Astérisque

THOMAS PETERFALVI

Le théorème de Bender-Suzuki II

Astérisque, tome 142-143 (1986), p. 235-295

<http://www.numdam.org/item?id=AST_1986__142-143__235_0>

Société Mathématique de France
Astérisque 142-143 (1986)

LE THÉORÈME DE BENDER-SUZUKI II

Par Thomas Peterfalvi

CHAPITRE V - CAS OÙ V A UN SOUS-GROUPE D'ORDRE PREMIER DONT LE CENTRALISATEUR EST DE 2-RANG 1

§ 1.- Structure de Q et de K 240

§ 2.- Lemmes préliminaires 242

§ 3.- Le théorème F 247

CHAPITRE VI - STRUCTURE DE H

§ 1.- Structure de Q 257

§ 2.- Le cas où st est d'ordre 5 261

§ 3.- Opération de KW sur S 264

CHAPITRE VII - CARACTÉRISATION DE PSU(3,q)

§ 1.- Les applications f, g, h 267

§ 2.- Calcul préliminaire 268

§ 3.- Détermination de f 275

§ 4.- Le cas où $V \neq W$ 278

APPENDICE X : Un cas particulier d'un théorème de Huppert 281

APPENDICE XI : Sur les presque-corps 284

APPENDICE XII : Le théorème de Feit-Sibley 287

INTRODUCTION

Dans cette seconde partie, nous exposons avec certaines simplifications l'article de M. Suzuki :

[S] On a class of doubly transitive groups II. Ann. of Maths, vol.79(1964), pp.514-589.

Nous supposons de nouveau que :

(B0) G est un groupe fini de 2-rang ≥ 2 et H est un groupe de Bender propre de G.

(B1) Tout groupe d'ordre $< |G|$ qui vérifie l'hypothèse du théorème B (chap.II) vérifie aussi sa conclusion.

(B2) $O_{2'}(G) = 1$.

Nous gardons les notations générales de l'introduction à la première partie. On note t un élément fixé de Inv(G-H), $D = H \cap H^t$, $V = C_D(t)$, $K = \{x \in D | x^t = x^{-1}\}$. D'après le théorème A (chap.I), G opère de manière 2-transitive sur l'ensemble Ω des conjugués de H dans G. D'après le théorème D (chap.III), il existe un sous-groupe Q de H tel que $H = Q \rtimes D$. On pose $W = C_V(K)$. D'après la prop. 4 du chap.II, §4, $W = C_D(\mathrm{Inv}(H))$.

Notre but est de démontrer la conclusion du théorème B : $O^{2'}(G)$ est isomorphe à l'un des groupes PSL(2,q), Sz(q), PSU(3,q) où q est une puissance de 2.

On supposera connue la classification des groupes de Zassenhaus. Selon cette classification, si G est un groupe de Zassenhaus, c'est à dire si le fixateur dans G de 3 points de Ω est réduit à 1, G est isomorphe à un groupe PSL(2,q) ou Sz(q). Il est facile de voir que G est un groupe de Zassenhaus si et seulement si $V = 1$. Compte tenu de l'hypothèse de récurrence, il suffira donc de démontrer :

Si $V \neq 1$, alors ou bien $O^{2'}(G) \neq G$ ou bien $G \tilde{=} PSU(3,q)$ pour une puissance q de 2.

La caractérisation finale de G se fait par la méthode des générateurs et relations de Suzuki, déjà utilisée par celui-ci pour la détermination des groupes de Zassenhaus. Tout élément x de G-H se met de manière unique sous la forme $x = adtb$ où $a, b \in Q$ et $d \in D$. La structure de G est alors déterminée par la structure de H, l'action de t sur D, et par les applications $f,g : Q^{\#} \to Q^{\#}$ et $h : Q^{\#} \to D$ telles que $txt = g(x)h(x)tf(x)$ pour $x \in Q^{\#}$. Ces applications satisfont certaines relations, déduites en particulier de l'associativité de la loi de G, à partir desquelles on doit les déterminer.

Mais auparavant, on doit déterminer la structure de H, et éliminer éventuellement certains cas où des théorèmes basés sur le transfert assurent que $O^{2'}(G) \neq G$.

Comme on l'a déjà vu dans la première partie, le cas où V a un sous-groupe P d'ordre premier p tel que $C_G(P)$ soit de 2-rang 1 présente une difficulté particulière, l'hypothèse de récurrence ne s'appliquant pas à $C_G(P)$. Le but est alors de démontrer que G a un quotient d'ordre p. Ce cas est traité dans le chapitre V. Dans [S], la démonstration est basée sur un lemme assez difficile, le lemme 37, qui affirme que si un groupe fini X vérifie certaines conditions compliquées, X a un quotient d'ordre p. Dans notre exposé, la formule des points fixes de H. Wielandt est utilisée pour calculer $|G|_p$, et la plus grande partie du lemme 37 de [S] devient alors inutile.

Dans les chapitres VI et VII, on suppose que si P est un sous-groupe d'ordre premier de V, $C_G(P)$ est de 2-rang ≥ 2, ce qui permet d'utiliser (B1).

Le chapitre VI a pour but la détermination de H. La principale difficulté est de montrer que Q est un 2-groupe. Une fois ceci connu, la classification des 2-groupes de Suzuki par G. Higman (voir [Hi]) permet de déterminer $Q \rtimes KW$. Après avoir écarté les cas conduisant à $O^{2'}(G) \cong PSL(2,q)$ ou Sz(q) (dans ces cas, l'hypothèse $V \neq 1$ implique $G \neq O^{2'}(G)$), on voit que $Q \rtimes KW$ est déterminé par $q = |\Omega_1(Q)|$, par un automorphisme de $\mathbb{F}_q$, et par $|W|$, qui divise q+1.

Dans [S], la démonstration du fait que Q est un 2-groupe est longue et morcelée en plusieurs cas. De plus, G. Glauberman a trouvé des lacunes dans cette preuve. Elle est simplifiée ici par l'utilisation d'un théorème de D.A. Sibley.

Si G est un groupe de Zassenhaus satisfaisant (BO), $H = Q \rtimes D$ est un groupe de Frobenius et Q est à intersections triviales dans G. Dans ce cas,

W. Feit avait démontré en 1960 que Q est un 2-groupe en utilisant la théorie des caractères exceptionnels. Cependant, dans notre cas plus général, on sait seulement que si Q n'est pas un 2-groupe, $O_{2'}(Q) \rtimes D$ est de Frobenius et $O_{2'}(Q)$ est à intersections triviales dans G. Le théorème de Sibley (1976), généralisant les résultats de Feit sur les caractères exceptionnels, permet de conclure dans cette situation.

Dans l'appendice XII, nous démontrons le théorème de Sibley, sous la forme qui nous est nécessaire.

Dans le chapitre VII, nous passons à la détermination des applications f, g, h. Dans [S], ceci est précédé par la démonstration de l'implication $V \neq W \Rightarrow O^{2'}(G) \neq G$. En étudiant la situation analogue aboutissant aux groupes unitaires en caractéristique $\neq 2$, W. Kantor et G. Seitz ont trouvé une erreur dans cette démonstration. Dans leur article "Finite groups with a split BN-pair of rank 1 - II" (J. of Alg. 20, 1972, pp.476-494, paragraphes 14 et 15), ils donnent une démonstration valable pour toute caractéristique. Nous avons d'autre part trouvé des erreurs dans le calcul final de l'application f dans [S]. Il y est affirmé qu'un certain cas est impossible (cas ii du lemme 64), alors que ce cas est réalisé si $G = PSU(3,q)$ et $q \equiv -1 \pmod 3$. Il suffit cependant de modifications peu importantes pour rendre ce calcul valable (paragraphes 1, 2, 3 du chapitre VII). Dans le cas où $V \neq W$, nous avons remplacé la démonstration de Kantor et Seitz, qui utilise des théorèmes de transfert, par le calcul plus élémentaire de l'application f.

Je remercie le professeur G. Glauberman, qui m'a communiqué ses notes sur l'article de M. Suzuki, ainsi que les membres de l'équipe des groupes finis de Paris qui m'ont encouragé pour cette rédaction.

Références et notations

On utilisera les rérérences suivantes :

[H] B. Huppert : Endliche Gruppen I (Springer Verlag, 1967).

[HB] B. Huppert, N. Blackburn : Finite groups II, III (Springer Verlag, 1982).

[Hi] G. Higman : Suzuki 2-groups. Illinois J. of Math. 7(1963), pp.79-96 .

[Is] I.M. Isaacs : Character theory of finite groups (Academic Press, 1976).

Dans le chap. V, §3, on supposera connu le théorème de Hall-Wielandt :

Soit P un p-groupe de Sylow d'un groupe fini G. Soit A un sous-groupe faiblement fermé de P relativement à G (cela signifie que pour $g \in G$, $A^g \subset P$ implique $A^g = A$). Si $A \subset Z_{p-1}(P)$ ou bien si A est abélien, alors $G/O^p(G) \tilde{=} N_G(A)/O^p(N_G(A))$.

Pour une démonstration, voir M. Hall : The theory of groups (The Macmillan company, 1959), p.212.

Rappelons qu'un couple (P,K) est un 2-groupe de Suzuki si P est un 2-groupe non-abélien tel que $|\mathrm{Inv}(P)| > 1$ et K est un groupe cyclique qui opère fidélement sur P et qui est transitif sur Inv(P). Nous dirons dans ce cas, par abus de langage, que P est un 2-groupe de Suzuki.

Soit (P,K) un 2-groupe de Suzuki, $Z = Z(P)$ et $q = |Z|$. D'après [Hi], on a $Z = \mathrm{Inv}(P) \cup \{1\}$ et $|P| = q^2$ ou q^3. Si $|P| = q^2$, P est dit "de type A", et si $|P| = q^3$, P est dit "de type B, C ou D". Dans tous les cas, P/Z est abélien élémentaire, et P est de type B si et seulement si P/Z est somme directe de deux $\mathbb{F}_2[K]$-modules isomorphes d'ordre q.

Pour chacun des types, [Hi] donne une famille d'applications $\mathbb{F}_2$-quadratiques $\chi : E \to \mathbb{F}_q$, où $E = \mathbb{F}_q$ ou $\mathbb{F}_q \times \mathbb{F}_q$, telle que l'extension $Z \to P \to P/Z$ soit isomorphe à l'extension de $\mathbb{F}_q$ par E associée à l'un des χ (Appendice VIII, lemme 1). Nous n'aurons pas besoin de la définition explicite des types C et D, et nous rappellerons au moment voulu quelle est la famille d'applications quadratiques définissant les groupes de type B.

Bien que les opérations d'un groupe sur un ensemble ou sur un groupe soient des opérations à droite, les matrices sont multipliées "lignes par colonnes" et si f, g, sont des applications, f o g(x) désigne f(g(x)).

CHAPITRE V. CAS OÙ V A UN SOUS-GROUPE D'ORDRE PREMIER DONT LE CENTRALISATEUR EST DE 2-RANG 1

§1.- STRUCTURE DE Q ET DE K

Proposition 1. a) Si $x \in K-\{1\}$ *, on a* $C_Q(x) = 1$.

b) Q *est nilpotent.*

c) $\mathrm{Inv}(H) \subset Z(Q)$ *et* $\mathrm{Inv}(H) \cup \{1\}$ *est un 2-groupe abélien élémentaire.*

a) Si $x \in K-\{1\}$, on a $|\Omega_x| = 2$ (chap.II, §4, prop.2). Puisque $C_G(x)$ opère sur Ω_x , on a $C_H(x) \subset D$, donc $C_Q(x) = 1$.

b) On sait que $|K| = |\mathrm{Inv}(H)| > 1$ (chap.I, §2) donc il existe $x \in K-\{1\}$. Comme $\langle x \rangle \subset K$, $\langle x \rangle$ opère alors sans point fixe sur Q d'après a), donc Q est nilpotent d'après le théorème de Thompson sur les noyaux de Frobenius.

c) Puisque Q est nilpotent d'ordre pair, $Z(Q)$ contient une involution. Comme D opère transitivement sur $\mathrm{Inv}(H)$, on a donc $\mathrm{Inv}(H) \subset Z(Q)$ et $\mathrm{Inv}(H) \cup \{1\}$ est un 2-groupe abélien élémentaire.

Dans la suite, on notera $Q_o = \mathrm{Inv}(H) \cup \{1\}$, $q = |Q_o|$, et on posera $Q = S \times Q_1$ où S est le 2-Sylow de Q.

Proposition 2. K *est un sous-groupe normal cyclique de* D.

Soient $\bar{D} = D/W$ et A tel que $W \subset A \subset D$ et $\bar{A} = F(\bar{D})$. Puisque $\bar{D}$ opère fidèlement sur Q_o et transitivement sur $Q_o^{\#}$, on peut lui appliquer la prop. de l'appendice X .

Montrons que $\bar{A} = J(\bar{D},t)$. D'après l'appendice X, $\bar{A}$ opère sans point fixe sur Q_o . Mais V centralise un élément de $Q_o^{\#}$ (chap.II, §4, prop.2), donc $\bar{A} \cap \bar{V} = 1$, d'où $\overline{C_A(t)} = C_{\bar{A}}(t) = 1$ et $\bar{A} \subset J(\bar{D},t)$ d'après l'appendice I .

D'autre part, D/A est abélien (appendice X), donc $J(D/A,t) = B/A$ est un groupe. Puisque t inverse les éléments de B/A et de A/W, $C_B(t) \subset C_A(t) \subset W$, donc t inverse les éléments de $\bar{B} = B/W$, donc $\bar{B}$ est abélien et $\bar{B} = J(\bar{D},t)$. D'après le théorème de Fitting, il en résulte que $\bar{A} = \bar{B} = J(\bar{D},t)$.

Puisque t opère sur A, on a $A = (A \cap K)(A \cap V)$ (appendice I). Mais, puisque $J(\bar{D},t) = \bar{A}$, on a $K \subset A$ et $A \cap V = W$, donc $A = KW$ et $|\bar{A}| = |K|$.

D'après l'appendice X, $\bar{A}$ est cyclique, donc il existe $k \in K$ tel que $\bar{A} = \langle\bar{k}\rangle$. Alors $|\langle k\rangle| \geq |\langle\bar{k}\rangle| = |\bar{A}| = |K|$, donc $K = \langle k\rangle$ est un groupe cyclique. On a $K \lhd D$ d'après l'appendice I .

Corollaire. Le 2-Sylow S *de* Q *est abélien ou est un 2-groupe de Suzuki.*

En effet, K opère régulièrement sur $\mathrm{Inv}(S) = \mathrm{Inv}(H)$ (chap.I, §2).

Si F est un corps et A un sous-groupe de Aut(F), on posera $L(F,A) = (F \rtimes F^*) \rtimes A$, où F^* opère sur le groupe additif F par multiplication à droite et A opère naturellement sur F et sur F^*.

Proposition 3. Il existe un groupe d'automorphismes A *de* $\mathbb{F}_q$ *et un isomorphisme de* $Q_o \rtimes (D/W)$ *sur* $L(\mathbb{F}_q,A)$ *qui identifie* Q_o *à* $(\mathbb{F}_q,+)$, K *à* $\mathbb{F}_q^*$ *et* V/W *à* A . *En particulier,* V/W *est cyclique.*

Puisque $\bar{K} = KW/W$ est un sous-groupe normal cyclique de $\bar{D} = D/W$ qui opère transitivement sur $Q_o^{\#}$, on peut appliquer l'appendice V . D'après a) de

cet appendice, Q_o est un $\mathbb{F}_q$-espace vectoriel de dimension 1 et K s'identifie au groupe des homotéties non nulles de cet espace. Soit $s \in Q_o^{\#}$ tel que $V = C_D(s)$ (chap.II, §4, prop.2) et identifions le $\mathbb{F}_q$-espace Q_o à $\mathbb{F}_q$ de sorte que s soit identifié à $1 \in \mathbb{F}_q$. D'après b) et c) de l'appendice V, $\overline{V} = V/W$ opère sur $Q_o \rtimes K \cong \mathbb{F}_q \rtimes \mathbb{F}_q^*$ comme un groupe d'automorphismes de corps.

