frac{q+2}{2}}$ les classes de T_2 ,

.) $C_{\frac{q+4}{2}}, \ldots, C_t$ les autres classes fortement

réelles de G. Soient $g_i \in G_i$. Nous posons:

$c_i = \mathrm{Card}\, C_G(g_i)$ et $a_i = \mathrm{Card}\{ (x,y) \mid x,y$ involutions et $xy = g_i\}$

.) On sait déjà que $a_1 = (q^2+1)(q-1)$, $c_1 = \mathrm{Card}(G)$

$c_2 = q^2$.

.) Montrons que $a_2 = q-2$. Soit x une involution qu'on peut supposer dans S . Alors $\mathrm{Card}\{ (z,y) \mid z.y = x \} = q-2 = a_2$; En effet, soient z et y tels que $zy = x$, alors $zyzy = 1$ et $zy = yz$; z et y sont dans le même 2-Sylow, par suite zy est dans ce 2-Sylow, donc z,y sont dans S. Comme z est dans S, que $zy = x$ et que $z \neq x$ (car $y \neq 1$), il s'en suit que $y = zx = xz$, d'où l'on déduit bien que $a_2 = q-2$.

.) Soit $g_i \in C_i$, pour $3 \leq i \leq \frac{q+2}{2}$.

G étant deux fois transitif, on peut supposer que g_i est dans M^*. D'autre part, on sait que $N_G(M) = M \times \langle\sigma\rangle$ contrôle ultra-

fortement la fusion dans M.

Si $xy = g_i$, alors $xxyx = yx = g_i^{-1}$; par suite, x est dans $N_G(M)$ et $y = xg_i$ aussi. Or les seules involutions de $N_G(M)$ sont les $m\sigma$ où $m \in M$. D'où, si $m \in M$, les seuls (x,y) tels que $x.y = m$ sont les $(m\sigma, \sigma)$. D'où $a_i = \text{Card}(M) = q-1$. Soit maintenant $x \in G$ tel que $xg_ix = g_i$; $x \in N_G(M)$ et comme $N_G(M)$ est diédral, il s'en suit que $x \in M$, et donc $c_i = q-1 = a_i$.

.) Soit $g_i \in C_i$; $\frac{q+4}{2} \leq i \leq t$. Nous posons :

$B_i = \{x \mid xg_ix = g_i^{-1}\}$; $b_i = \text{Card}(B_i)$,

$A_i = \{(x,y) \mid xy = g_i$, et x et y sont des involutions$\}$.

Si $x \in B_i$, alors $(x,xg_i) \in A_i$.

Inversement, si $(x,y) \in A_i$, on a $xxyx = yx = g_i^{-1}$; alors $x \in B_i$ et par suite $a_i = b_i$.

Si x et y appartiennent à B_i, alors $xy \in C_G(g_i)$; or, soit $x \in B_i$ $xy = xy'$ si et seulement si $y' = y$. Il y a donc au moins $b_i = a_i$ éléments distincts qui centralisent g_i et $a_i \leq c_i$.

Les propositions 1 et 2 précisent que $a_i = c_i$.

PROPOSITION 1. Si $g \in G^*$ est d'ordre impair et fortement réel, et si $x^{-1}gx = g^{-1}$, alors x est une involution.

DEMONSTRATION. Posons $\text{Card}(\langle x\rangle) = 2^u.v$, où v est impair. On sait que $u \leq 2$, car G ne contient pas de 2-éléments d'ordre supérieur à 4. On voit que x^v est un 2-élément et on peut supposer que x^v est dans S.

$S \cap S^{x^{2^u}} \supset \langle x^v\rangle$, donc x^{2^u} , qui centralise x^v $(\neq 1)$, est dans S. Comme c'est un 2'-élément, il est égal à 1, et x est donc un 2-élément. Si $u = 2$, alors x^2 centralise g_i et par suite g_i est dans S. Ceci est impossible car g est d'ordre

impair ; donc $u \neq 1$ et x est une involution.

PROPOSITION 2. Si g_i est dans T_0 alors $C_G(g_i)$ est d'ordre impair.

En effet, si x est un 2-élément de $C_G(g_i)$, g_i le centralise et par suite g_i et x sont dans le même 2-Sylow. Ce qui est impossible car g ne fixe aucun point.

COROLLAIRE. T_0 contient $\frac{q}{2}$ classes fortement réelles.

DEMONSTRATION. Montrons d'abord que $a_i = c_i$, pour $\frac{q+4}{2} \leq i \leq t$. On sait déjà que $a_i \leq c_i$. Soit x une involution inversant g_i (il en existe car g_i est fortement réel). Soit $y \in C_G(g_i)$; xy inverse g_i qui est d'ordre impair; par suite xy est une involution et $b_i \neq a_i \geq c_i$.

Maintenant, en comptant toutes les classes fortement réelles de G, on obtient :

$$(q^2+1)(q-1)^2 = (q^2+1)(q-1) + (q-2)(q^2+1)(q-1) + \frac{q-2}{2}(q-1)q^2(q^2+1) + \sum_{i \geq \frac{q+4}{2}} \mathrm{Card}S(q);$$

tout calcul fait, on trouve :

$$\frac{q}{2} = \sum_{i = \frac{q+4}{2}}^{t} 1 \quad , \text{ ce qui achève la preuve.}$$

PROPOSITION 3. Soit $g \in G$ d'ordre impair et fortement réel. Alors $C_G(g)$ est abélien maximal.