§2.- LEMMES PRÉLIMINAIRES

Nous étudions d'abord une famille de groupes qui vérifient des propriétés moins restrictives que celles de G : on dira que (L,M) appartient à la famille $\mathcal{F}$ si L est un groupe fini, M est un sous-groupe propre d'ordre pair de L, L opère de manière 2-transitive sur l'ensemble des conjugués de M dans L, et pour $x \in L-M$, $M \cap M^x$ est d'ordre impair et a un complément normal dans M.

Le sous-groupe $\mathcal{N}(L) = \bigcap_{x \in L} M^x$ sera alors appelé noyau de L.

On a ainsi $(G,H) \in \mathcal{F}$, avec de plus $\mathcal{N}(G) = 1$ et G de 2-rang ≥ 2.

Lemme 1. *Soient* $(L,M) \in \mathcal{F}$, $t \in \mathrm{Inv}(L-M)$, $D = M \cap M^t$ *et* $M = Q \rtimes D$.
a) Tout élément de L-M *se met de manière unique sous la forme* xty, *où* $x \in M$ *et* $y \in Q$.
b) Il existe un couple (s,r) *et un seul tel que* $tst = r^{-1}tr$, $s \in \mathrm{Inv}(Q)$ *et* $r \in Q$.
c) $\mathcal{N}(L) = C_D(Q) \subset C_D(t)$ *et si* $\overline{L} = L/\mathcal{N}(L)$, *on a* $(\overline{L},\overline{M}) \in \mathcal{F}$, $\overline{Q} \cong Q$ *et l'ordre de* $\overline{s}\,\overline{t}$ *est le même que celui de* st, s *étant l'élément défini dans b).*

a) Puisque L est 2-transitif sur $\{M^x | x \in L\}$ et t normalise D, on a $L - M = MtM = MtDQ = MDtQ = MtQ$, d'où l'existence de x et y. D'autre part, si $x_i \in M$, $y_i \in Q$ $(i=1,2)$ et $x_1ty_1 = x_2ty_2$, alors $tx_2^{-1}x_1t = y_2y_1^{-1} \in M^t \cap Q = 1$, d'où l'unicité.

b) Soient $K = J(D,t)$ et $u \in \mathrm{Inv}(Q)$. D'après le §2 du chap. I, $k \mapsto u^k$ est une bijection de K sur Inv(Q). Il suffit donc de montrer qu'il existe un unique $k \in K$ tel que tu^kt soit de la forme $y^{-1}ty$, où $y \in Q$. D'après a), il existe $x \in M$ et $y \in Q$ tels que $tut = xty$. Alors $xty.xty = 1$, d'où $t(yx)t = (yx)^{-1}$ et $a = yx \in J(M,t) = K$.
On a donc, pour $k \in K$:

$$tk^{-1}ukt = ktutk^{-1} = ky^{-1}atyk^{-1} = (ky^{-1}k^{-1})kak.t.(kyk^{-1}),$$

et tu^kt est de la forme voulue si et seulement si $kak = 1$, ou $k^{-2} = a$. Comme $k \mapsto k^2$ est une bijection : $K \to K$, il existe bien un unique $k \in K$ tel que $k^{-2} = a$.

c) Puisque Q est un sous-groupe normal régulier de M opérant sur $\{M^x \mid x \in L-M\}$, le stabilisateur D de M^t dans M opère de manière équivalente sur Q et sur $\{M^x \mid x \in L-M\}$, donc $N(L) = C_D(Q)$. Puisque $N(L) \lhd L$ et t est conjugué à un élément de Q, il en résulte que t centralise $N(L)$. Puisque $N(L) \subset D$, on a $\overline{M} = \overline{Q} \rtimes \overline{D}$, $(\overline{L},\overline{M}) \in \bar{F}$ et $\overline{Q} \cong Q$. Les éléments de $\langle st \rangle \cap N(L)$ sont inversés par t, centralisés par t et d'ordre impair, donc $\langle st \rangle \cap N(L) = 1$ et l'ordre de $\overline{s}\,\overline{t}$ est le même que celui de st.

L'expression xty de a) sera appelée forme canonique de l'élément $z = xty$, l'élément s de b) sera appelée l'involution distinguée de Q (relativement à t) et l'égalité $tst = r^{-1}tr$ l'identité de structure de L. Remarquons que L est transitif sur l'ensemble des couples (M',t') où M' est un conjugué de M et $t' \in \mathrm{Inv}(L-M')$ (2-transitivité de L et transitivité de D sur Inv(M)), donc l'ordre de st est indépendant du choix de M et de t.

Revenons à l'étude du groupe G. On notera s l'involution distinguée de Q, relativement à t.

Lemme 2. *Soit* X *un sous-groupe* $\neq 1$ *de* V.

a) Si $L = C_G(X)$, *alors* $(L, L \cap H) \in \mathcal{F}$, $\mathcal{N}(L) = C_{L \cap D}(L \cap Q) \subset L \cap V$ *et* $M \mapsto L \cap M$ *est une bijection de* Ω_X *sur l'ensemble des conjugués de* $L \cap H$ *dans* L.

b) $N_G(X) = C_G(X) N_V(X)$.

c) Supposons que $C_G(X)$ *soit de 2-rang* ≥ 2 . *Alors* $N_H(X) = C_S(X) \rtimes N_D(X)$, *en particulier,* $C_{Q_1}(X) = 1$, *et si* $F = O^{2'}(C_G(X))$ *et* $\ell = |C_{Q_0}(X)|$, *on a l'un des 3 cas :*

F/Z(F) $\cong$ PSL(2,ℓ) , st *est d'ordre 3,* $C_Q(X)$ *est abélien élémentaire d'ordre* ℓ.

F/Z(F) $\cong$ Sz(ℓ), st *est d'ordre 5,* $C_Q(X)$ *est un 2-groupe de Suzuki de type* A, *d'ordre* ℓ^2.

F/Z(F) = PSU(3,ℓ) , st *est d'ordre 3,* $C_Q(X)$ *est un 2-groupe de Suzuki d'ordre* ℓ^3.

a) D'après le chap.II, §4, prop. 1, $M \mapsto L \cap M$ est une bijection de Ω_X sur une classe de groupes de Bender propres de L. D'après l'appendice II, (7), on a alors $(L, L \cap H) \in \mathcal{F}$ et $C_H(X) = C_Q(X) \rtimes C_D(X)$.

b) Si $g \in N_G(X)$, il existe $f \in C_G(X)$ tel que gf fixe H et H^t, car $C_G(X)$ est 2-transitif sur Ω_X d'après a). Donc $N_G(X) = C_G(X) N_D(X)$, mais $N_D(X) = N_K(X) N_V(X) \subset C_G(X) N_V(X)$ (chap.II, §4, lemme 1).

c) Puisque $C_G(X)$ est de 2-rang ≥ 2 , $|C_K(X)| = |\mathrm{Inv} C_H(X)| > 1$ d'après le chap. I, §2, et on peut utiliser la prop. 3 du chap. II, §4. Puisque $C_S(X)$ est l'unique 2-Sylow de $C_H(X)$, on a $N_H(X) = C_S(X) \rtimes N_D(X)$ d'après le b) de cette proposition. D'après l'assertion c) de la même proposition, $\bar{F} = F/Z(F)$ est isomorphe à l'un des groupes indiqués. Puisque $F \cap H = C_S(X) \rtimes (F \cap D)$ et F est 2-transitif sur Ω_X(toujours d'après la même prop.), $(F, F \cap H) \in \mathcal{F}$ et $\mathcal{N}(F) = O_{2'}(F) = Z(F)$. D'après le lemme 1 b), l'identité de structure de F est la même que celle de G, donc $\bar{s}$ est l'involution distinguée de $\bar{F}$, relativement

à $\bar{t}$. D'après le lemme 1 c), l'ordre de st est égal à l'ordre de $\bar{s}\,\bar{t}$ dans $\bar{F}$ et $C_Q(X) \cong \overline{C_Q(X)}$ est le 2-Sylow de $\overline{C_H(X)}$. Les assertions sur l'ordre de st et la structure de $C_Q(X)$ résultent donc de la structure des groupes PSL(2,ℓ), Sz(ℓ), PSU(3,ℓ) (voir la remarque après le lemme 1).

Pour les 2-Sylow de PSL(2,ℓ) et Sz(ℓ) voir [H], chap.II, (8-2) et [HB], chap. XI, (3-1) et (3-3). La structure du 2-Sylow de PSU(3,ℓ) est donnée dans [H], chap. II, (10-12). Pour l'ordre de st dans PSL(2,ℓ) et Sz(ℓ), où s est l'involution distinguée, voir [HB], chap. XI, (10-7). Enfin, en prenant la présentation de PSU(3,ℓ) donnée dans [H], chap.II, (10-12), si s et t sont les images dans PSU(3,ℓ) des matrices

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

respectivement, on voit que $s^2 = t^2 = 1$ et $tst = sts$, donc s est l'involution distinguée de Q, relativement à t, et st est d'ordre 3.

Lemme 3. *a)* $V = C_D(s)$

b) Soient X,Y *des parties de* V *conjuguées dans* G. *Alors* X *et* Y *sont conjugués dans* V.

a) D'après le lemme 2 a), $(C_G(V), C_H(V)) \in \mathcal{F}$. D'après le lemme 1 b), l'identité de structure de $C_G(V)$ est la même que celle de G, donc $s \in C_G(V)$. Alors $V \subset C_D(s)$ et $|V| = |C_D(s)| = |D/K|$ d'après le chap. I, §2.

b) Soit $g \in G$ tel que $Y = X^g$. Alors H, H^t, H^g, H^{tg} appartiennent à Ω_Y. D'après le lemme 2 a), $C_G(Y)$ est 2-transitif sur Ω_Y, donc il existe $h \in C_G(Y)$ tel que $H^{gh} = H$ et $H^{tgh} = H^t$. Alors $X^{gh} = Y$ et $gh \in D$. En appliquant l'homomorphisme canonique $: D \to V$ aux deux membres de $X^{gh} = Y$, on voit que X et Y sont conjugués dans V.

Rappelons qu'un élément de G est dit fortement réel s'il est produit de deux involutions.

Lemme 4. Soit x *un élément fortement réel de* G *tel que* $x^2 \neq 1$. *Alors* x *est conjugué dans* G *à un élément de la forme* ut,u $\in Q_o^{\#}$, *et* $|C_G(x)|$ *est impair.*

Soit $x = uv$, $u,v \in \mathrm{Inv}(G)$. Puisque les involutions de H commutent deux à deux (§1) mais $x^2 \neq 1$, on a $H(u) \neq H(v)$. La première assertion résulte du corollaire 1 du théorème A (chap. I, §6). Ensuite, $N_G(\langle x\rangle) \cap H(u)$ est un groupe de Bender propre de $N_G(\langle x\rangle)$, donc $N_G(\langle x\rangle)$ a une seule classe d'involutions. Comme $C_G(x) \lhd N_G(\langle x\rangle)$ et $u \in N_G(\langle x\rangle) - C_G(x)$, il en résulte que $|C_G(x)|$ est impair.

Lemme 5. Supposons que st *soit d'ordre* 3 *et que* $V \neq 1$. *Alors* $\langle Q_o,K,t\rangle = Q_oK \cup Q_oKtQ_o$ *est isomorphe à* PSL(2,q).

On a $tst = sts$ car st est d'ordre 3. Donc pour $k \in K$, $ts^kt = ktstk^{-1} = ksk^{-1}.k^2t.ksk^{-1}$, d'où $tQ_ot \subset Q_oKtQ_o$. Compte tenu de ce que t normalise K et K normalise Q_o , cela prouve que $Q_oK \cup Q_oKtQ_o$ est un sous-groupe de G, d'ordre $q(q-1)(q+1)$. Ce sous-groupe est d'ordre $< |G|$, car $V \neq 1$, et a un groupe de Bender propre Q_oK, donc ne peut qu'être isomorphe à PSL(2,q) d'après l'hypothèse de récurrence. (En fait, l'hypothèse $V \neq 1$ est inutile, car on voit facilement que la loi de composition de $Q_oK \cup Q_oKtQ_o$ est déterminée de manière unique si q est donné).

Lemme 6. Supposons que st *soit d'ordre* 3 *et que* Q *soit un 2-groupe de Suzuki d'ordre* q^3 . *Alors* W *est un groupe cyclique et* |W| *divise* q+1 . *Si de plus* $W \neq 1$, *alors* Q *est un 2-groupe de Suzuki de type* B .

Soit $w \in W^{\#}$. Puisque $Q_o \subset C_Q(w)$ et st est d'ordre 3, le lemme 2 montre que $C_Q(w) = Q_o$ ou Q , mais puisque D opère fidèlement sur $\Omega - \{H\}$, on a $C_Q(w) = Q_o$. Soit X un K-sous-groupe d'ordre q^2 de Q (un tel sous-groupe existe d'après la description des 2-groupes de Suzuki). Supposons que $X^w = X$. Puisque w centralise s et $|\{x \in X/x^2 = s\}| = (q^2 - q)/(q-1) = q$, w centra-

lise un élément de $\{x \in X/x^2 = s\}$, ce qui contredit $C_Q(w) = Q_o$. Donc $X^w \neq X$ et puisque w centralise K, X^w est un K-sous-groupe de Q isomorphe à X comme K-groupe. D'après [Hi], il en résulte que si $W \neq 1$, Q est un 2-groupe de Suzuki de type B et qu'on peut identifier K à $\mathbb{F}_q^*$ et $\bar{Q} = Q/Q_o$ à un espace vectoriel de dimension 2 sur $\mathbb{F}_q$ de manière que K opère sur $\bar{Q}$ comme le groupe des homothéties non nulles de $\bar{Q}$.

Alors W s'identifie à un sous-groupe de $GL(\bar{Q}) \cong GL(2,q)$. De plus W opère sans point fixe sur l'ensemble des q+1 K-sous-groupes d'ordre q^2 de Q, donc $|W|$ divise q+1, et W est cyclique d'après la structure des sous-groupes de GL(2,q) (voir [H], chap. II, §8).

§3.- LE THÉORÈME F

Nous supposerons dans ce paragraphe :

(F1) *V a un sous-groupe* P *d'ordre premier* p *tel que* $C_G(P)$ *soit de 2-rang 1.*

Remarquons qu'on a alors $C_K(P) = 1$. Nous démontrerons ici :

Théorème F. Sous l'hypothèse (F1), *la conclusion du théorème* B *est vraie pour* G.

Remarque : Si G est l'un des groupes qui figurent dans la conclusion du théorème B et si les hypothèses (B0), (B2) et (F1) sont satisfaites, alors $G = G_o \rtimes P$ où G_o est isomorphe à $PSL(2,2^p)$, $Sz(2^p)$, $PSU(3,2^p)$ ou $PGU(3,2^p)$.

Si G a un sous-groupe normal d'indice p, la conclusion du théorème est vraie d'après l'hypothèse de récurrence (B1). On supposera donc :

(F2) *G n'a pas de sous-groupe normal d'indice* p.

(1) *On a* $V = W \rtimes P$, $|Q_o| = 2^p$, $N_G(P) = C_G(P)$ *et* $C_D(P) = C_W(P) \times P$.

Puisque $P \cap W = 1$, P opère comme un groupe d'automorphismes de corps

sur Q_o (§1, prop. 3). Alors $|C_{Q_o}(P)| = 2$ implique que $|Q_o| = 2^p$ et puisque V/W s'identifie à un sous-groupe de $Aut(\mathbb{F}_{2^p})$, on a $V = W \rtimes P$. On a $N_G(P) = C_G(P)N_V(P)$ (§2, lemme 2b)) mais $N_V(P) = C_W(P)P$, donc $N_G(P) = C_G(P)$. On a $C_D(P) = C_K(P)C_V(P) = C_V(P)$ d'après (F1).

(2) a) $(C_G(P), C_H(P)) \in \bar{F}$ *et son noyau est* $N = C_D(C_Q(P)) \cap C(P)$.

b) *Il existe un presque-corps* F *tel que* $C_G(P)/N = (F \rtimes C_Q(P)) \rtimes \Sigma$ *avec* $C_Q(P) \cong F^*$, $\Sigma = \overline{C_W(P)}$ *s'identifie à un groupe d'automorphismes de* F, $C_Q(P) \rtimes \Sigma$ *opérant de façon naturelle sur* F.

a) résulte du §2, lemme 2 a) ; b) résulte alors du §2, lemme 1 c) et de la prop. 1 de l'appendice XI.

(3) *Pour tout nombre premier* r *tel que* $r \mid |Q_1|$, *il existe* i *tel que* $0 \leq i \leq p-1$ *et* $r \equiv 2^i \pmod{2^p-1}$. *En particulier,* $r \neq p$.

Soit M un r-sous-groupe abélien élémentaire de Q_1 normalisé par KP, tel que $M \neq 1$ et minimal pour ces propriétés. On note additivement la loi de composition de M. Puisque KP est un groupe de Frobenius et K opère sans point fixe sur M, on a $C_M(P) \neq 0$ et $C_M(P)$ est de dimension 1 sur $\mathbb{F}_r$ d'après (2) b).

De plus, d'après [Is] (15-16), on a $\dim M = p \dim C_M(P) = p$ (dimensions sur $\mathbb{F}_r$). D'après le théorème de Clifford ([Is](5-5)), M est somme directe de $\mathbb{F}_r[K]$-modules irréductibles ayant tous même dimension, et puisque $\dim M$ est premier, ou bien M a un sous-$\mathbb{F}_r[K]$-module de dimension 1 sur $\mathbb{F}_r$, ou bien M est irréductible comme $\mathbb{F}_r[K]$-module.

Dans le premier cas, puisque K opère sans point fixe sur M et $|K| = 2^p - 1$, on a $r \equiv 1 \pmod{2^p - 1}$. Supposons qu'on soit dans le deuxième cas. D'après l'appendice V, on peut munir M d'une structure de corps telle que $K \rtimes P$ soit un groupe d'applications semi-linéaires : $M \to M$, et $P = Aut(M)$ car $\dim M = p$. Il existe donc $a \in P^\#$ tel que $x^a = x^r$ pour tout $x \in K$. D'après la prop. 3

du §1, $K \rtimes P$ s'identifie aussi au groupe des applications semi-linéaires $\neq 0$: $\mathbb{F}_{2^p} \to \mathbb{F}_{2^p}$. Il existe donc i tel que $1 \leq i \leq p-1$ et $x^a = x^{2^i}$ pour tout $x \in K$. Il en résulte que $r \equiv 2^i \pmod{2^p-1}$.

(4) $|Q| = |C_Q(P)|^p = |F^*|^p$.

Puisque KP est un groupe de Frobenius de noyau K, on a $\sum_{x \in K} P^x + K = KP + |K|.1$ dans $\mathbb{Z}[KP]$. En appliquant la formule des points fixes de Wielandt ([HB], chap.XI, (12-4)) pour KP opérant sur Q, on obtient alors $|C_Q(P)|^p = |Q|$.

(5) *Supposons que* F *ne soit pas un corps, c'est à dire que* $C_Q(P)$ *ne soit pas abélien. Alors* F *est isomorphe au presque-corps* $F_{9,2}$ *et* $Q_1 = 1$.

D'après (2), $C_Q(P)$ est un complément de Frobenius. Puisque Q est nilpotent, il en résulte que $C_{Q_1}(P)$ est cyclique, et si $C_Q(P)$ n'est pas abélien, $C_S(P)$ n'est pas abélien. D'après le §1, corollaire de la prop. 2, S est alors un 2-groupe de Suzuki, donc d'exposant 4. Puisque $C_S(P)$ est de 2-rang 1, il est donc quaternionien d'ordre 8.

Le groupe $F^* \cong C_Q(P)$ a un sous-groupe cyclique d'indice 2, donc F est isomorphe à un presque-corps $F_{r^2,2}$ et $|Z(F^*)| = r-1$ (appendice XI, prop. 2). D'après la structure $C_Q(P)$, on a $|F^*/Z(F^*)| = 4$ mais $|F^*/Z(F^*)| = (r^2-1)/(r-1) = r+1$, donc $r = 3$, $|C_Q(P)| = 8$, et $Q_1 = 1$ d'après (4).

Soit f l'ordre de st. Alors f est la caractéristique de F d'après (2), le lemme 1 c) du §2 et l'appendice III, (4).

(6) *Supposons que* $Q_1 = 1$. *Si* $F \cong F_{9,2}$, *alors* $|\Sigma| = 1$ *ou* 3. *Sinon,* $|F| = f$ *ou* 9 *et* $\Sigma = 1$.

Un groupe d'automorphismes d'ordre impair de $F_{9,2}$ ne peut être que d'ordre 1 ou 3 car $F^*_{9,2}$ est quaternionien d'ordre 8. Supposons que $F \not\cong F_{9,2}$.

D'après (5), F est un corps et F^* est un 2-groupe par hypothèse. Si $|F| = f^a$, il existe donc un entier b tel que $f^a = 2^b + 1$. D'après un lemme arithmétique ([HB], chapitre IX,(2-7)), il en résulte que $a = 1$ ou $f^a = 9$. Puisque $|\Sigma|$ est impair, on a donc $\Sigma = 1$.

(7) *On a* $N = P$ *et* $\Sigma \cong C_W(P)$. (N a été défini dans (2) a))

D'après (1), $N = (N \cap W) \times P$. Supposons que $N \cap W \neq 1$. Si $R = C_Q(N \cap W)$, d'après le lemme 2 c) du §2, on a $f = 3$ et $|R| = |Q_o|$ ou $|Q_o|^3$, ou $f = 5$ et $|R| = |Q_o|^2$. Puisque N centralise $C_Q(P)$, on a $C_Q(P) \subset R$, et Q est un 2-groupe d'après (4). D'après (6) et (2) b), on est donc dans l'un des 3 cas :

a) $|F| = 3$, $|C_Q(P)| = 2$; b) $|F| = 9$, $|C_Q(P)| = 8$; c) $|F| = 5$, $|C_Q(P)| = 4$

D'après (4), on a respectivement pour chaque cas :

a) $|Q| = |Q_o|$; b) $|Q| = |Q_o|^3$; c) $|Q| = |Q_o|^2$

Puisque $N \cap W$ opère fidèlement sur Q, $Q_o \subset R \subset_{\neq} Q$, donc le cas a) est impossible. Dans les cas b) et c), $C_Q(P)$ a un élément d'ordre 4 car $|C_{Q_o}(P)| = 2$, donc $Q_o \subset_{\neq} R \subset_{\neq} Q$. Donc c) est impossible et dans le cas b), $|R| = |Q_o|^2$ d'où $f = 5$, ce qui est absurde.

(8) *Supposons que* $Q_1 \neq 1$. *Soit* $\ell = |\Sigma|$. *Si* $\ell \neq 1$, *alors* ℓ *est premier et* F *est un corps de cardinal* 3^ℓ, 5^ℓ *ou* 9^ℓ.

D'après (5), F est un corps. Soit $w \in C_W(P)^\#$. D'après l'hypothèse de récurrence, on a $f = 3$ ou 5 et $C_Q(w)$ est un 2-groupe, donc $C_{F^*}(w)$ est un 2-groupe. Puisque $C_{F^*}(w)$ est le groupe multiplicatif du corps des points fixes de w dans F, il existe des entiers a et b tels que $|C_F(w)| = f^a$ et $f^a = 2^b + 1$. On a donc $|C_F(w)| = f$ ou 9. De plus, si $f = 3$, il ne peut exister w_1 et $w_2 \in C_W(P)^\#$ tels que $|C_F(w_i)| = 3^i$ $(i = 1,2)$, sinon w_1 serait d'ordre pair. Donc $|C_F(w)|$ est indépendant de $w \in C_W(P)^\#$, donc $\ell = |C_W(P)|$ est premier et $|F| = |C_F(w)|^\ell$.

(9) *Supposons que* $Q_1 \neq 1$. *Alors* $p = f \neq \ell$.

D'après (F2) et le théorème de transfert de Burnside, P n'est pas un

p-Sylow de G, donc d'après (2) et (7), p divise $|F|.|F^*|.|\Sigma|$. D'après (3), $p \nmid |F^*|$ donc d'après (8), on a $p = f$ ou $p = \ell$. Supposons $p = f = \ell$. D'après (8), $|F| = 3^3$, 5^5 ou 9^3 , d'où $|C_Q(P)| = |F|-1 = 2.13$, 4.11.71 ou 8.7.13 respectivement. Mais cela contredit (3) car $13 \equiv 2^i \pmod 7$, $0 \leq i \leq 2$ et $11 \equiv 2^i \pmod{31}$, $0 \leq i \leq 4$ sont impossibles.

Supposons $p = \ell \neq f$. D'après (8), on a $|F| = 3^p$, 5^p ou 9^p et d'après (4), $|Q| = (3^p-1)^p$, $(5^p-1)^p$ ou $(9^p-1)^p$. Puisque $p \neq f$, on a $|Q| \equiv 2$, 4 ou $8 \pmod p$, donc $|Q| + 1 \equiv 3,5$ ou $9 \pmod p$, donc $p \nmid (|Q|+1)$. Puisque $|G| = (|Q|+1)|H|$, il en résulte que si T est un p-Sylow de W normalisé par P, TP est un p-Sylow de G. D'après l'hypothèse de récurrence pour $C_G(w)$, $w \in W^\#$, W opère sans point fixe sur Q_1 , donc T est cyclique et TP est nilpotent de classe $\leq 2 < p$ (voir [H], chap. I, (14-9)). D'après le théorème de Hall-Wielandt, on a $G/O^p(G) \cong$ $\cong N_G(TP)/O^p(N_G(TP))$.

D'après le lemme 2 b) du §2, $N_G(TP) = C_G(TP)N_V(TP)$, donc $[N_G(TP),TP] =$ $= [N_V(TP),TP]$. Mais $[N_V(TP),TP] \subset (TP) \cap W = T$ car V/W est abélien, donc $T \lhd N_G(TP)$ et $N_G(TP)$ centralise (TP)/T . Cela implique que $N_G(TP)$ a un quotient d'ordre p car si R est un complément de TP dans $N_G(TP)$ (théorème de Zassenhaus), $N_G(TP)/T = (TP)/T \times (TR)/T$, donc $TR \lhd N_G(TP)$. Ainsi, G a un quotient d'ordre p, ce qui contredit l'hypothèse (F2).

(10) *Posons* $|F| = f^m$. *On a* $p = f$ *et on est dans l'un des 2 cas suivants :*

(10-1) $p \nmid |\Sigma|$ *et* $|G|_p = p^{m+2}$

(10-2) $p = |\Sigma| = 3$, $F \cong F_{9,2}$, W *est cyclique d'ordre 3 ou 9 et* $|G|_3 = 3^4|W|$.

Si $p \nmid |\Sigma|$, alors $p = f$ d'après (F2) et le théorème de transfert de Burnside. Si $p||\Sigma|$, on a $Q_1 = 1$ d'après (9), donc $p = |\Sigma| = 3$ et $F \cong F_{9,2}$ d'après (6).

Dans les deux cas, $|F^*| = p^m - 1$ donc d'après (4),

$|Q| + 1 = 1 + (-1 + p^m)^p = 1 - 1 + p.p^m - \binom{p}{2}p^{2m} + \ldots + p^{pm} \equiv p^{m+1} (\text{mod. } p^{m+2})$

donc $(|Q| + 1)_p = p^{m+1}$. On a $|G|_p = (|Q| + 1)_p |H|_p = p^{m+1}.|W|_p.p.$

Si $p \nmid |\Sigma|$, alors $p \nmid |C_W(P)|$ donc $p \nmid |W|$, d'où $|G|_p = p^{m+2}$.

Si $p \mid |\Sigma|$, alors $|Q| = |F^*|^p = 8^3$. Puisque $C_Q(P) \tilde{=} F^*$ n'est pas abélien, Q est un 2-groupe de Suzuki et W est cyclique d'ordre 3 ou 9 d'après le lemme 6 du §2. De plus, $|G|_3 = 3^{m+2}|W|_3 = 3^4|W|$.

Remarque : Si on ne suppose pas (F2), le cas (10-2) est obtenu effectivement pour G isomorphe à PSU(3,8) $\rtimes$ Aut $\mathbb{F}_8$ ou PGU(3,8) $\rtimes$ Aut $\mathbb{F}_8$.

(11) *Soit* R *l'image réciproque de* F *dans* G. *Alors* $R = T \times P$, *où* T *est un sous-groupe normalisé par* $C_Q(P)C_W(P)$, *et* $T \rtimes C_Q(P) \tilde{=} F \rtimes F^*$. *De plus,* $C_Q(P)$ *opère régulièrement sur* $A-\{P\}$, *A étant l'ensemble des sous-groupes d'ordre* p *de* R *qui ne sont pas dans* T .

Supposons R non abélien. Alors $[R,R] = Z(R) = P$ car $C_Q(P)$ est transitif sur F^*. On a $N(R) \subset N(P)$, et dans le cas (10-1), R est un p-Sylow de N(P), donc de G. Mais $|R| = p^{m+1}$, ce qui contredit (10). Dans le cas (10-2), $R\,C_W(P)$ est un 3-Sylow de N(P). Puisque Σ opère non trivialement sur $R/P \tilde{=} F$, on a $Z(RC_W(P)) = Z(R) = P$, donc $N(RC_W(P)) \subset N(P)$ et $RC_W(P)$ est un 3-Sylow de G. Mais $|RC_W(P)| = 3^4$, ce qui contredit (10).

Donc R est abélien et la première assertion est vérifiée avec $T = [R,s]$.

On a $|A| = (p^{m+1} - p^m)/(p-1) = p^m = |F|$. Pour la deuxième assertion, il suffit donc de montrer qu'un élément a de $C_Q(P)^\#$ ne normalise aucun élément de $A-\{P\}$. Soit $P_1 \in A$ tel que a normalise P_1 . Puisque a normalise T et centralise $R/T \tilde{=} P$, $[a,P_1] \subset P_1 \cap T = 1$ et a centralise P_1 . Mais a opère sans point fixe sur R/P, donc $C_R(a) = P$, d'où $P_1 = P$.

(12) *On est dans le cas (10-2).*

Supposons qu'on soit dans le cas (10-1).

D'après (10), R n'est pas un p-Sylow de $N_G(R)$, donc $N_G(P) \subset_{\neq} N_G(R)$. Soit $\mathcal{A}'$ l'orbite de P par $N_G(R)$. Soit $P_1 \in \mathcal{A}'$. Puisque P_1 est conjugué à P, les éléments de $P_1^{\#}$ ne sont pas fortement réels (§2, lemme 4). Mais les éléments de T sont inversés par s, donc $P_1 \cap T = 1$ et $\{P\} \subsetneq \mathcal{A}' \subset \mathcal{A}$. Puisque $C_Q(P)$ opère régulièrement sur $\mathcal{A}-\{P\}$, il en résulte que $\mathcal{A}' = \mathcal{A}$.

On a donc $|N_G(R) : N_G(P)| = |\mathcal{A}| = p^m$. D'après (10), on a alors $m = 1$ et $|G|_p = |N_G(R)|_p = p^3$.

Dans $N_G(R)/R$, on a $\overline{C(P)} = \overline{C_Q(P)} \rtimes \overline{C_W(P)}$, $\overline{C_Q(P)}$ opère régulièrement sur $\mathcal{A}-\{P\}$ et $\overline{C_W(P)}$ opère fidèlement sur $\overline{C_Q(P)}$. On peut donc appliquer la proposition 1 de l'appendice XI à $N_G(R)/R$ opérant sur $\mathcal{A}$, donc $N_G(R)/R = (R_1/R) \rtimes C_Q(P)C_W(P)$ où R_1 est un p-Sylow de G et $C_Q(P)$ opère régulièrement sur $(R_1/R)^{\#}$.

Puisque R_1 est non-abélien d'ordre p^3, R_1 est de classe $2 < p$ et on a $G/O^p(G) = N_G(R_1)/O^p(N_G(R_1))$ d'après le théorème de Hall-Wielandt.