DEMONSTRATION. Soit $y \in C_G(g)$ et x une involution inversant g_i ; xy inverse g d'où (proposition 1) xy est une involution. Par suite $xyx = y^{-1}$, et $C_G(g)$ est donc abélien, et entant que centralisateur, abélien maximal.

COROLLAIRE. $C_G(g_i)$ est un sous-groupe de Hall de G.

DEMONSTRATION. Soit $p > 2$ un diviseur premier de $\mathrm{Card}(C_G(g_i))$. Soient $g \in C_G(g_i)$ un élément d'ordre p, et P un p-Sylow de G contenant g. Soit $y \in Z(P)$. Comme $g \in C_G(g_i)$, il existe une involution x telle que $xgx = g^{-1}$; par suite $xhx = h^{-1}$ pour tout h dans $C_G(g_i)$. En particulier, $xyx = y^{-1}$. Donc $C_G(y)$ est abélien (proposition 3); or P est contenu dans $C_G(y)$, donc P est abélien et par suite contenu dans $C_G(g)$. Comme $g_i \in C_G(g)$, on a $C_G(g_i) \supset C_G(g)$, donc il y a égalité et $P \subset C_G(g_i)$.

PROPOSITION 4. $N_G(C(g_i))$ contrôle ultra-fortement la fusion des π_i-sous groupes de G, où π_i désigne l'ensemble des diviseurs premiers de $C(g_i)$.

DEMONSTRATION.

.) Si L est un π_i-sous groupe de Hall, il est conjugué à $C(g_i)$. Par suite $N_C(C_G(g_i))$ (qui contient $C_G(g_i)$) contient tous les π_i-sous groupes de G qui sont abéliens (et donc nilpotents).

.) Soit $P \neq \{1\}$ un π_i-sous groupe de $N_G(C_G(g_i))$; P est abélien, donc nilpotent, et contenu dans $C_G(g_i)$. Si P^x est contenu dans $N_G(C_G(g_i))$ pour un $x \in G$, alors on a:

$$(C_G(g_i))^x \cap C_G(g_i) \supset P \neq \{1\} .$$

Soit $y \in P$; $C_G(y) = C_G(g_i) = (C_G(g_i))^x$ car y est d'ordre impair et fortement réel (proposition 3); par suite, $x \in N_G(C_G(g_i))$.

PROPOSITION 5. Si $g \in C_G(g_i)$ et si $g \neq 1$, alors $g \in T_0$.

DEMONSTRATION. Supposons que g fixe a , alors g fixe $g_i(a)$, $g_i(a) \neq a$, car $g_i \in T_0$. On a: $g(g_i(a)) = g_i(g(a)) = g_i(a)$. Par suite $g \in T_2$; on peut supposer $g \in M$, mais alors $M^{g_i} \cap M$ contient $\{g\} \neq \{1\}$; par suite $g_i \in N_G(M) = M \rtimes \langle\sigma\rangle$ et comme g_i est d'ordre impair, alors $g_i \in M$ et fixe donc deux points - ce qui est absurde -

COROLLAIRE. Sachant que l'on a l'inclusion suivante:

$$\bigcup_{j=\frac{q+4}{2}}^{t} \bigcup_{x \in G} (C_G^*(g_j))^x \subset T_0 ,$$

en choisissant les $g_{j_i} = y_i$, $i = 1,2,\ldots,v$, tels que les $C_G(y_i)$ ne soient pas conjugués, et en posant $c_i' = c_{j_i} = \mathrm{Card}(C_G(y_i))$, il vient:

$$\mathrm{Card}(T_0) = \frac{q^3(q-1)^2}{2} \geq \sum_{i=1}^{v} \frac{\mathrm{Card}(G)}{\mathrm{Card}N_G(C_G(y_i))}(c_i'-1) .$$

Le but des propositions 6 et 7 est d'établir que $v = 2$.

PROPOSITION 6. (Structure de $N_G(C_G(y_i))$)

$N_G(C_G(y_i)) / C_G(y_i)$ est cyclique d'ordre 4.

DEMONSTRATION. Soit σ une involution inversant y_i. On a :

$$(C_G(y_i) \rtimes \langle\sigma\rangle) \lhd N_G(C_G(y_i)) .$$

Soit y un élément de $N_G(C_G(y_i))$; $y^{-1}\sigma y' = \sigma'$ est une involution de $N_G(C_G(y_i))$; donc σ' normalise $C_G(y_i)$ et σ' ne fixe aucun point de $C_G(y_i)$, car $C_G^*(y_i)$ est impair. Par suite, $\sigma' g' = g^{-1}$ pour tout g de $C_G(y_i)$ (cf. lemme X.2.6 de (E.B.)). Donc $\sigma' = \sigma g'$ pour $g' \in C_G(y_i)$, soit $\sigma' \in C_G(y_i) \rtimes \langle\sigma\rangle$.