Puisque $N_G(R)$ opère transitivement sur $\mathcal{A}$, on a $T \lhd R_1$; puisque R_1/T est abélien et $C_{R_1/R}(s) = 1$, on a $R_1/T = (R/T) \times (T_1/T)$ où $T_1 = [R_1/T, s]$. Si $\mathcal{A}_1$ est l'ensemble des sous-groupes d'ordre p de R_1/T distincts de T_1/T, on voit comme dans (11) que $C_Q(P)$ opère régulièrement sur $\mathcal{A}_1-\{R/T\}$, puis comme ci-dessus que si $N_G(R) \subset_{\neq} N_G(R_1)$, alors $N_G(R_1)$ opère transitivement sur $\mathcal{A}_1$ et $|N_G(R_1):N_G(R)| = |\mathcal{A}_1| = p$, ce qui est contraire à (10). Donc $N_G(R_1) = N_G(R)$. Puisque T_1 est normalisé par $C_Q(P)C_W(P)$ et par P, $T_1C_Q(P)C_W(P)$ est un sous-groupe normal d'indice p de $N_G(R_1)$ et l'hypothèse (F2) est contredite.

Nous terminons maintenant la démonstration dans le cas (10-2). Pour une autre méthode possible de démonstration dans ce cas, voir la remarque à la fin du §3 du chap. VII.

On pose $\Sigma = C_W(P)$ et $Z_1 = \langle st \rangle$.

(13) $C_G(Z_1)$ *est un 3-groupe.*

D'après l'appendice I et le lemme 4 du §2, on a $|C_G(Z_1)| = |C_G(Z_1) \cap C(s)|.|J|$ où $J = \{x \in C_G(Z_1)/x^s = x^{-1}\}$. On a $C(Z_1) \cap C(s) = C(t) \cap C(s) = V = WP$. Il suffit donc de montrer que $|J|$ est une puissance de 3. Soit r un diviseur premier de $|J|$. Alors J contient un élément x d'ordre r ; puisque x est fortement réel, x est conjugué dans G à un élément de $\langle Q_o, K, t\rangle \cong PSL(2,8)$ (lemmes 4 et 5 du §2) . Puisque $|PSL(2,8)| = 8.9.7$, on a r=3 ou 7. Mais si r=7, x est conjugué à un élément de $K^\#$ et $C_G(x)$ est conjugué à $C_G(K) = K \times W$ (rappelons que les éléments de $K^\#$ n'ont que 2 points fixes), donc x ne peut centraliser un élément fortement réel d'ordre 3.

(14) *Avec la notation de* (11), $Z(R\Sigma) = Z_1P$. *Il existe un 3-sous-groupe* R_1 *de* G *tel que* $N_G(R\Sigma)/R\Sigma = (R_1/R\Sigma) \rtimes \langle s\rangle \cong \mathfrak{S}_3$. *Soit* R_2 *un 3-Sylow de* G *contenant* R_1 . *Alors* $|R_2:R_1| = 1$ *ou* 3 , $Z_1 = Z(R_1) = Z(R_2)$ *et* $R_2 = C_G(Z_1)$.

On a $Z_1P \subset Z(R\Sigma)$ (remarquer que $Z_1 \subset T$), $|R\Sigma/Z_1P| = 9$ et $R\Sigma$ est non-abélien, donc $Z_1P = Z(R\Sigma)$. Puisque $Z_1 = [R\Sigma, R\Sigma]$, $N_G(R\Sigma)$ opère sur l'ensemble $\mathcal{A}_2$ des sous-groupes d'ordre 3 de Z_1P distincts de Z_1 . On a $\mathcal{A}_2 \subset \mathcal{A}$ donc $\langle s\rangle$ opère régulièrement sur $\mathcal{A}_2 - \{P\}$ d'après (11). D'après (10), $R\Sigma$ n'est pas un 3-Sylow de G, donc $N_G(R\Sigma) \not\subset N_G(P)$. Il en résulte que $N_G(R\Sigma)$ induit le groupe $\cong \mathfrak{S}_3$ de toutes les permutations de $\mathcal{A}_2$. Le noyau de l'opération de $N_G(R\Sigma)$ sur $\mathcal{A}_2$ est $R\Sigma$ car ce noyau est inclus dans $N_G(P) = RC_Q(P)\Sigma$ et les éléments de $C_Q(P)^\#$ sont sans point fixe sur $\mathcal{A} - \{P\}$. L'existence de R_1 résulte alors de la structure de $\mathfrak{S}_3$.

On a $|R_2:R_1| = 1$ ou 3 d'après (10). On a $Z(R_1) \subset C_{R_1}(P) = R\Sigma$, donc $Z(R_1) \subset Z(R\Sigma) = Z_1P$. D'après la transitivité de R_1 sur $\mathcal{A}_2$, $Z(R_1) = Z_1$. On a $Z(R_2) \subset R_2 \cap C_G(P) \subset R_1$ d'où $Z(R_2) = Z(R_1) = Z_1$. On a donc $R_2 \subset C_G(Z_1)$ et $R_2 = C_G(Z_1)$ d'après (13).

(15) *Il existe un sous-groupe* L *de* R_1 *tel que* L *soit cyclique d'ordre 9, in-*

versé par s, *normalisé par* V, *centralisé par* W *mais pas par* P. *On a* $|R_2:LV| = 3$, $Z(LV) = Z_1\Sigma$ *et* $\Omega_1(LV) = Z_1\Sigma P$.

Soit $L = C_G(st) \cap \langle Q_o,K,t\rangle$. Puisque $\langle Q_o,K,t\rangle \cong PSL(2,8)$, L est cyclique d'ordre 9 et ses éléments sont inversés par s. On a $L \subset \langle Q_o,K,t\rangle \subset C_G(W)$. Puisque P normalise $\langle Q_o,K,t\rangle$ et centralise st, P normalise L, mais ne le centralise pas d'après la structure de $C_G(P)$ ($T\Sigma$ est d'exposant 3). Puisque $|LP:Z_1P| = 3$, L normalise Z_1P donc L normalise $C_G(Z_1P) = C_G(P) \cap C_G(st) = R\Sigma$, donc $L \subset R_1$. D'après (10), $|R_2:LV| = 3$. On a $Z_1\Sigma \subset Z(LV)$ et $Z(LV) \subset LW$ car LV est non-abélien, donc $Z(LV) \subset C_{LW}(P) = Z_1\Sigma$. Puisque $LV/Z_1\Sigma$ est abélien, $\Omega_1(LV)$ est l'ensemble des éléments d'ordre ≤ 3 de LV ([H], chap. III, 1-3-b). On a $Z_1\Sigma P \subset \Omega_1(LV)$ et $\Omega_1(LW) = Z_1\Sigma$ donc $\Omega_1(LV) = Z_1\Sigma P$.

(16) *On a* $Z_1P\Sigma \subset Z_2(R_1)$, Z_1 *est le seul sous-groupe d'ordre 3 de* $Z_1P\Sigma$ *formé d'éléments fortement réels et* $N_G(Z_1P\Sigma) = N_G(Z_1) = R_2\langle s\rangle$.

D'après (14), $Z(R_1) = Z_1 \subset Z_1P = Z(R\Sigma) \lhd R_1$, donc $Z_1P \subset Z_2(R_1)$. D'après (15), $Z_1\Sigma = Z(LV) \lhd R_1$ donc $Z_1\Sigma \subset Z_2(R_1)$. Soit X un sous-groupe d'ordre 3 de $Z_1P\Sigma$ formé d'éléments fortement réels tel que $X \cap Z_1 = 1$. Puisque $Z(R_1) = Z_1 \subset Z_1X \subset Z_2(R_1)$, R_1 permute transitivement les sous-groupes d'ordre 3 de Z_1X distincts de Z_1 . Donc les éléments de Z_1X sont fortement réels, ce qui est absurde car $(Z_1X) \cap (P\Sigma) \neq 1$.

On a donc $N_G(Z_1P\Sigma) \subset N_G(Z_1) = C_G(Z_1)\langle s\rangle$ et $C_G(Z_1) = R_2$ d'après (14). D'autre part, $Z_1P\Sigma = \Omega_1(LV)$ est normal dans $R_2\langle s\rangle$.

(17) *Conclusion.*

Soit $x \in G$ tel que $(Z_1P\Sigma)^x \subset R_2$.

Supposons que $Z_1^x \not\subset LV$. Alors $R_2 = (LV) \rtimes Z_1^x$ et $(Z_1P\Sigma)^x = A \times Z_1^x$ où A est un sous-groupe de type (3,3) de LV. On a $A \subset \Omega_1(LV) = Z_1\Sigma P$. D'après (16), les éléments de $A^\#$ ne sont pas fortement réels, donc $A \cap Z_1 = 1$ et $Z_1\Sigma P = Z_1A$. Il en résulte que Z_1^x centralise $Z_1\Sigma P$, donc $Z_1\Sigma \subset Z(R_2)$ ce qui

contredit (14).

Donc $Z_1^x \subset \Omega_1(LV) = Z_1 \Sigma P$, d'où $Z_1^x = Z_1$ d'après (16) et $x \in N_G(Z_1) = R_2\langle s\rangle$, donc x normalise $Z_1 P\Sigma$.

Le sous-groupe $Z_1 P\Sigma$ de G est donc faiblement fermé dans R_2 , et puisque $Z_1 P\Sigma$ est abélien, on a $G/O^3(G) \cong R_2\langle s\rangle/O^3(R_2\langle s\rangle)$ d'après le théorème de Hall-Wielandt.

Si $\overline{R}_1 = R_1/Z_1$, $\overline{R}_1$ est engendré par les sous-groupes $\overline{R\Sigma} = \overline{T} \times \overline{P} \times \overline{\Sigma}$ et $\overline{L\Sigma P} = \overline{L} \times \overline{\Sigma} \times \overline{P}$ car $L \not\subset R\Sigma$. Donc $[\overline{R}_1 , \overline{R}_1]$ est le sous-groupe normal de $\overline{R}_1$ engendré par un commutateur $[\overline{x},\overline{y}]$ où $\overline{x} \in \overline{T}^{\#}$ et $\overline{y} \in \overline{L}^{\#}$. Mais $\overline{R}_1$ est de classe ≤ 2 car $Z_1 P\Sigma \subset Z_2(R_1)$ et $|R_1 : Z_1 P\Sigma| = 9$. Donc $[\overline{x},\overline{y}] \in Z(\overline{R}_1)$ et $[\overline{R}_1 , \overline{R}_1]$ est d'ordre 1 ou 3. Puisque s centralise $\overline{\Sigma}\overline{P}$, $\overline{R}_1/[\overline{R}_1 , \overline{R}_1]$ a donc un sous-groupe d'ordre 3 centralisé par s, donc $(\overline{R}_1/[\overline{R}_1 , \overline{R}_1]) \rtimes \langle s\rangle$ a un quotient d'ordre 3. Si $|W| = 3$, on a $R_2 = R_1$ et l'hypothèse (F2) est alors contredite.

Donc $|W| = 9$. D'après (14), s inverse les éléments de $R_1/R\Sigma$ donc $C_{R_1}(s) \subset R\Sigma$ et $C_{R_1}(s) = P\Sigma$, donc $W \not\subset R_1$. Il en résulte que $R_2 = R_1 W$, donc s centralise R_2/R_1 et $R_1\langle s\rangle \lhd R_2\langle s\rangle$. L'hypothèse (F2) est encore contredite.

CHAPITRE VI. STRUCTURE DE H

§1.- STRUCTURE DE Q

Supposons que $V = 1$. Alors G est 2-transitif sur Ω, les éléments de $D^{\#}$ n'ont que deux points fixes (chap.II, §4, prop. 2) et G n'a pas de sous-groupe normal régulier sur Ω (car $O_{2'}(G) = 1$), donc G est un groupe de Zassenhaus. D'après [HB], chapitre XI, théorème 11.16, G est isomorphe à PSL(2,q) ou à Sz(q) et la conclusion du théorème B est vraie. Compte tenu du théorème F, on supposera donc désormais :

(B3) $V \neq 1$ *et pour tout sous-groupe* P *d'ordre premier de* V, $C_G(P)$ *est de 2-rang* ≥ 2 .

Théorème G. Q *est un 2-groupe.*

Supposons que $Q_1 \neq 1$. Soit P un sous-groupe d'ordre premier de D. Si $|\Omega_P| = 2$, on a $C_H(P) \subset D$ donc $C_Q(P) = 1$. Si $|\Omega_P| \geq 3$, P est conjugué dans D à un sous-groupe de V (chap. II, §4, prop.2), donc d'après (B3) et le lemme 2 c) du §2 du chapitre V, $C_{Q_1}(P) = 1$. Donc D opère sans point fixe sur Q_1 . De plus, pour $x \in G-H$, $Q \cap Q^x \subset Q \cap (H \cap H^x) = 1$ car $H \cap H^x$ est conjugué à D dans H. Les hypothèses du théorème de Feit-Sibley, tel qu'il est énoncé dans l'appendice XII, sont donc satisfaites. D'après ce théorème, $S = \{\chi \in \mathrm{Irr}(H) | Q_1 \not\subset \mathrm{Ker}\ \chi\}$ est cohérent pour Ind_H^G .

Soit λ un caractère linéaire $\neq 1_H$ de H tel que $QK \subset \mathrm{Ker}\ \lambda$. Un tel caractère existe car $H/QK \cong V$ est résoluble et $\neq 1$.

Puisque $D = KV$ opère sans point fixe sur Q_1, on a $(|K|,|V|) = 1$ donc QK est un sous-groupe de Hall de H.

Soient $x \in H$ et $g \in G$ tels que $x^g \in H$. Montrons que $\lambda(x^g) = \lambda(x)$. Si π est l'ensemble des diviseurs premiers de $|QK|$ et y est la π'-composante de x, on a $\lambda(x) = \lambda(y)$ et $\lambda(x^g) = \lambda(y^g)$ car la π-composante de x est dans QK. On peut donc supposer que x est un π'-élément. Alors x et x^g sont conjugués à des éléments de V dans H, d'après un théorème de Hall, et on peut supposer que $x \in V$ et $x^g \in V$. D'après le lemme 3 du §2 du chapitre V, x et x^g sont conjugués dans V, donc $\lambda(x) = \lambda(x^g)$.

D'après la définition de Ind_H^G, il en résulte que pour $x \in H$, on a $(\mathrm{Ind}_H^G\lambda)(x) = \lambda(x)(\mathrm{Ind}_H^G 1_H)(x)$, donc :

$$[\mathrm{Ind}_H^G\lambda,\mathrm{Ind}_H^G\lambda] = [\mathrm{Res}_H^G \mathrm{Ind}_H^G\lambda,\lambda] = [\lambda\mathrm{Res}_H^G \mathrm{Ind}_H^G 1_H ,\lambda] = [\mathrm{Res}_H \mathrm{Ind}_H^G 1_H, 1_H] =$$

$$[\mathrm{Ind}_H^G 1_H,\mathrm{Ind}_H^G 1_H] = 2$$

car $|\lambda(x)| = 1$ pour $x \in H$ et G est 2-transitif sur Ω.

Posons $\mathrm{Ind}_H^G\lambda = f_1 + f_2$, avec $f_i \in \mathrm{Irr}(G)$ $(i = 1,2)$. On a $[\mathrm{Ind}_H^G\lambda,1_G] = [\lambda,1_H] = 0$, donc $f_i \neq 1_G$.

Soit $S = \{\chi_1, \ldots, \chi_n\}$, avec $\chi_i(1) = a_i|D|$ et $a_1 = 1$, et soient $e_i \in \pm \mathrm{Irr}(G)$ tels que $\mathrm{Ind}_H^G(\chi_i - a_i\chi_1) = e_i - a_ie_1$ pour $i \geq 2$, qui existent d'après la cohérence de S.