.) Par l'argument de Frattini appliqué à $C_G(y_i) \rtimes \langle\sigma\rangle$, $N_G(C_G(y_i))$ et $\langle\sigma\rangle$, Sylow de $C_G(y_i)$, on a:

$$N_G(C_G(y_i)) = C_G(y_i).(N_G(\langle\sigma\rangle) \cap N_G(C_G(y_i)))$$

$$= C_G(y_i).(C_G(\sigma) \cap N_G(C_G(y_i))).$$

.) $(C_G(y_i) \rtimes \langle\sigma\rangle) \cap C_G(\sigma) = L$ contient une seule involution, à savoir σ. En effet, si $\sigma_1 \neq \sigma$ était une autre involu-

tion, alors $\sigma_1\sigma$ en serait une qui fixerait y_i d'ordre impair, ce qui est impossible.

.) $C_G(\sigma) \cap N_G(C_G(y_i)) = L$ est un 2-groupe car $C_G(\sigma)$ l'est déjà ; il contient une seule involution; donc ce groupe est soit cyclique, soit quaternionien (cf. Théorème 1.3.8 de (E.B.)). Comme il ne contient que des éléments d'ordre ≤ 4, le groupe L est soit cyclique, soit égal à Q_3.

Dans Q_3 les éléments d'ordre 4 sont réels. Or dans G les éléments d'ordre 4 ne sont pas réels; par suite, L est cyclique d'ordre 2 ou 4. Nous avons :

$$C_G(\sigma) \cap N_G(C_G(y_i)) = N_G(C_G(y_i)) / C_G(y_i).$$

On va montrer que $N_G(C_G(y_i)) / C_G(y_i)$ est d'ordre 4. S'il était d'ordre 2, nous aurions les inégalités suivantes :

$$\frac{q^3(q-1)^2}{2} \geq \frac{(q^2+1)q^2(q-1)}{2} - \frac{(q^2+1)q^2(q-1)}{2c_i'} + \sum_{j \neq i} \frac{Card(G)}{Card\ N_G(C_G(y_j))}(c_j'-1)$$

$$\text{d'où } \frac{(q^2+1)q^2(q-1)}{2c_i'} \geq \frac{(q^2+1)q^2(q-1) - q^3(q-1)^2}{2} + \sum_{j \neq i} \frac{Card(G)}{4c_j'}(c_j'-1)$$

$$\geq \frac{(q-1)(q+1)q^2}{2} + \sum_{j \neq i} \frac{Card(G)}{4c_j'}(c_j'-1) ,$$

.) Premièrement, si v était strictement plus grand que 1, on aurait, pour un $j \neq i$, l'inégalité suivante:

$$\frac{(q^2+1)q^2(q-1)}{2c_i'} \geq \frac{q^2(q-1)(q+1)}{2} + \frac{Card(G)}{4c_j'}(c_j'-1) \quad , \text{ d'où :}$$

$\frac{1}{2c_i'} \geq \frac{1}{4} - \frac{1}{4c_j'}$; mais c_i' et c_j' sont au moins égaux à 5 (cf. ci-dessous), on aurait alors une contradiction :

$$\frac{1}{4} \leq \frac{1}{2c_i'} + \frac{1}{4c_j'} \leq \frac{1}{10} + \frac{1}{20} = \frac{3}{20} < \frac{1}{4} \quad .$$

- Le fait que c_k' est au moins égal à 5 résulte bien évidemment de ce que 3 ne divise pas Card(G) : Card(G) = 2 mod(3), car q = -1 mod(3).

.) Deuxièmement, si v était égal à 1, on aurait simplement : $c_1' \leq \frac{q^2+1}{q+1}$. Comme $C_G(y_i)$ est abélien, il y aurait $\frac{c_1'-1}{2}$ classes dans $N_G(C_G(y_i))$, donc dans G, car $N_G(C_G(y_i))$ contrôle la fusion des π_i-groupes de G. on aurait alors :

$$\frac{q}{2} = \frac{c_1'-1}{2} \quad \text{d'où} \quad q+1 = c_1' \leq \frac{q^2+1}{q+1} \quad ,$$

soit encore $(q+1)^2 \leq q^2+1$, ce qui est absurde.

.) Finalement, $\mathrm{Card}(N_G(C_G(y_i))) = 4c_i'$

PROPOSITION 7. v = 2.

DEMONSTRATION. On sait que $q^3(q-1)^2 \geq (\mathrm{Card}(G))\left(\sum_{i=1}^{v} \frac{c_i'-1}{2c_i'}\right)$,

soit encore $\frac{q(q-1)}{q^2+1} \geq \sum_{i=1}^{v} \frac{c_i'-1}{2c_i'}$.