Supposons que $f_1 = \pm e_i$ pour un i. Remarquons que $\bar{\chi}_i \neq \chi_i$ car d'après le lemme 2 de l'appendice XII, la restriction de χ_i au groupe d'ordre impair Q_1D est irréductible, et $\bar{\chi}_i \in S$. Il existe donc $e_i' \in \{e_j/j \neq i\}$ tel que $\mathrm{Ind}_H^G(\chi_i - \bar{\chi}_i) = e_i - e_i'$. On a $\mathrm{Res}_H^G(e_i - e_i') = \chi_i - \bar{\chi}_i$ d'après [Is], 7-7 car Q est un sous-groupe de Hall de H et $\chi_i - \bar{\chi}_i$ s'annule sur H-Q. Donc $[\mathrm{Ind}_H^G\lambda,e_i - e_i'] = [\lambda,\chi_i - \bar{\chi}_i] = 0$, donc $\mathrm{Ind}_H^G\lambda = \pm(e_i + e_i')$ et $|Q| + 1 = (\mathrm{Ind}_H^G\lambda)(1) = \pm 2e_i(1)$ ce qui est impossible car $|Q|$ est pair.

Il en résulte que pour $j = 1$, 2 et $i \geq 2$, $[f_j, e_i - a_i e_1] = 0$, d'où $[\mathrm{Res}_H^G f_j, \chi_i - a_i\chi_1] = 0$. Il existe donc $b_j \in \mathbb{N}$ et ψ_j , caractère de H, tels que $Q_1 \subset \mathrm{Ker}\,\psi_j$ et $\mathrm{Res}_H^G f_j = b_j(\Sigma a_i\chi_i) + \psi_j$. On a alors :

$$|Q| + 1 = f_1(1) + f_2(1) \geq (b_1 + b_2)\,\Sigma a_i\chi_i(1) = (b_1 + b_2)(|H| - |H/Q_1|)/|D|$$

$$= (b_1 + b_2)|S|(|Q_1| - 1) .$$

Donc $(b_1 + b_2)(|Q_1| - 1) \leq |Q_1|$ et $b_1 + b_2 \leq |Q_1|/(|Q_1| - 1) < 2$.

Il en résulte qu'il existe $j \in \{1,2\}$ tel que $b_j = 0$, donc $Q_1 \subset \mathrm{Ker}\, f_j$.

Alors $N = \mathrm{Ker}\, f_j$ est un sous-groupe normal de G tel que $1 \neq N \neq G$ et $O_{2'}(N) \subset O_{2'}(G) = 1$. Cela implique que $S \subset N$ (chap. I, §6, cor. 3) et d'après l'hypothèse de récurrence, $H \cap N = S(D \cap N)$ ce qui est en contradiction avec $Q_1 \subset H \cap N$.

Remarque. Supposons que nous voulions seulement démontrer la conséquence suivante du théorème B : "Si H est un groupe de Bender d'un groupe fini G de 2-rang ≥ 2 et si $O_{2'}(G) = 1$, alors $O_{2'}(H) = 1$" (Cette conséquence est utilisée dans la démonstration d'un théorème de Gorenstein et Walter : voir "composants et p-composants d'un groupe fini" par J.Y. Hée - Publications de l'équipe des groupes finis de Paris, 1980).

La démonstration pourrait alors s'arrêter ici. En effet, chaque fois que nous avons appliqué l'hypothèse de récurrence à un groupe F d'ordre $< |G|$, nous n'avons utilisé que des propriétés de F qui sont maintenant connues pour G (chap. II, hypothèse (B1-a) et démonstration de la prop. 3 du §4 - dans le chap. V, le $3^{\text{ème}}$ cas du lemme 2 c) du §2 n'est utilisé que lorsqu'on sait déjà que $Q = S$) ou bien F était un groupe de Zassenhaus (chap. III, §5, prop.2).

Proposition. On a l'un des 3 cas suivants :

a) $S = Q_o$, st *est d'ordre 3.*

b) S *est un 2-groupe de Suzuki de type* A, st *est d'ordre 5 et* $W = 1$.

c) S *est un 2-groupe de Suzuki de type* B, st *est d'ordre 3 et* $W \neq 1$.

Soit P un sous-groupe d'ordre premier p de V, et si $W \neq 1$, supposons que $P \subset W$. Soit $F = O^{2'}(C_G(P))$ et $\ell = |C_{Q_o}(P)|$. D'après (B3) et le lemme 2 du §2 du chap. V, on a l'un des 3 cas :

st est d'ordre 3, $C_S(P)$ est abélien élémentaire, $F/Z(F) \cong PSL(2,\ell)$.

st est d'ordre 5, $C_S(P)$ est un 2-groupe de Suzuki de type A, $F/Z(F) \cong Sz(\ell)$.

st est d'ordre 3, $C_S(P)$ est un 2-groupe de Suzuki d'ordre ℓ^3, $F/Z(F) \cong PSU(3,\ell)$. On sait que S est abélien ou est un 2-groupe de Suzuki (chap.V, §1).

1) Supposons que S soit abélien.

Alors $C_S(P)$ est abélien, donc st est d'ordre 3 et $C_S(P) \subset Q_o$. Supposons que $S \neq Q_o$. Il existe alors $x \in S$ tel que $x^2 = s$ (car K est transitif sur $Q_o^{\#}$) et puisque S est abélien, $\{y \in S | y^2 = s\} = xQ_o$. Mais P centralise s (chap. V, §2, lemme 3) donc normalise xQ_o de cardinal premier à p, donc $C_S(P) \not\subset Q_o$, ce qui est absurde. Donc $S = Q_o$.

2) Supposons que S soit non-abélien d'ordre q^2.

Alors S est un 2-groupe de Suzuki de type A. Soit $x \in S$ tel que $x^2 = s$. Puisque $|\{y \in S | y^2 = s\}| = (q^2 - q)/(q-1) = q$, on a encore $\{y \in S | y^2 = s\} = xQ_o$, P normalise xQ_o donc $C_S(P)$ est d'exposant 4. Si $W \neq 1$, $C_S(P)$ est un K-sous-groupe de S d'exposant 4 donc $C_S(P) = S$ ce qui est absurde car D opère fidèlement sur S. Donc $W = 1$. D'après la prop. 3 du §1 du chap. V, V opère alors comme un groupe d'automorphismes de corps sur Q_o et d'après le théorème de Galois, $C_V(C_{Q_o}(P)) = P$.

Mais si $G_o = PSU(3,\ell)$, si S_o est un 2-Sylow de G_o et $N_{G_o}(S_o) = S_o \rtimes D_o$, on vérifie que $C_{D_o}(\Omega_1(S_o)) \neq 1$.

Il en résulte que $F/Z(F)$ ne peut pas être isomorphe à $PSU(3,\ell)$, donc puisque $C_S(P)$ est d'exposant 4, $F/Z(F) \cong Sz(\ell)$ et st est d'ordre 5.

3) Supposons que S soit non-abélien d'ordre q^3.

Si S est un 2-groupe de Suzuki de type C ou D, S/Q_o est un $\mathbb{F}_2[K]$-module tel que $S/Q_o = X \oplus Y$, X et Y étant des $\mathbb{F}_2[K]$-modules non isomorphes d'ordre q. Il en résulte que X et Y sont les seuls $\mathbb{F}_2[K]$-sous-modules d'ordre q de S/Q_o . Comme P opère sur $(S/Q_o) \rtimes K$, P normalise donc X et Y .

Supposons que st soit d'ordre 5, donc que $C_S(P)$ soit de type A. Si S est de type B, tout élément d'ordre 4 de S engendre un K-sous-groupe d'ordre q^2, et le nombre des K-sous-groupes d'ordre q^2 de S est q+1 . Puisque P centralise un élément d'ordre 4 de S, il en résulte que P normalise au moins deux K-sous-groupes X, Y d'ordre q^2 de S. Ceci est aussi vrai si S est de type C ou D d'après le paragraphe précédent. Comme dans 2), P centralise alors un $x \in X$ et un $y \in Y$ tels que $x^2 = y^2 = s$. Mais puisque $C_S(P)$ est de type A, il en résulte que $y \in x\Omega_1 C_S(P)$ et $y \in X$, ce qui est absurde. Donc st est d'ordre 3.

Supposons que $W = 1$. Alors, comme dans 2), $C_V(C_{Q_o}(P)) = P$, $F/Z(F)$ n'est pas isomorphe à $PSU(3,\ell)$, et puisque st est d'ordre 3, on est dans le cas où $C_S(P)$ est abélien élémentaire. Mais $[K,P] \rtimes P$ est un groupe de Frobenius opérant sur S/Q_o et $[K,P]$ opère sans point fixe sur S/Q_o , donc $C_{S/Q_o}(P) \neq 1$ et on a une contradiction. Donc $W \neq 1$.

D'après le chapitre V, §2, lemme 6, S est alors de type B.

§2.- LE CAS OÙ st EST D'ORDRE 5

Proposition. Dans le cas b) de la proposition du §1, (SK) ∪ (SKtS) *est un sous-groupe de* G.

Il suffit de montrer que $tSt \subset SKtS$. Soient $f,g : S^{\#} \to S^{\#}$ et $h:S^{\#} \to D$ les applications telles que pour $x \in S^{\#}$, $txt = g(x)\, h(x)\, tf(x)$. L'existence de ces applications résulte de ce que $txt \notin H \cup (Ht) \cup (tH)$ et du chapitre V, §2, lemme 1 . Il suffit donc de montrer que $h(x) \in K$ pour tout $x \in S^{\#}$.

La mise sous forme canonique de $tx^a t = atxta^{-1}$, pour $a \in K$, montre que :

(1) $f(x^a) = f(x)a^{-1}$, $g(x^a) = g(x)a^{-1}$, $h(x^a) = ah(x)a$ $(x \in S^{\#}, a \in K)$.

Il suffit donc de montrer que $h(x) \in K$ pour x parcourant un système de représentants de K-orbites de $S^{\#}$. Soit

(2) $tst = r^{-1}tr$

l'identité de structure de G(chapitre V, §2, lemme 1). On a $(st)^2 = (st)^r$, et st étant d'ordre 5, $(st)^{r^2} \neq st$, donc $r^2 \neq 1$ et r est d'ordre 4.

D'après (2), on a :

(3) $trt = rts$, $tr^{-1}t = str^{-1}$

En particulier $h(s) = h(r) = h(r^{-1}) = 1$. Soit $k \in K - \{1\}$, et soit ℓ l'élément de K tel que $sksk^{-1} = s^{\ell}$. On a :

$$trr^{-k}t = trt.tr^{-k}t = rts.k.str^{-1}.k^{-1} = rt.sksk^{-1}.tk^{-2}r^{-k-1} =$$
$$= r\ell.r^{-1}tr.\ell^{-1}k^{-2}r^{-k-1} = rr^{-\ell^{-1}}\ell^2k^2tr\ell^{-1}k^{-2}r^{-k-1}$$

c'est à dire :

(4) $f(rr^{-k}) = r^{\ell^{-1}k^{-2}}r^{-k^{-1}}$, $g(rr^{-k}) = rr^{-\ell^{-1}}$, $h(rr^{-k}) = \ell^2k^2$.

En particulier, $h(rr^{-k}) \in K$. Il suffit donc de montrer que s, r, r^{-1} et les rr^{-k} , $k \in K^{\#}$, forment un système de représentants de K-orbites de $S^{\#}$, ou puisque $|S^{\#}|/|K| = q + 1 = |K^{\#}| + 3$, que ces éléments sont deux à deux non conjugués par des éléments de K.

D'abord, r étant d'ordre 4 et $|K|$ impair, s, r et r^{-1} sont dans des K-orbites distinctes deux à deux. Si $k \in K^{\#}$ et $rr^{-k} = z \in Q_o$, on a $(r^2)^k = (r^k)^2 = (rz)^2 = r^2$, ce qui est impossible. Donc rr^{-k} est d'ordre 4 et n'est pas K-conjugué à s pour $k \in K^{\#}$.

Il en résulte que pour $k \in K^{\#}$, $f(rr^{-k}) = (rr^{-k\ell})\ell^{-1}k^{-2}$ et $g(rr^{-k}) = rr^{-\ell^{-1}}$ sont d'ordre 4, donc d'après (1) et (3), rr^{-k} n'est K-conjugué ni à r ni à r^{-1}. Il reste à montrer que les rr^{-k} sont dans des K-orbites distinctes deux à deux pour $k \in K^{\#}$.

Puisque K opère régulièrement sur $(S/Q_o)^{\#}$, on peut identifier S/Q_o à $\mathbb{F}_q$ et K à $\mathbb{F}_q^*$ de sorte que l'opération de K sur S/Q_o soit identifiée à l'opération de $\mathbb{F}_q^*$ sur $\mathbb{F}_q$ par multiplication (appendice V). Soit $\alpha : S \to \mathbb{F}_q$ la surjection canonique.

Soient $a \in K$ et $k_1, k_2 \in K^{\#}$ tels que $rr^{-k_2} = (rr^{-k_1})^a$. En appliquant α aux égalités $rr^{-k_2} = (rr^{-k_1})^a$, $h(rr^{-k_2}) = h((rr^{-k_1})^a)$ et $f(rr^{-k_2}) = f((rr^{-k_1})^a)$, on obtient d'après (1) et (4) :

(5) $\quad 1 + k_2 = a(1 + k_1)$

(6) $\quad \ell_2 k_2 = a\ell_1 k_1$

(7) $\quad \ell_2^{-1}k_2^{-2} + k_2^{-1} = a^{-1}(\ell_1^{-1}k_1^{-2} + k_1^{-1})$

avec $sk_isk_i^{-1} = s^{\ell_i}$ $(i = 1, 2)$. Donc, en divisant membre à membre (5) par (6) et en multipliant (6) par (7), si $x_i = \ell_i^{-1}(k_i^{-1} + 1)$ et $y_i = k_i^{-1} + \ell_i$, on a $x_1 = x_2$ et $y_1 = y_2$. Mais on a :

$(x_i + 1)k_i^{-1} = x_iy_i + 1$, donc $k_1 = k_2$ à condition que $x_i \neq 1$.

Montrons que pour $k \in K^{\#}$ et ℓ tel que $sksk^{-1} = s^{\ell}$, on a $\ell^{-1}(k^{-1} + 1) \neq 1$. Sinon, $\ell = k^{-1} + 1$ et $\alpha(f(rr^{-k})g(rr^{-k})) = \ell^{-1}k^{-2} + k^{-1} + 1 + \ell^{-1} = (k^{-1} + 1)(1 + \ell^{-1}(k^{-1} + 1)) = 0$. Donc en posant $f = f(rr^{-k})$, $g = g(rr^{-k})$, $h = h(rr^{-k})$, on a $fg \in Q_o$ et

$(trr^{-k}t)^2 = g\,h\,t\,f\,g\,h\,t\,f = g\,t(fg)^h\,t\,f$

Comme rr^{-k} est d'ordre 4, $fg \neq 1$ et $t(fg)^h t\,fg$ est une involution. C'est absurde car $t(fg)^h\,t \in \mathrm{Inv}(G-H)$ et $fg \in \mathrm{Inv}(H)$.

§3.- OPÉRATION DE KW SUR S

Supposons qu'on soit dans l'un des cas a) ou b) de la proposition du §1. Alors $G_o = (SK) \cup (SKtS)$ est un sous-groupe de G (§2 et chapitre V, §2, lemme 5). On a $G = H \cup (HtS) = \langle G_o, V \rangle$ et V normalise S, K et t donc $G_o \lhd G$ et $|G/G_o| = |V|$. La conclusion du théorème B résulte alors de l'hypothèse de récurrence. On supposera donc désormais :

(B4) S *est un 2-groupe de Suzuki de type* B, st *est d'ordre 3 et* $W \neq 1$.

Soient $F = \mathbb{F}_q$ et $E = \mathbb{F}_{q^2}$. Soit θ l'automorphisme d'ordre impair de F tel que S soit un 2-groupe de Suzuki de type $B(n,\theta,\varepsilon)$, pour l'opération de K sur S. Cela signifie que S est une extension centrale :

$$F \rightarrowtail S \twoheadrightarrow F \times F$$

l'application quadratique associée $\chi : F \times F \to F$ étant donnée par

$$\chi(a,b) = a^{1+\theta} + \varepsilon ab^{\theta} + b^{1+\theta}$$

et $\varepsilon \in F$ est tel que $\chi(a,b) = 0 \Rightarrow a = b = 0$. D'après [Hi], on peut identifier K à F^* de sorte que les opérations de K sur S/Q_o et sur Q_o , identifiés respectivement à $F \times F$ et à F, soient données par :

$(a,b)^x = (xa,xb)$ et $c^x = x^{1+\theta}c$ $(x \in F^*$, $(a,b) \in F \times F$, $c \in F)$.

Pour $x \in E$, on posera $\bar{x} = x^q$.

Proposition. Il existe un isomorphisme de $S \rtimes KW$ *sur un groupe* $S_1 \rtimes K_1W_1$, *qui envoie* S *sur* S_1 , K *sur* K_1 *et* s *sur* (0,1) , *où* $S_1 \rtimes K_1W_1$ *vérifie les conditions suivantes.*

S_1 *est l'ensemble des couples* (x,y) , $x,y \in E$, *avec* $y \in F$ *si* $\theta \neq 1$ *et* $y + y^q = x^{1+q}$ *si* $\theta = 1$. *La loi de composition de* S_1 *est :*

$$(x,z)(y,u) = (x+y, z+u+\phi(x,y))$$

Si $\theta = 1$, $\phi(x,y) = xy^q$. *Sinon,* ϕ *est une application biadditive :* $E \times E \to F$ *telle que* $\phi(ax,by) = ab^\theta\phi(x,y)$ *pour* $a,b \in F$ *et telle que* $\phi(x,x) \neq 0$ *pour* $x \neq 0$.

K_1W_1 *est un sous-groupe de* E^* , *avec* $K_1 = F^*$, W_1 *étant un sous-groupe* $\neq 1$ *de* $\{x \in E^* | x^{1+q} = 1\}$. *Il existe un automorphisme* σ *de* E *dont la restriction à* F *est* θ *et tel que* $x^\sigma = x^{-1}$ *pour* $x \in W_1$. *L'opération de* K_1W_1 *sur* S_1 *est donnée par* $(x,y)^a = (ax,a^{1+\sigma}y)$ *pour* $a \in K_1W_1$.

1) Identification de $(S/Q_o) \rtimes KW$ à $E \rtimes K_1W_1$: D'après le chapitre V, §2, lemme 6, W est cyclique d'ordre divisant q+1 et opère sans point fixe sur l'ensemble des K-sous-groupes de S/Q_o . Soit w un générateur de W. Alors w est un automorphisme F-linéaire de $S/Q_o \cong F \times F$.

Si $\theta = 1$, une identification de S/Q_o à E, compatible à sa structure de F-espace, a été faite dans l'appendice VIII, prop. 2, de manière que l'application quadratique χ associée à l'extension $F \to S \to E$ soit $\chi(x) = x\bar{x}$. D'après la prop. 3 de l'appendice VIII, il existe $\omega \in E^*$ et un automorphisme τ de E tels que pour $x \in S/Q_o \cong E$, $x^w = \omega x^\tau$ et pour $y \in Q_o \cong F$, $y^w = \omega\bar{\omega}y^\tau$. Puisque w opère trivialement sur Q_o , on a $\omega\bar{\omega} = 1$ et $x^\tau = x$ ou $x^\tau = \bar{x}$. Mais dans le deuxième cas, w serait d'ordre pair, et on a donc $x^w = \omega x$ pour $x \in E$.

Si $\theta \neq 1$, le polynôme caractéristique P(T) de w comme F-automorphisme de S/Q_o est irréductible car w ne laisse stable aucun sous-espace de dimension 1 de S/Q_o , donc S/Q_o peut être identifié de manière F-linéaire à $F[T]/(P) \cong E$, l'opération de w sur S/Q_o étant identifiée à la multiplication par un élément ω de E tel que $P(\omega) = 0$.

2) Existence de σ : Si $\theta = 1$ et $x^\sigma = x^q$, on a $\sigma_{|F} = \theta$ et $x^\sigma = x^{-1}$ pour $x \in W_1$. Supposons que $\theta \neq 1$. Soit $\chi : E \to F$ l'application quadratique associée à l'extension centrale $F \to S \to E$. Soient $\lambda_{\mu\nu} \in E$ tels que

$\chi(x) = \Sigma\lambda_{\mu\nu} x^{\mu}x^{\nu}$, la sommation étant étendue aux parties $\{\mu,\nu\}$ de cardinal 1 ou 2 de Aut(E) (Appendice VIII, lemme 2 c)). En écrivant que $\chi(x) = \overline{\chi(x)}$ et que $\chi(ax) = a^{1+\theta}\chi(x)$ pour $a \in F$ et $x \in E$, et en appliquant le lemme qui vient d'être cité, on voit que $\lambda_{\overline{\mu}\,\overline{\nu}} = \overline{\lambda}_{\mu\nu}$ et que si $\lambda_{\mu\nu} \neq 0$ alors $a^{\mu}a^{\nu} = aa^{\theta}$ pour $a \in F$, donc que $\{\mu_{|F}, \nu_{|F}\} = \{1_F, \theta\}$. Il en résulte que si σ est un automorphisme de E qui prolonge θ, on a

$$\chi(x) = \lambda_1 x^{1+\sigma} + \overline{\lambda_1}\,\overline{x}^{1+\sigma} + \lambda_2 x^{q+\sigma} + \overline{\lambda_2}\,\overline{x}^{q+\sigma}$$

avec $\lambda_1, \lambda_2 \in E$ non tous deux nuls. Puisque w opère trivialement sur Q_o , on on a $\chi(\omega x) = \chi(x)$, donc d'après le même lemme, $\omega^{1+\sigma} = 1$ si $\lambda_1 \neq 0$ et $\omega^{q+\sigma} = 1$ si $\lambda_2 \neq 0$. Puisque $\omega^q \neq \omega$, on a donc en remplaçant éventuellement σ par $\overline{\sigma}$, $\lambda_2 = 0$ et $\omega^{1+\sigma} = 1$.

3) Identification de S à S_1 : posons $\phi(x,y) = xy^q$ si $\theta = 1$ et $\phi(x,y) = \lambda_1 xy^{\sigma} + \overline{\lambda_1}\,\overline{xy}^{\sigma}$ si $\theta \neq 1$. On constate alors que la loi de composition donnée dans l'énoncé fait de S_1 un groupe et que $F \overset{\iota}{\to} S_1 \overset{\pi}{\to} E$ (avec $\iota(y) = (0,y)$ et $\pi(x,y) = x$) est une extension centrale dont l'application quadratique associée est χ . D'après le lemme 1 c) de l'appendice VIII, cette extension est équivalente à l'extension $F \to S \to E$.

4) Opération de K_1W_1 sur S_1 : Soit A l'image de KW dans $\mathrm{Aut}(S_1)$, KW opérant par conjugaison sur $S \overset{\sim}{=} S_1$. On constate que la formule donnée dans l'énoncé définit une opération de K_1W_1 sur S_1 . Soit B l'image de K_1W_1 dans $\mathrm{Aut}(S_1)$ pour cette opération. Soit U le groupe des automorphismes de S_1 qui induisent l'identité sur $Z(S_1)$ et sur $S_1/Z(S_1)$. Alors $U \lhd \mathrm{Aut}(S_1)$ et d'après 1), $B \subset U\,A$. Mais U est un 2-groupe (appendice VIII, lemme 1 d)), donc d'après un théorème de Zassenhaus, il existe $u \in U$ tel que $A^u = B$, et u induit un isomorphisme de $S_1 \rtimes A$ sur $S_1 \rtimes B$.

5) Enfin, puisque K est transitif sur $Q_o^{\#}$, on peut supposer que s est identifié à (0,1) en composant l'isomorphisme $S \rtimes KW \to S_1 \rtimes K_1W_1$ avec un automorphisme intérieur de $S_1 \rtimes K_1W_1$.

CHAPITRE VII. CARACTÉRISATION DE PSU(3,q)

§1.- LES APPLICATIONS f, g, h

Dans ce chapitre, nous terminons la démonstration du théorème B. Nous montrerons en particulier que si $V = W$, alors G est isomorphe à PSU(3,q) ou à PGU(3,q). La démonstration se fera par un calcul explicite de la loi de composition de G, selon une méthode due à M. Suzuki.

Supposons que L soit un groupe fini qui opère de manière 2-transitive sur un ensemble X, et soient M le stabilisateur dans L d'un point de X, $t \in \mathrm{Inv}(L-M)$ et $D = M \cap M^t$. Supposons qu'il existe un sous-groupe Q de M tel que $M = Q \rtimes D$ (ces hypothèses signifient que L a une BN-paire scindée de rang 1).

Il existe alors des applications $f,g : Q^\# \to Q^\#$ et $h : Q^\# \to D$ déterminées de manière unique, telles que pour $x \in Q^\#$,

$$txt = g(x)\, h(x)\, t\, f(x)$$

En effet, on voit comme dans le chap. V, §2, lemme 1 que tout élément de L-M se met de manière unique sous la forme atb où $a \in M$ et $b \in Q$, et puisque $Q^t \cap M = 1$, on a $txt \notin M \cup (Mt) \cup (tM)$.

Ces applications satisfont les identités suivantes :

H1. $f(x^{-1}) = g(x)^{-1}$

H2. $f(f(x)) = x$

H3. $f(x^a) = f(x)a^t$ pour $a \in D$.

H4. $h(x^a) = a^{-t}h(x)a$ pour $a \in D$, $h(x^{-1}) = h(x)^{-t}$, $h(f(x)) = h(x)^{-1}$

H5. Soit j l'application $x \mapsto x^{-1}$ de $Q^{\#}$ dans $Q^{\#}$. $(f \circ j)^3(x) = x^{h(x)^{-1}}$

H6. Si $x,y \in Q^{\#}$ et $xy \neq 1$, alors $f(x)g(y) \neq 1$,

$$f(xy) = f(f(x)g(y))^{h(y)^t} f(y) \quad \text{et} \quad h(xy) = h(x)h(f(x)g(y))h(y)$$

Les démonstrations des identités H1. à H4. se font par des calculs évidents. Soit $x \in Q^{\#}$. Alors $txt = g(x)h(x)tf(x)$, donc $tf(x)t = h(x)^{-1}g(x)^{-1}tx$, donc $g(f(x)) = g(x)^{-h(x)}$. D'après H1., on a alors $(j \circ f)^2(x) = (f \circ j(x))^{h(x)}$ et d'après H2 et H3, $x = (f \circ j)^2(f \circ j(x))^{h(x)} = ((f \circ j)^3(x))^{h(x)}$, ce qui démontre H5. Soient $x,y \in Q^{\#}$ tels que $xy \neq 1$ et $z = f(x)\,g(y)$. Alors $txyt = g(x)h(x)tzh(y)tf(y) = g(x)h(x)tzt\,h(y)^t f(y)$, donc $z \neq 1$ et $txyt = g(x)h(x)g(z)h(z)tf(z)h(y)^t f(y) = g(x)h(x)g(z)h(z)h(y)t\,f(z)^{h(y)^t} f(y)$, ce qui démontre H6.

Remarquons que d'après H2,H3,H5, $\langle f,j \rangle$ opère sur l'ensemble des orbites de $Q^{\#}$ sous D, et le groupe de permutations de cet ensemble induit par $\langle f,j \rangle$ est isomorphe à un quotient du groupe diédral d'ordre 6.

Lemme. *Si* L *opère fidèlement sur* X, $\langle Q^x | x \in L \rangle$ *est déterminé à isomorphisme près par la donnée de* Q *et de* f *et* L *est déterminé à isomorphisme près par la donnée de* $M = Q \rtimes D$ *et de* f .

Si $M = L_a$, on peut identifier X à $Q \cup \{a\}$, $x \in Q$ étant identifié à a^{tx}. Alors l'action de t sur X est déterminée par f et l'action de Q (resp. M) est déterminée par la donnée de Q (resp. la donnée $Q \rtimes D$). Mais $\langle Q^x | x \in L \rangle = \langle Q, Q^{tx} | x \in Q \rangle \subset \langle Q,t \rangle$ et $L = \langle M,t \rangle$.

Dans les calculs qui suivent, on reprend les hypothèses de la fin du chapitre VI et on essaie de déterminer f pour $L = G$ et $M = H$. On identifiera $Q \rtimes KW$ au groupe $S_1 \rtimes K_1W_1$ défini dans le §3 du chapitre VI.

§2.- CALCUL PRÉLIMINAIRE

D'après (B4), on a $tst = sts$ donc d'après H3 et H4 :

(1) Pour $a \in K$, $f(s^a) = g(s^a) = s^{a^{-1}}$ et $h(s^a) = a^2$.

D'après H6 appliqué à $x = \omega \in Q - Q_0$ et $y = s^a$, on a :

(2) $f(\omega s^a) = f(f(\omega)s^{a^{-1}})a^{-2}\, s^{a^{-1}}$ pour $\omega \in Q - Q_0$, $a \in K$.

En appliquant H6 à $x = s^a$ et $y = \omega$, on a aussi :

(3) $f(\omega s^a) = f(g(\omega)s^{a^{-1}})^{h(\omega)^t}\, f(\omega)$

(4) $f(\omega x) = f(\omega)y$, $\omega \in Q - Q_0$, $x,y \in Q_0 \Rightarrow x = 1$

Si $x \neq 1$, il existe $k \in K$ tel que $x = s^k$. D'après (3), on a alors $f(\omega)y = f(g(\omega)s^{k^{-1}})^{h(\omega)^t}\, f(\omega)$, donc $f(g(\omega)s^{k^{-1}}) \in Q_0$, d'où $g(\omega) \in Q_0$ puis $\omega \in Q_0$, ce qui est absurde.

(5) $f(\omega) = (\omega y)^a$, $\omega \in Q - Q_0$, $y \in Q_0$ et $a \in D \Rightarrow y \neq 1$ et $a \notin K$.

Puisque $|D|$ est impair, j n'a pas de point fixe dans l'ensemble des orbites de $Q-Q_0$ sous D, et puisque f est conjugué à j dans le groupe des permutations de cet ensemble induit par $\langle f,j \rangle$, f n'en a pas non plus, donc $y \neq 1$. D'après H2 et H3, $f(\omega y) = \omega^{a^{-t}} = (f(\omega)a^{-1}y)^{a^{-t}} = (f(\omega)y^a)^{a^{-1}a^{-t}}$, donc $a^{-1}a^{-t} \neq 1$ d'après (4), d'où $a \notin K$.

(6) $f(\omega x) = (f(\omega)y)^a$, $\omega \in Q - Q_0$, $x,y \in Q_0$, $x \neq 1$ et $a \in D \Rightarrow a \notin K$.

Soit $k \in K$ tel que $x = s^k$. D'après (2), $(f(\omega)y)^a = f(f(\omega)s^{k^{-1}})^{k^{-2}}s^{k^{-1}}$, d'où $f(f(\omega)s^{k^{-1}}) = ((f(\omega)y)^a s^{k^{-1}})^{k^2} = (f(\omega)s^{k^{-1}}.s^{k^{-1}}ys^{k^{-1}}a^{-1})^{ak^2}$. D'après (5), il en résulte que $ak^2 \notin K$, d'où $a \notin K$.

(7) Soient $\omega,\omega' \in Q-Q_0$ et pour $i = 1,2$, $x_i,y_i \in Q_0$ et $a_i \in D$ tels que $x_1 \neq x_2$ et $f(\omega x_i) = (\omega' y_i)^{a_i}$. Alors $a_2 \notin a_1 K$.

L'hypothèse entraîne que

$f(\omega x_2) = (f(\omega x_1)^{a_1^{-1}} y_1 y_2)^{a_2} = (f(\omega x_1)(y_1 y_2)^{a_1})^{a_1^{-1}a_2}$. D'après (6), $a_1^{-1}a_2 \notin K$.

Posons $|W| = m$ et $n = (q+1)/m = |E^*/KW|$. Pour $\omega \in Q$, on note $\bar{\omega}$

l'image de ω dans Q/Q_o . Si $\omega = (\alpha,\beta)$, $\bar{\omega}$ s'identifie à $\alpha \in E$. Soient $\omega_1,\ldots,\omega_n \in Q - Q_o$ tels que les $\bar{\omega}_i$ forment un système de représentants des orbites de $(Q/Q_o)^{\#}$ sous KW .