Si on avait $v \geq 3$, il viendrait : $\frac{q(q-1)}{q^2+1} \geq \frac{3}{2} - \frac{1}{2c_1'} - \frac{1}{2c_2'} - \frac{1}{2c_3'}$

$$\geq \frac{3}{2} - \frac{3}{2} \times \frac{1}{5} \geq \frac{6}{5} > 1,$$

ce qui est absurde.
Si on avait v = 1, on aurait : $\frac{q}{2} = \frac{c_1'-1}{4}$; $c_1' = 2q + 1$ et c_1' diviserait $(q^2+1)(q-1)$, car c_1' est impair, q^2 est une puissance de 2 et c_1' divise déjà $(q^2+1)q^2(q-1)$. On voit aisément

que $2q+1$ et $q-1$ sont premiers entre eux, donc que $2q+1$ diviserait q^2+1, ce qui est absurde, puisque, pour tout $n \neq 2$, $2n+1$ ne peut diviser n^2+1 : en effet, supposons $n^2+1 = s(2n+1)$; $s > 1$, car $n \neq 2$; $n^2 - 2sn = s-1$ et n divise $s-1$, d'où $n \leq s$, et $(2n+1)s \geq 2n^2+n > n^2+1$, ce qui est absurde. Finalement $v = 2$.

PROPOSITION 8. T_0 ne contient pas d'éléments non fortement réels, $T_0 = \bigcup_{i=2}^{2} \left(\bigcup_{x \in G} C_G^*(y_i)^x \right)$, et en supposant $c_1' \geq c_2'$, alors $c_1' = q+2r+1$ et $c_2' = q-2r+1$, où $r = 2^n$.

DEMONSTRATION. Supposons qu'il existe un g de T_0 non fortement réel; soit y un élément de $C_G(g)$; y n'est pas fortement réel, sinon g le serait.

On va montrer que $C_G(g)$ est premier avec $c_1'c_2'$ et $q^2(q-1)$. Soit donc p un diviseur premier de $C_G(g)$, et soit y d'ordre p, P un p-Sylow de G contenant y. Il existerait x dans G tel que y^x soit dans $C_G(y_i)$ (cf. Proposition 4). Si p divisait $c_1'c_2'$, y^x serait conjugué à un élément de S, et si p divisait $q^2(q-1)$, y^x serait conjugué à un élément de M; dans les deux cas, y serait fortement réel, ce qui est absurde.

$$\text{Card}(T_0) = \frac{q^3(q-1)^2}{2} = (\text{Card } G)\left(\frac{c_1'-1}{4c_1'} + \frac{c_2'-1}{4c_2'}\right) + \sum_{g \in I} \frac{\text{Card } G}{\text{Card } C_G(g)},$$

où I est un ensemble de représentants des classes de T_0 non fortement réelles. Posons alors :

$$\frac{\text{Card } G}{\text{Card } C_G(g)} = q^2(q-1)c_1'c_2'm_g \quad ; \text{ on obtient l'égalité :}$$

$$\frac{q^3(q-1)^2}{2} = q^2(q-1)c_1'c_2'N + \text{Card}(G)\left(\frac{c_1'-1}{4c_1'} + \frac{c_2'-1}{4c_2'}\right)$$

où N est un entier. L'égalité s'écrit encore:

$$(q^2+1)(q+1) = (q+1)c_1'c_2' + 2(c_1'c_2')^2N \ ,$$

compte tenu de $c_1' + c_2' = 2q+2$, et comme $c_1'c_2'$ divise q^2+1, et que q^2+1 et $q+1$ sont premiers entre eux, alors $q+1$ divise N; posons $N = t(q+1)$; l'égalité ci-dessus devient:

$$q^2+1 = c_1'c_2' + 2(c_1'c_2')^2t \ ,$$

et comme on a supposé $c_1' \geq c_2'$, et que $c_1'^2 > q^2+1$, on obtient $q^2+1 < q^2+1$, ce qui est absurde. Donc $N = 0$, et on achève en calculant c_1' et c_2' comme racines de l'équation :

$$\lambda^2 - 2(q+1)\lambda + q^2+1 = 0 \ .$$

THEOREME 2.4. $A_i = C_G(y_i)$ est cyclique, avec $i = 1,2$.

DEMONSTRATION. Soit g un élément de A_i^* ; comme $g^n = 1$, g est diagonalisable dans la clôture algébrique de $\mathbb{F}_2$ et ses valeurs propres sont des racines $n^{\text{ièmes}}$ de l'unité.

Soit μ une valeur propre de g différente de 1 (il en existe car $g \neq 1$); $\mathrm{Card}(\langle g \rangle)$ divise q^2+1; soit m l'ordre de μ; m divise n, donc divise aussi q^2+1; les entiers $q-1$, q^2-1, et q^3-1 sont premiers avec q^2+1 , car si p est un facteur premier de $q-1$, il est forcément différent de 2 et on a:

$$q-1 = q^2-1 = q^3-1 = 0 \bmod(p), \text{ tandis que } q^2+1 = 2 \bmod(p);$$

par suite, $\mu \notin \mathbb{F}_q, \mathbb{F}_{q^2}, \mathbb{F}_{q^3}$. Or μ est racine d'un polynôme de degré 4 sur $\mathbb{F}_q$, par suite $\mu \in \mathbb{F}_{q^4}$; les valeurs propres de g sont alors :

$$\mu \ , \mu^q, \mu^{q^2} , \mu^{q^3} \ ,$$ et donc, 1 n'est pas valeur propre de g.

Supposons que A_i ne soit pas cyclique. Soit $\langle a,b \rangle$ un sous-groupe de type (p,p) de A_i (il en existe, puisque par hypothèse, A_i possède au moins un p-sous-groupe non cyclique !). Si $g \in \langle a,b \rangle$,

les valeurs propres de g sont des racines $p^{\text{ièmes}}$ de l'unité. Soit μ une valeur propre de a et ν une valeur propre de b . Comme a et b commutent, ils sont diagonalisables par rapport à une même base. Alors $\mu^r\nu^s$ est valeur propre de a^rb^s.

Posons $\nu = \mu^{q\alpha}$ (car $\mu \longrightarrow \mu^q$ engendre le groupe de Galois de $\mathbb{F}_{q^p}$). Choisissons alors des entiers r et s convenablement ; c'est-à-dire dans le but d'obtenir une contradiction: on choisit d'abord s de sorte que $(s,p) = 1$, ce qui entraîne aussi $(sq,p) = 1$; posons maintenant $r = -\alpha sq + p$; nous trouvons alors les deux choses suivantes:

.) $a^rb^s \neq 1$, parce que $b^s \neq 1$, ceci résultant de $(s,p) = 1$,

.) $\mu^r\nu^s = \mu^{r+\alpha sq} = \mu^p = 1$.

Ainsi, on aurait un élément de A_i^* , à savoir a^rb^s, qui admettrait 1 pour valeur propre, ce qui contredit le début de la démonstration.

3. LES CARACTERES IRREDUCTIBLES DE G .

1) Le caractère principal et le caractère doublement transitif.

.) Soit 1_G le caractère principal de G.

.) Soit X_0 le caractère de degré q^2 dont l'existence est établie dans la proposition 3.2.6 de (E.B.); il est doublement transitif.

2) Les caractères de G obtenus par induction de caractères du sous-groupe H.

.) En notant $\lambda_0 = 1_H$, puis $\lambda_1,\lambda_2,\ldots,\lambda_{q-2}$ (avec indices adéquats) les caractères linéaires de H, on en déduit (cf. proposition X.2.8 de (E.B.)) des caractères $\lambda_1^*,\lambda_2^*,\ldots,\lambda_{\frac{q-2}{2}}^*$

qui sont irréductibles de degré q^2+1, de G.

.) Autres caractères de G obtenus par induction de caractères de H.

Le sous-groupe H a $q+2$ classes de conjugaison, à savoir les $q-1$ classes qui contiennent des éléments de M, la classe des involutions et les deux classes d'éléments d'ordre 4.

Ainsi H possède 3 caractères non linéaires (de degré au moins deux) qu'on notera μ , ϑ_1, ϑ_2.

- μ est le caractère doublement transitif de degré $q-1$ obtenu à partir de la représentation double transitive de $H/Z(S)$.

- H a deux classes de conjugaison réelles, la classe de l'élément neutre et la classe des involutions.

Ainsi H ne possède que 2 caractères réels : 1_H et μ . Par suite, $\vartheta_1 = \bar{\vartheta}_2$. De plus, nous avons :

$$\text{Card}(H) = q^2(q-1) = (q-1) + (q-1)^2 + 2(\vartheta_1(1))^2,$$

soit $\vartheta_1(1) = (q-1)(\frac{q}{2})^{\frac{1}{2}}$.

En appliquant le théorème 1 à H, G et aux caractères ϑ_1, ϑ_2, on obtient deux caractères X_1 et X_2 de G vérifiant:

$$\vartheta_1^* - \vartheta_2^* = \epsilon(X_1 - X_2) \quad , \text{ où } \quad \epsilon = \pm 1.$$

En échangeant ϑ_1 et ϑ_2 , on peut supposer $\epsilon = 1$.
La relation de réciprocité de Frobénius donne alors :

$$(\vartheta_i^*, \vartheta_i^*)_G = \frac{r^2(q-1)^2}{(q-1)} + 1 = r^2(q-1) + 1 .$$

On applique alors le théorème 1, et on obtient:

$$\vartheta_i = X_i + r\Omega \quad , \text{ où } \quad \Omega \text{ est une somme de caractères}$$

de G, distincts de X_1 et de X_2 . On a alors $X_{i\,H} = \vartheta_i$, et par

suite, $X_i(1) = r(q-1)$. En comparant les degrés, on voit aisément que $X_i \neq 1_G$, X_0, λ_j^* , pour $j = 1,2,\ldots, \frac{q-2}{2}$.

3) Caractères obtenus à partir des caractères induits des sous-groupes A_1 et A_2.

Le sous-groupe $N_G(A_1)$ est un groupe de Frobénius d'ordre $4(q+2r+1)$, le sous-groupe $N_G(A_2)$ d'ordre $4(q-2r+1)$; A_i est le noyau de $N_G(A_i)$, pour $i = 1,2$; nous noterons N_i au lieu de $N_G(A_i)$, pour simplifier l'écriture.

- Le sous-groupe N_1 possède $\frac{q+2r}{4}$ caractères irréductibles non linéaires : $\sigma_1,\sigma_2,\ldots,\sigma_{\frac{q+2r}{4}}$.

- Le sous-groupe N_2 possède $\frac{q-2r}{4}$ caractères irréductibles non linéaires : $\pi_1,\pi_2,\ldots,\pi_{\frac{q-2r}{4}}$.