(8) Le nombre des $x \in Q_o$ tels $\overline{f(\omega_1 x)}$ soit dans l'orbite de $\bar{\omega}_i$ sous KW est m si $i > 1$ et est m-1 si $i = 1$.

Soit m_i le nombre des $x \in Q_o$ tels que $\overline{f(\omega_1 x)}$ soit dans l'orbite de $\overline{\omega_i}$ sous KW . D'après (7) avec $\omega = \omega_1$, $\omega' = \omega_i$, on a $m_i \leq m$ pour $i > 1$. De même, d'après (7) et (5), on a $m_1 \leq m-1$. ALors $q = \Sigma m_i \leq nm - 1 = q$, donc toutes ces inégalités sont des égalités.

Soit $\mathfrak{I}$ un générateur de W. D'après (B4) , $\mathfrak{I} \neq 1$.

(9) Pour tout i ($1 \leq i \leq n$), il existe $\omega_i' \in Q - Q_o$ et $y_i \in Q_o^{\#}$ tels que $\overline{\omega_i'}$ soit dans l'orbite de $\overline{\omega_i}$ sous KW et $f(\omega_i') = (\omega_i' y_i)^{\mathfrak{I}}$.

Soit ω l'un des ω_i . D'après (5), (7) et (8), il existe $x,z \in Q_o$ et $k \in K$ tels que $f(\omega x) = (\omega z)^{k\mathfrak{I}}$. Si $a \in K$, on a

$$f((\omega x)^a) = f(\omega x)^{a^{-1}} = (\omega z)^{a^{-1}k\mathfrak{I}} = ((\omega x)^a (xz)^a)^{a^{-2}k\mathfrak{I}}$$

En prenant $a \in K$ tel que $a^2 = k$ et en posant $\omega' = (\omega x)^a$, $y = (xz)^a$, on a $f(\omega') = (\omega' y)^{\mathfrak{I}}$. D'après (5), $y \neq 1$.

On supposera désormais dans le §2 que les ω_i ont été choisis de manière que $f(\omega_i) = (\omega_i y_i)^{\mathfrak{I}}$, $y_i \in Q_o^{\#}$.

Dans (10)-(18) , ω désigne l'un des ω_i et on pose $y_i = y = (0,\alpha)$.

(10) Soient $a,b \in K$ tels que $b^{1+\theta} = \alpha + a^{-(1+\theta)}$. Alors $f(\omega s^a) =$

$= (f(\omega s^b) s^a)^{\mathfrak{I}a^{-2}}$. D'après (2), $f(\omega s^a) = f(f(\omega) s^{a-1})^{a-2} s^{a-1} =$

$= f(\omega y\, s^{a-1})^{\mathfrak{I}a^{-2}} s^{a-1} = (f(\omega s^b) s^a)^{\mathfrak{I}a^{-2}}$.

On notera τ l'application réciproque de $u \mapsto u^{1+\theta} : F^* \to F^*$ qui est bijective car θ est d'ordre impair. Comme $f(\omega) = (\omega y)^{\mathfrak{I}}$, (10) permet de définir

par récurrence des suites (u_i), (v_i), (d_i) telles que $u_i, v_i \in F$, $d_i \in KW$ et $f(\omega(0,u_i)) = (\omega(0,v_i))^{d_i}$:

(11) $u_1 = 0$, $v_1 = \alpha$, $d_1 = \mathfrak{I}$.

si $u_i \neq \alpha$, $u_{i+1} = 1/(\alpha+u_i)$, $v_{i+1} = v_i + u_{i+1} d_i^{-(1+\sigma)}$, $d_{i+1} = d_i \mathfrak{I} u_{i+1}^{-2\tau}$.

Ces suites s'arrêtent dès qu'on a trouvé un indice i tel que $u_i = \alpha$.

Posons

$$\begin{pmatrix} a_i \\ b_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}^i \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (i \geq 0 , a_i, b_i \in F).$$

On voit alors par récurrence sur i que si $u_i \neq \alpha$, alors $b_i \neq 0$ et $u_{i+1} = a_i/b_i$.

Soient β et β^{-1} les racines du polynôme caractéristique $X^2 + \alpha X + 1$ de $\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$:

(12) $\beta + \beta^{-1} = \alpha$, $\beta \in E$ et si $\beta \notin F$, alors $\beta^{-1} = \beta^q$.

Puisque $\alpha \neq 0$, on a :

$$\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \beta & \beta^{-1} \end{pmatrix} \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \beta & \beta^{-1} \end{pmatrix}^{-1} \qquad \text{d'où}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}^i = \frac{1}{\alpha} \begin{pmatrix} 1 & 1 \\ \beta & \beta^{-1} \end{pmatrix} \begin{pmatrix} \beta^i & 0 \\ 0 & \beta^{-i} \end{pmatrix} \begin{pmatrix} \beta^{-1} & 1 \\ \beta & 1 \end{pmatrix} = \frac{1}{\alpha} \begin{pmatrix} \beta^{i-1}+\beta^{-i+1} & \beta^i+\beta^{-i} \\ \beta^i + \beta^{-i} & \beta^{i+1}+\beta^{-i-1} \end{pmatrix}$$

Il en résulte que $a_i = (1/\alpha)(\beta^i + \beta^{-i})$, $b_i = (1/\alpha)(\beta^{i+1}+\beta^{-i-1})$ et

$$(13) \quad u_i = \frac{\beta^{i-1}+\beta^{-i+1}}{\beta^i + \beta^{-i}}$$

D'après (11), on voit alors par récurrence sur i que

$$(14) \quad d_i = \mathfrak{I}^i \left(\frac{\beta^i+\beta^{-i}}{\alpha}\right)^{2\tau}$$

(15) Les suites (u_i), (v_i), (d_i) sont définies jusqu'à $i = m-1$ et

$u_{m-1} = \alpha = \beta^{m-1} + \beta^{-m+1}$. Tout $u \in F$ tel que $\overline{f(\omega(0,u))}$ soit dans l'orbite de $\overline{\omega}$ sous KW est l'un des u_i .

Soit m_1 le dernier indice pour lequel u_i est défini. On a $m_1 \leq m-1$ car sinon $d_m \in K$ d'après (14), ce qui contredit (5). On a $u_{m_1} = \alpha$ et $f(\omega(0,\alpha)) = (\omega(0,v_{m_1}))^{d_{m_1}}$. Mais $f(\omega) = (\omega(0,\alpha))^{\mathfrak{I}}$ d'où $f(\omega(0,\alpha)) = \omega^{\mathfrak{I}-1}$ D'après (14), il en résulte que $d_{m_1} = \mathfrak{I}^{m_1}(\frac{\beta^{m_1}+\beta^{-m_1}}{\alpha})^{2\tau} = \mathfrak{I}^{-1}$. Puisque $K \cap W = 1$, on a donc $\beta^{m_1} + \beta^{-m_1} = \alpha$ et $\mathfrak{I}^{m_1+1} = 1$. Puique $\mathfrak{I}$ est d'ordre m, $m_1 = m-1$. Les $u_i (1 \leq i \leq m-1)$ sont deux à deux distincts car les d_i le sont. La dernière assertion résulte donc de (8).

(16) β est un générateur de W. En particulier, $\beta^{\sigma} = \beta^{-1}$.

Pour $1 \leq i \leq m-1$, on a $b_{i-1} = (1/\alpha)(\beta^i + \beta^{-i}) \neq 0$ donc $\beta^i \neq 1$. D'après (15), β^{m-1} est une racine de $X^2 + \alpha X + 1$ donc $\beta^{m-1} = \beta$ ou β^{-1} , et comme $\beta^{m-2} \neq 1$, on a $\beta^m = 1$.

(17) Pour $1 \leq i \leq m-1$, $f(\omega(0,u_i)) = (\omega(0,u_i + \alpha))^{d_i}$

Pour $1 \leq i \leq m-2$, on a $u_{i+1} \neq 0$ et d'après (13) et (14) ,

$$\frac{u_i}{u_{i+1}} = \frac{(\beta^{i-1}+\beta^{-i+1})(\beta^{i+1}+\beta^{-i-1})}{(\beta^i+\beta^{-i})^2} = \frac{\beta^{2i}+\beta^{-2i}+\beta^2+\beta^{-2}}{\beta^{2i}+\beta^{-2i}} = 1 + \left(\frac{\beta+\beta^{-1}}{\beta^i+\beta^{-i}}\right)^2 = 1 + d_i^{-(1+\sigma)},$$

donc $v_{i+1} + u_{i+1} = v_i + (1 + d_i^{-(1+\sigma)})u_{i+1} = v_i + u_i$, d'où $v_i + u_i = v_1 + u_1 = \alpha$ pour $1 \leq i \leq m-1$.

(18) $(h(\omega)\mathfrak{I}^{-1})^m = 1$

D'après (13) et (16) , $u_i^{\theta} = u_i$ donc $u_i^{2\tau} = u_i$. D'après H6 et (1), on a pour $2 \leq i \leq m-1$, $h(\omega(0,u_i)) = h(\omega)h((\omega(0,\alpha))^{\mathfrak{I}}(0,u_i^{-1}))u_i^{2\tau} = h(\omega)\, h(\omega(0,u_{i-1}))^{\mathfrak{I}}\, u_i = (h(\omega)\mathfrak{I}^{-1})\, h(\omega(0,u_{i-1}))(\mathfrak{I}u_i)$, donc par récurrence $h(\omega(0,u_i)) = (h(\omega)\mathfrak{I}^{-1})^i\, \mathfrak{I}^i\alpha/(\beta^i+\beta^{-i})$ pour $1 \leq i \leq m-1$. En particulier, $h(\omega(0,\alpha)) = (h(\omega)\mathfrak{I}^{-1})^{m-1}\, \mathfrak{I}^{-1}$. Mais d'après H4, $h(\omega(0,\alpha)) = h(f(\omega)^{\mathfrak{I}-1}) =$

$\mathfrak{F}\, h(\omega)^{-1}\mathfrak{F}^{-1}$, d'où $(h(\omega)\mathfrak{F}^{-1})^m = 1$.

Dans (19)-(20), on suppose que $n \geq 2$ et on pose $y_1 = (0,\alpha_1)$, $y_2 = (0,\alpha_2)$, de sorte que $f(\omega_1) = (\omega_1(0,\alpha_1))^{\mathfrak{F}}$, $f(\omega_2) = (\omega_2(0,\alpha_2))^{\mathfrak{F}}$. Soient (u_i), (v_i), (d_i) les suites définies par (11) à partir de $\alpha = \alpha_1$, et (u'_i), (v'_i), (d'_i) les suites analogues définies à partir de $\alpha = \alpha_2$. D'après (7) et (8), il existe $x_1, x_2 \in F$ et $k \in K$ tels que

$$f(\omega_1(0,x_1)) = (\omega_2(0,x_2))^k$$

(19) Pour $0 \leq i \leq m-1$, on a :

a) $f[\omega_2(0,x_2 + 1/(k^{1+\theta}(x_1+u_i)))] = [\omega_1(0,v_i+1/(d_i^{1+\sigma}(x_1+u_i)))]^{e_i}$

b) $f[\omega_1(0,x_1 + 1/(k^{1+\theta}(x_2+u'_i)))] = [\omega_2(0,v'_i+1/(d'^{1+\sigma}_i(x_2+u'_i)))]^{e'_i}$

avec $e_i = kd_i(x_1+u_i)^{2\tau}$ et $e'_i = kd'_i(x_2+u'_i)^{2\tau}$.

Puisque $\overline{f(\omega_1(0,x_1))}$ n'est pas dans l'orbite de $\overline{\omega_1}$ sous KW, $x_1 \neq u_i$. Soit $a \in K$ tel que $x_1 + a^{-(1+\theta)} = u_i$. Alors d'après (2) ,

$f(\omega_2(0,x_2)s^{ak-1})^{k-1} = f((\omega_2(0,x_2))^k s^a) = f(\omega_1(0,x_1)s^{a^{-1}})^{a^{-2}}\, s^{a^{-1}} =$

$= f(\omega_1(0,u_i))^{a^{-2}}\, s^{a^{-1}} = (\omega_1(0,v_i))^{d_i a^{-2}}\, s^{a^{-1}} = (\omega_1(0,v_i)s^{ad_i^{-1}})^{d_i a^{-2}}$,

ce qui donne a). On a $f(\omega_2(0,x_2))^{k-1} = \omega_1(0,x_1)$, donc $f(\omega_2(0,x_2)) =$

$= (\omega_1(0,x_1))^k$, d'où b), en échangeant les rôles de ω_1 et de ω_2 .

(20) On a $\alpha_1 = \alpha_2$ et en posant $\alpha = \alpha_1$, pour tout x tel que $\overline{f(\omega_1(0,x))}$ soit dans l'orbite de $\overline{\omega_2}$ sous KW, on a

$$f(\omega_1(0,x)) = (\omega_2(0,x+\alpha))^{d(x)} \quad , \text{ avec } d(x) \in KW .$$

Les éléments x_1 et $x_1+1/(k^{1+\theta}(x_2+u'_i))$ sont deux à deux distincts, donc d'après (8) et (19), sont tous les éléments x tels que $\overline{f(\omega_1(0,x))}$ soit dans l'orbite de $\overline{\omega_2}$ sous KW. D'après (19) a), on a

$f[\omega_1(0,v_i+1/(d_i^{1+\sigma}(x_1+u_i)))] = [\omega_2(0,x_2+1/(k^{1+\theta}(x_1+u_i)))]^{e_i^{-t}}$

et d'après (19) b),

$f[\omega_1(0,x_1+1/(k^{1+\theta}(x_2+u'_{m-i})))] = [\omega_2(0,v'_{m-i}+1/(d'^{1+\sigma}_{m-i}(x_2+u'_{m-i})))]^{e'_{m-i}}$

D'après (14) et (19), $e_i^{-t} \in e'_{m-i}K$, donc d'après (7), on a pour $1 \leq i \leq m-1$:

(*) $v_i+1/(d_i^{1+\sigma}(x_1+u_i)) = x_1+1/(k^{1+\theta}(x_2+u'_{m-i}))$

(**) $v'_i+1/d'^{1+\sigma}_i(x_2+u'_i)) = x_2+1/(k^{1+\theta}(x_1+u_{m-i}))$

(***) $d_i^{-t}(x_1+u_i)^{2\tau} = d'_{m-i}(x_2+u'_{m-i})^{2\tau}$.

L'égalité (***) pour $i = 1$ puis pour $i = m-1$ donne :

$$x_1 = x_2 + \alpha_2 \ , \ x_1 + \alpha_1 = x_2$$

donc $\alpha_1 = \alpha_2 = x_1 + x_2$, ce qui prouve la première assertion de (20), et la deuxième assertion pour $x = x_1$. Puisque $\alpha_1 = \alpha_2$, on a $u'_i = u_i$, $v'_i = v_i$, $d'_i = d_i$.

D'après (13) et (11), on a $u_{m-i} = 1/u_{i+1} = u_i + \alpha$ pour $1 \leq i \leq m-2$, donc $x_1 + u_{m-i} = x_1+ \alpha + u_i = x_2 + u_i$ pour $1 \leq i \leq m-1$, et (**) peut s'écrire :

$v_i + 1/(d_i^{1+\sigma}(x_2+ u_i)) = x_2+ 1/(k^{1+\theta}(x_2+u_i)) = x_1+ 1/(k^{1+\theta}(x_2+ u_i)) + \alpha$

D'après (19) b), on a donc $f(\omega_1(0,x)) = (\omega_2(0,x + \alpha))^{d(x)}$ avec $d(x) \in KW$ pour $x = x_1 + 1/(k^{1+\theta}(x_2+ u_i))$.

Proposition. *Supposons que* D *opère sans point fixe sur* $(Q/Q_o)^{\#}$. *Alors il existe* i , $1 \leq i \leq n$, *tel que pour* $\omega = \omega_i$ *on ait* $f(\omega) = (\omega^{-1})^{\mathfrak{I}}$ *et* $h(\omega) \in W$.