Comme le noyau de Frobénius de N_i est abélien, il s'en suit que les σ_i et les π_j sont des caractères induits respectivement de A_1 et de A_2.

Comme A_i est cyclique, nous avons $\sigma_i(1) = \pi_j(1) = 4$, pour tout i et tout j.

Dans la suite, nous supposons $q \geq 2^5$ (pour $q \leq 2^4$, les caractères de G sont faciles à déterminer).

Pour $q \geq 2^5$, on a $\frac{q\pm 2r}{4} \geq 3$; on peut donc appliquer le théorème 1 successivement aux caractères σ_i et π_j. On obtient alors les résultats suivants:

A) G possède les caractères distincts et irréductibles θ_i , au nombre de $\frac{q+2r}{4}$, satisfaisant:

$$\sigma_i^* - \sigma_j^* = \epsilon\,(\theta_i - \theta_j) \text{ , avec } \epsilon = \pm 1 .$$

Ces caractères sont distincts de 1_G, X_0, λ_i^*, X_1, X_2. En voici la démonstration. Sur l'identité, $\partial_1^* - \partial_2^*$ prend la valeur 0, ainsi que sur les éléments de T_2 et ceux de T_0, tandis que les $\sigma_i^* - \sigma_j^*$ prennent la valeur 0 sur T_1 ; on obtient donc: $0 = (X_1 - X_2, \theta_i - \theta_j)_G = (\partial_1^* - \partial_2^* , \sigma_i^* - \sigma_j^*)_G$.

Par suite, si θ_i, θ_j ne sont pas distincts de X_1, X_2 , ils seraient contenus dans $X_1 - X_2$ avec le même ordre de multiplicité, ce qui est impossible. Par suite, $\theta_i \neq X_1, X_2$, pour tout i satisfaisant $1 \leq i \leq \frac{q+2r}{4}$.

- Par ailleurs, $(\lambda_k^* , \theta_i - \theta_j)_G = (\lambda_k^* , \sigma_i^* - \sigma_j^*)_G = 0$, puisque $\lambda_k^* = 0$ sur T_0 et $\sigma_i^* - \sigma_j^*$ s'annule sur l'identité, sur T_1 et T_2. Par suite $\theta_i \neq \lambda_j^*$ pour tout i et pour tout j.

- Enfin, par la formule de réciprocité de Frobénius:

$$(\sigma_i^*, X_0)_G = (\sigma_i, X_0)_{N_1} = \frac{1}{\mathrm{Card}(N_1)} \sum_{N_2} \sigma_i(g) X_0(g)$$

$$= \frac{1}{\mathrm{Card}(N_1)} (\sigma_i(1) X_0(1) + \sum_{N_1^*} \sigma_i(g) X_0(g))$$

et comme $X_0(1) = q^2$, $\sigma_i(1) = 4$ et $X_0(g) = -1$ pour $g \in N_1^*$, il s'en suit que :

$$(\sigma_i^*, X_0)_G = \frac{1}{\mathrm{Card}(N_1)} (4q^2 + 4 - \sum_{N_1} \sigma_i(g))$$

$$= \frac{1}{\mathrm{Card}(N_1)} (4q^2+4) = \frac{4(q^2+1)}{4(q+2r+1)} = q-2r+1 .$$

Par suite, $(\theta_i - \theta_j , X_0)_G = (\sigma_i^* - \sigma_j^* , X_0)_G = 0$, d'où suit que l'on a $\theta_i \neq X_0$ pour $1 \leq i \leq \frac{q+2r}{4}$.

B) G possède les caractères distincts et irréductibles γ_j, au nombre de $\frac{q-2r}{4}$, satisfaisant :

$$\pi_i^* - \pi_j^* = \epsilon(\gamma_i - \gamma_j) \text{ , avec } \epsilon = \pm 1.$$

De la même manière que précédemment (en A) , on montre que $\gamma_i \neq 1_G$, λ_j^*, X_0, X_1, X_2 , pour tout i et tout j convenables.

Reste à démontrer donc que $\gamma_i \neq \theta_j$, pour tout i et tout j. Or nous avons : $0 = (\theta_i - \theta_j, \gamma_1 - \gamma_k)_G = (\sigma_i^* - \sigma_j^*, \pi_1^* - \pi_k^*)_G$, d'où le résultat cherché.

Résumons : nous avons obtenu les caractères irréductibles et distincts de G suivants :

- 1_G , X_0 de degré q^2 ,
- λ_i^* , $1 \leq i \leq \frac{q-2}{2}$, tous de degré q^2+1 ,
- X_1 , X_2 , tous deux de degré $r(q-1)$,
- θ_i , $1 \leq i \leq \frac{q+2r}{4}$,
- γ_j , $1 \leq j \leq \frac{q-2r}{4}$.

Soit au total : $2 + \frac{q-2}{2} + 2 + \frac{q+2r}{4} + \frac{q-2r}{4} = q+3$.

Le groupe G ayant $q+3$ classes de conjugaison, les caractères donnés ci-dessus sont les seuls caractères irréductibles de G . Nous achevons notre description en calculant :

C.) Les degrés des carctères θ_i et γ_j.

Nous allons établir que : $\theta_i(1) = (q-2r+1)(q-1)$ pour $1 \leq i \leq \frac{q+2r}{4}$,

$$\gamma_j(1) = (q+2r+1)(q-1) \text{ pour } 1 \leq j \leq \frac{q-2r}{4} .$$

On a : $(\mu^*, \lambda_i^*)_G = 1$, $(\mu^*, X_0)_G = 1$ et $(\mu^*, 1_G)_G = 0$.

Posons :

$$\mu^* = X_0 + \sum_{i=1}^{\frac{q-2}{2}} \lambda_i^* + a_1 X_1 + a_2 X_2 + \sum_{i=1}^{\frac{q+2r}{4}} b_i \theta_i + \sum_{j=1}^{\frac{q-2r}{4}} c_j \gamma_j .$$

La relation de réciprocité de Frobénius et les relations d'orthogonalité donnent alors :

$$(\mu^*, X_1 - X_2)_G = (\mu^*, \partial_1 - \partial_2)_G = (\mu^*, \partial_1 - \partial_2)_H = 0 \ ,$$

par suite $a_1 = a_2 = a$.

De la même manière, on obtient :

$$(\mu^*, \theta_i - \theta_j)_G = (\mu^*, \gamma_i - \gamma_j)_G = 0 \ ,$$ et par suite les b_i sont égaux entre eux et les c_i sont égaux entre eux ; nous poserons donc $b_i = b$ et $c_i = c$. On a alors:

$$(\mu^*, \mu^*)_G = q = 1 + \frac{q-2}{2} + 2a^2 + \frac{q+2r}{4} b^2 + \frac{q-2r}{4} c^2 \ , \text{ soit}$$

$$\frac{q}{2} = 2a^2 + \frac{q+2r}{4} b^2 + \frac{q-2r}{4} c^2 \ .$$

Par suite, on a: b et $c \leq 1$ (car $q = 2r^2$). Examinons les divers cas possibles :

.) Si $b = c = 0$; alors il vient: $\frac{q}{2} = 2a^2$, soit $q = (2a)^2$, ce qui est impossible car $q = 2^{2n+1}$ n'est pas un carré.

.) Si $b = 1$ et $c = 0$; alors il vient: $\frac{q}{2} = 2a^2 + \frac{q+2r}{4}$, d'où $\frac{q}{2} - 2a^2 = \frac{q}{4} + \frac{r}{2}$, ou encore, en tenant compte du fait que $q = 2^{2n+1}$ et $r = 2^n$: $r^2 - 4a^2 = r$, soit $(r - 2a)(r + 2a) = r$, ce qui est impossible, comme onle voit en mettant la plus haute puissance de 2 contenue dans a en facteur.

.) De la même manière on montre qu'on ne peut pas avoir $b = 0$ et $c = 1$.

.) Reste donc le seul cas possible : $b = c = 1$, soit:

$$[1] \qquad \mu^* = X_0 + \frac{q-2}{\Sigma^2}_{i=1} \lambda_i^* + \frac{q+2r}{4\Sigma}_{i=1} \theta_i + \frac{q-2r}{4\Sigma}_{j=1} \gamma_j \ .$$

En utilisant la relation de réciprocité de Frobénius et les valeurs de λ_i et γ_j, on trouve:

$$(\partial_1^*, X_0)_G = (\partial_1^*, \lambda_i)_G = r \quad \text{et} \quad (\partial_1^*, 1_G)_G = 0.$$

Par suite, nous avons: $(\partial_1^*, \theta_i - \theta_j)_G = (\partial_1^*, \gamma_i - \gamma_j)_G = 0$.

Posons alors: $\partial_1^* = aX_1 + \Omega$; comme $\partial_1 = X_1 - X_2 + \partial_2^*$, l'on a:

$$[2] \quad \partial_1^* = rX_0 + r \sum_{i=1}^{\frac{q-2}{2}} \lambda_i^* + aX_1 + bX_2 + c \sum_{i=1}^{\frac{q+2r}{4}} \theta_i + d \sum_{j=1}^{\frac{q-2r}{4}} \gamma_j .$$

Par suite, $(\partial_1^* - r\mu, \partial_i)_G = (\partial_1 - r\mu, \partial_i)_H = \begin{matrix} 0 \text{ si } i = 2 \\ 1 \text{ si } i = 1 \end{matrix}$.

Comme $(X_i, \mu^*)_G = 0$, l'on obtient :

$$a - b = (\partial_1^* - r\mu^*, X_1 - X_2)_G = (\partial_1^* - r\mu^*, \partial_1^* - \partial_2^*)_G = 1 ,$$

c'est-à-dire $a = b = 1$.

Les égalités [1] et [2] donnent alors :

$$\partial_1 - r\mu^* = aX_1 + (a-1)X_2 + (c-r) \sum_{i=1}^{\frac{q+2r}{4}} \theta_i + (d-r) \sum_{j=1}^{\frac{q-2r}{4}} \gamma_j .$$

Or, $(\partial_1^* - r\mu^*, \partial_1^* - r\mu^*)_G = r^2 + 1$; aussi a-t-on :

$$r^2+1 = a^2 + (a-1)^2 + \frac{q+2r}{4}(c-r)^2 + \frac{q-2r}{4}(d-r)^2.$$

Comme $q = 2r^2$ et $q \geq 2^5$, l'on a $|c-r|$, $|d-r| \leq 1$.

.) Si $c = d = r$, alors $r^2 = 2a(a-1)$, et comme a ou a-1 est impair, il s'en suit que $a = 2$ obligatoirement, d'où $q = 8$, ce qui cotredit l'hypothèse $q \geq 2^5$.

.) Si $|c-r| = 1$ et $|d-r| = 0$, on obtient :

$$r^2+1 = a^2 + (a-1)^2 + \frac{q+2r}{4} = 2a^2 - 2a + \frac{2r^2+2r}{4} + 1 ,$$

soit, après simplification :

$$r^2 - r = 4(a-1)^2 + 4(a-1) = r(r-1) = 4a(a-1) ,$$

c'est-à-dire, puisque a ou a-1 est impair,

$$4(a-1) = 0 \pmod r \quad \text{ou} \quad 4a = 0 \pmod r .$$

Supposons que $4(a-1) = tr$; il s'en suit $r-1 = t(\frac{tr}{4} + 1)$ ce qui est impossible (on commence par voir que $t \leq 2$, puis l'on vérifie que l'égalité n'est pas vérifiée pour $t = 0,1,2$)

Supposons maintenant que $4a = tr$; alors $r-1 = t(\frac{tr}{4} - 1)$, ou encore $4r - 4 = tr - 4$; il s'en suit que $t \leq 2$, puis que cette égalité ne peut être vérifiée pour $t = 0,1,2$. L'on ne peut donc avoir $|c-r| = 1$ et $|d-r| = 0$.

.) Supposons maintenant que $|c-r| = 0$ et $|d-r| = 1$. Il en découle:

$$r^2+1 = a^2 + (a-1)^2 + \frac{q-2r}{4} ,$$ soit encore $r(r+1) = 4a(a-1)$, et comme précédemment, on vérifie que c'est impossible.

.) Reste donc la seule possibilité : $|c-r| = |d-r| = 1$ et l'on a :

$$\begin{aligned} r^2 + 1 &= 1 + 2(a-1)^2 + 2(a-1) + \frac{q+2r}{4} + \frac{q-2r}{4} \\ &= 1 + 2(a-1)^2 + 2(a-1) + \frac{q}{2} \\ &= 1 + 2(a-1)^2 + 2(a-1) + r^2 , \text{ c'est-à-dire } a = 1. \end{aligned}$$

On a donc :

$$r^2 + 1 = 1 + (c-r)^2 \frac{q+2r}{4} + (d-r)^2 \frac{q-2r}{4} ,$$

où $c = r + \epsilon_1$, $d = r + \epsilon_2$, et $\epsilon_i = \pm 1$, pour $i = 1,2$.

La relation [2] devient alors:

$$\partial_1^* = rX_0 + r \sum_{i=1}^{\frac{q-2}{2}} \lambda_i^* + X_1 + (r+\epsilon_1) \sum_{i=1}^{\frac{q+2r}{4}} \theta_i + (r+\epsilon_2) \sum_{j=1}^{\frac{q-2r}{4}} \gamma_j .$$

Or $(\partial_1^*,\partial_1^*)_G = r^2(q-1) + 1$, par suite :

$$r^2(q-1) + 1 = r^2 + \frac{q-2}{2} r^2 + 1 + \frac{q+2r}{4} (r+\epsilon_1)^2 + \frac{q-2r}{4} (r+\epsilon_2)^2$$

En utilisant $q = 2r^2$, on obtient:

$$2r(r^2- 1) = (r+1)(r+\epsilon_1)^2 + (r-1)(r+\epsilon_2)^2 ;$$

on en déduit $\epsilon_1 + \epsilon_2 = 0$, puis $\epsilon_1 = -1$ et $\epsilon_2 = +1$.

Par suite:

$$\partial_1^* = rX_0 + r \sum_{i=1}^{\frac{q-2}{2}} \lambda_i^* + X_1 + (r-1) \sum_{i=1}^{\frac{q+2r}{4}} \theta_i + (r+1) \sum_{j=1}^{\frac{q-2r}{4}} \gamma_j .$$

De la même manière que précédemment, on obtient:

$$\partial_2^* = rX_0 + r \sum_{i=1}^{\frac{q-2}{2}} \lambda_i^* + X_2 + (r-1) \sum_{i=1}^{\frac{q+2r}{4}} \theta_i + (r+1) \sum_{j=1}^{\frac{q-2r}{4}} \gamma_j .$$

Par suite:

$$\theta_{i|H} = (r-1)(\partial_1 + \partial_2) + \mu$$

$$\gamma_{i|H} = (r+1)(\partial_1 + \partial_2) + \mu ,$$

d'où le résultat recherché (degrés de θ_i et de γ_j) .

REFERENCE.

(E.B.) Cours de Enguehard - Broué , Polycopié, Université Paris 7, Année 1980.

(C.R.) Curtis W.C. and Reiner I. , Representation Theory of finite groups and associative algebras, Wiley,Interscience,New York,1962.