D'après l'hypothèse, les groupes de Sylow de D sont cycliques. Alors (18) implique que si ω est l'un des ω_i , $h(\omega) \in W$. En effet, si p est un nombre premier, si x est la p-composante de $h(\omega)^{\mathfrak{I}^{-1}}$ et P est un p-Sylow de D contenant x,on a $x^{m_p} = 1$ et $|P \cap W| = m_p$ car $W \lhd D$, donc $x \in W$.

Posons $\omega_1^2 = (0,r)$ et soient i,k tels que $\overline{f(\omega_1^{-1})}$ soit dans l'orbite de $\overline{\omega_i}$ sous KW et $\overline{f(\omega_1^{-1}(0,\alpha))}$ soit dans l'orbite de $\overline{\omega_k}$ sous KW. Alors, d'a-

près (17) et (20), on a :

$$f((\omega_k(0,r))^{KW}) = (\omega_1(0,\alpha+r))^{KW}$$

$$f\circ j((\omega_1(0,\alpha+r))^{KW}) = \omega_1^{KW}$$

$$f\circ j(\omega_1^{KW}) = (\omega_i(0,\alpha+r))^{KW}$$

De plus, d'après H4, $h(\omega_k^{-1}(0,r)) \in KW$. D'après H5, il en résulte que $(\omega_k^{-1}(0,r))^{KW} = (\omega_i(0,\alpha+r))^{KW}$ donc $i = k$ et $\omega_i^2 = (0,\alpha)$. Alors $f(\omega_i) = (\omega_i(0,\alpha))^{\mathfrak{I}} = (\omega_i^{-1})^{\mathfrak{I}}$.

§3.- DÉTERMINATION DE f

Proposition. Supposons qu'il existe $\omega \in Q-Q_0$ *et* $\mathfrak{I} \in W^{\#}$ *tels que* $f(\omega) = (\omega^{-1})^{\mathfrak{I}}$ *et* $h(\omega) \in W$. *Alors* $\theta = 1$ *et pour tout* $\rho = (\overline{\rho},y) \in Q-Q_0$, *on a* $f(\rho) = (\overline{\rho}/y,1/y)$.

(1) Pour $a \in K$, on a $f(\omega s^a)^{\mathfrak{I}^{-1}} a^2 s^a = f(\omega s^a)^{\mathfrak{I}^{-2}} \omega^{\mathfrak{I}^{-1}}$.

On a $(f\circ j)^3(\omega^{-1}) = (f\circ j)^2(\omega^{-\mathfrak{I}}) = f\circ j(\omega^{-\mathfrak{I}^2}) = \omega^{-\mathfrak{I}^3}$. D'après H5 et puisque $h(\omega^{-1}) = h(\omega)^{-t} \in W$, il en résulte que $h(\omega^{-1}) = \mathfrak{I}^{-3}$. On a $f(\omega^{-1}) = \omega^{\mathfrak{I}^{-1}}$, $g(\omega^{-1}) = \omega^{\mathfrak{I}}$ donc d'après (2) et (3) du §2 : $f(\omega^{-1}s^{a-1}) = f(\omega^{\mathfrak{I}^{-1}}s^a)a^2s^a = f(\omega^{\mathfrak{I}}s^a)^{\mathfrak{I}^{-3}}\omega^{\mathfrak{I}^{-1}}$.

(2) Pour $a \in K$, $\overline{f(\omega s^a)} = \overline{\omega}/(a^2+\mathfrak{I}^{-1})$ (le deuxième membre est calculé dans E).

D'après (1), $\mathfrak{I}^{-1}a^2\,\overline{f(\omega s^a)} = \mathfrak{I}^{-2}\,\overline{f(\omega s^a)} + \mathfrak{I}^{-1}\,\overline{\omega}$, donc $(a^2 + \mathfrak{I}^{-1})\overline{f(\omega s^a)} = \overline{\omega}$.

(3) $\theta = 1$ et $\omega^2 = (0,\mathfrak{I} + \mathfrak{I}^{-1})$.

Posons $\omega^2 = (0,\alpha)$. D'après (2) du §2, on a pour $a \in K$:

$$\overline{f(\omega s^a)} = \overline{f(\omega^{-\mathfrak{I}}s^{a^{-1}})a^{-2}} = \mathfrak{I}a^{-2}\,\overline{f(\omega(0,\ \alpha+a^{-(1+\theta)}))}$$

Donc d'après (2), si $a \neq \alpha^{-\tau}$ et $b^{1+\theta} = \alpha + a^{-(1+\theta)}$,

$1/(a^2 + \vartheta^{-1}) = \vartheta a^{-2}/(b^2 + \vartheta^{-1})$, d'où $b^2 = \vartheta + \vartheta^{-1} + a^{-2}$. Il en résulte que $b^{2(1+\theta)} = \alpha^2 + (a^{-2})^{1+\theta} = (\vartheta + \vartheta^{-1} + a^{-2})^{1+\theta}$. Comme $\vartheta \in W$, on a $(\vartheta + \vartheta^{-1})^{\theta} = \vartheta^{\sigma} + \vartheta^{-\sigma} = \vartheta + \vartheta^{-1}$. L'égalité ci-dessus s'écrit donc :

(*) $\alpha^2 + \vartheta^2 + \vartheta^{-2} + (\vartheta + \vartheta^{-1})(a^{-2} + a^{-2\theta}) = 0$

Donc $X + X^{\theta} = c$ est indépendant de X pour $X \in F - \{0,\alpha^{2\tau}\}$. Si $\theta \neq 1$, on a $|F| \geq 8$ car θ est d'ordre impair, et il existe donc $X,Y \in F$ tels que $\{X,Y,X+Y\} \cap \{0,\alpha^{2\tau}\} = \emptyset$ et $c = X + Y + (X+Y)^{\theta} = c + c = 0$. Donc $X^{\theta} = X$ pour $X \in F - \{0,\alpha^{2\tau}\}$, d'où $\theta = 1$. L'égalité (*) donne alors $\alpha = \vartheta + \vartheta^{-1}$.

(4) Pour tout $y \in E$ tel que $y + y^q = \overline{\omega}^{1+q}$, $f(\overline{\omega},y) = (\overline{\omega}/y,1/y)$.

Soit $\omega = (\overline{\omega},x)$. D'après (1) et (3), on a pour $a \in F - \{0\}$,

$f(\overline{\omega},x + a)^{\vartheta^{-1}a}(0,a) = f(\overline{\omega},x + a)^{\vartheta^{-2}}(\overline{\omega},x)^{\vartheta^{-1}}$.

D'après (2) $f(\overline{\omega},x + a) = (\overline{\omega}/(a + \vartheta^{-1}) , \gamma(a))$ où $\gamma(a) \in E$. On a donc :

$(\vartheta^{-1}a\overline{\omega}/(a+\vartheta^{-1}),a^2\gamma(a)+a) = (\vartheta^{-2}\overline{\omega}/(a+\vartheta^{-1})+\vartheta^{-1}\overline{\omega},\gamma(a)+x+\vartheta^{-1}\overline{\omega}^{1+q}/(a+\vartheta^{-1}))$

Comme $\overline{\omega}^{1+q} = \vartheta + \vartheta^{-1}$ d'après (3), l'égalité des deuxièmes termes de ces couples donne :

(*) $(a^2 + 1)\gamma(a) = x + a + (1+\vartheta^{-2})/(a + \vartheta^{-1})$

Pour $a = 1$, cette égalité devient $x + 1 + (1 + \vartheta^{-1}) = x + \vartheta^{-1} = 0$, donc $x = \vartheta^{-1}$. L'égalité (*) s'écrit alors

$(a^2 + 1)\gamma(a) = a + \vartheta^{-1} + (1 + \vartheta^{-2})/(a + \vartheta^{-1}) = (a^2 + 1)/(a + \vartheta^{-1})$. Donc pour $a \in F - \{0,1\}$, $\gamma(a) = 1/(a + \vartheta^{-1})$. Cela signifie que pour $y \in E - \{\vartheta^{-1},\vartheta^{-1} + 1\}$ tel que $y + y^q = \overline{\omega}^{1+q}$, $f(\overline{\omega},y) = (\overline{\omega}/y,1/y)$.

Pour $y = \vartheta^{-1}$, $(\overline{\omega},y) = \omega$ et on a encore $f(\omega) = \omega^{-\vartheta} = (\overline{\omega},\vartheta)^{\vartheta} = (\overline{\omega}/y,1/y)$.

Puisque $f(\omega^{-1}) = \omega^{\Im^{-1}}$, tous les résultats qui précèdent restent valables quand on remplace ω par ω^{-1} et $\Im$ par $\Im^{-1}$. En particulier, pour tout $y \in E - \{\Im+1\}$ tel que $y + y^q = \varpi^{1+q}$, on a $f(\overline{\omega},y) = (\overline{\omega}/y,1/y)$, ce qui complète la preuve car $\Im + 1 \neq \Im^{-1} + 1$.

(5) Pour tout $\rho = (\overline{\rho},y) \in Q-Q_0$, on a $f(\rho) = (\overline{\rho}/y,1/y)$.

Si $f(\overline{\rho},y) = (\overline{\rho}/y,1/y)$ et si $d \in KW$, on a d'après H3 :

$f(d\overline{\rho},d^{1+q}\, y) = f(\overline{\rho},y)^{d^t} = (\overline{\rho}/y,1/y)^{d^{-q}} = (\overline{\rho}/d^q y,1/d^{1+q} y)$.

Si $\overline{\rho}$ est dans l'orbite de $\overline{\omega}$ sous KW , (5) résulte donc de (4). Sinon, en remplaçant éventuellement ρ par un élément de ρQ_0 , on peut supposer d'après (8) du §2 que $\overline{f(\rho)}$ est dans l'orbite de $\overline{\omega}$ sous KW . Posons $\rho = (\overline{\rho},x)$, $f(\rho) = (\overline{\omega}',x')$. Alors $(\overline{\rho},x) = f(\overline{\omega}',x') = (\overline{\omega}'/x',1/x')$, donc $\overline{\omega}' = \overline{\rho}/x$, $x' = 1/x$.

D'après (2) du §2, on a pour $a \in F - \{0\}$:

$f(\overline{\rho},x+a) = f(\overline{\omega}',x'+a^{-1})a^{-1}\ (0,a^{-1}) = (\overline{\omega}'/(x'+a^{-1}),1/(x'+a^{-1}))^{a^{-1}}\ (0,a^{-1}) =$
$(\overline{\omega}'/(ax'+1),a^{-1}(1/(ax'+1)+1)) = (\overline{\rho}/(x+a),1/(x+a))$
ce qui prouve (5) .

Corollaire 1. Sous l'hypothèse de la proposition, $O^{2'}(G) \cong PSU(3,q)$. *En particulier, si* $V = W$, G *est isomorphe à* $PSU(3,q)$ *ou à* $PGU(3,q)$.

Si G satisfait l'hypothèse de la proposition, Q et f sont bien déterminés par la donnée de q . D'après le lemme du §1, $O^{2'}(G) = \langle Q^x \mid x \in G\rangle$ est donc déterminé à isomorphisme près.

Supposons que $V = W$. Alors l'hypothèse de la proposition est satisfaite d'après la proposition du §2. En particulier PGU(3,q) satisfait cette hypothèse, donc $O^{2'}(G) \cong O^{2'}(PGU(3,q)) = PSU(3,q)$. Il en résulte que $(q+1)/(q+1,3) \leq |W|$ et si $|W| = (q+1)/(q+1,3)$, G est isomorphe à $PSU(3,q)$. Sinon, $|W| = q+1$ et G est isomorphe à

PGU(3,q) d'après le lemme du §1 .

Corollaire 2. Si $G \cong PSU(3,q)$ *et si* $\mathfrak{I} \in W^{\#}$, *il existe* $\omega \in Q-Q_o$ *tel que* $f(\omega) = \omega^{-\mathfrak{I}}$ *et* $h(\omega) = \mathfrak{I}^3$

On a $\mathfrak{I}^{-1}+\mathfrak{I}^{-q} \neq 0$, donc il existe $\overline{\omega} \in E-\{0\}$ tel que $\overline{\omega}^{1+q} = \mathfrak{I}^{-1}+\mathfrak{I}^{-q}$. Alors $\omega = (\overline{\omega},\mathfrak{I}^{-1}) \in Q$, $\omega^{-1} = (\overline{\omega},\mathfrak{I})$ et $f(\omega) = (\mathfrak{I}\overline{\omega},\mathfrak{I}) = \omega^{-\mathfrak{I}}$. En appliquant H5, on voit alors que $h(\omega) = \mathfrak{I}^3$.

Remarque. L'étude du cas (10-2) du chap. V, §3 peut être faite en utilisant la proposition de ce paragraphe. En effet, dans ce cas, on a $h(\omega) = 1$ si $\omega \in C_Q(P)^{\#}$ d'après (11) du chap. V, §3, et on voit que $f(\omega) = \omega^{-\mathfrak{I}}$ pour un $\mathfrak{I} \in C_W(P)^{\#}$ en utilisant (5) du §2 du chap. VII et le fait que $C_Q(P)$ est quaternionien et $|C_W(P)| = 3$.

§4.- LE CAS OÙ $V \neq W$

D'après la proposition du §2 et le corollaire 1 de la proposition du §3, on peut supposer pour finir la preuve du théorème B que D a un sous-groupe P d'ordre premier p tel que $C_{Q/Q_o}(P) \neq 1$. Puisque $C_Q(P) \neq 1$, P a trois points fixes dans Ω donc est conjugué dans D à un sous-groupe de V. On peut donc supposer que $P \subset V$. Puisque W opère sans point fixe sur Q/Q_o , $P \cap W = 1$.

(1) Soit $U = O^{2'}(C_G(P))$. Alors $U/(P \cap U) \cong PSU(3,\ell)$, avec $q = \ell^p$ et $\ell > 2$.

D'après (B3), $C_G(P)$ est de 2-rang ≥ 2 et d'après le lemme 2 c) du chapitre V, §2, $U/Z(U) \cong PSU(3,\ell)$ pour un $\ell > 2$ car st est d'ordre 3 et $C_Q(P)$ d'exposant 4. On a $|C_{Q_o}(P)| = \ell$ donc $q = \ell^p$ car P opère comme un groupe d'automorphismes de corps sur Q_o (chapitre V, §1, prop.3). Comme $Z(U) \subset C_V(C_{Q_o}(P))$, on a $Z(U) \subset PW$ d'après le théorème de Galois. Puisque $PZ(U)$ centralise $C_Q(P) \not\subset Q_o$, on a $PZ(U) \cap W = 1$, donc $Z(U) \subset P$.

(2) Il existe $\omega \in Q-Q_o$, $\mathfrak{I} \in W^{\#}$ et $\eta \in P$ tels que $f(\omega) = \omega^{-\mathfrak{I}}$, $h(\omega) = \mathfrak{I}^3\eta^{-1}$ et η centralise ω et $\mathfrak{I}$.

D'après la structure de $PSU(3,\ell)$, $(V \cap U)/(P \cap U)$ centralise $C_{Q_o}(P)$. Donc $V \cap U \subset PW$ d'après le théorème de Galois, et puisque $U \subset C_G(P)$, $V \cap U \subset P \times C_W(P)$. De plus, $|(V \cap U)/(P \cap U)| = (\ell + 1)/(\ell + 1,3) \neq 1$ car $\ell > 2$. Soit $\mathfrak{z}_1 \in (V \cap U) - (P \cap U)$ et soit $\mathfrak{z} \in C_W(P)$ tel que $\mathfrak{z}_1 \in \mathfrak{z}P$. Si f_1, h_1 sont les applications f,h relatives à U, $U \cap H$ et t, d'après le corollaire 2 de la proposition du §3, il existe $\omega \in (Q-Q_o) \cap U$ tel que $f_1(\omega) \in \omega^{-\mathfrak{z}_1}(P \cap U)$ et $h_1(\omega) \in \mathfrak{z}_1^3(P \cap U)$. D'après l'unicité de la forme canonique d'un élément de G-H, $f(\omega) = f_1(\omega) = \omega^{-\mathfrak{z}_1} = \omega^{-\mathfrak{z}}$ et $h(\omega) = h_1(\omega) \in \mathfrak{z}^3 P$.

Dans le calcul qui suit, nous identifions encore $Q \rtimes KW$ au groupe $S_1 \rtimes K_1W_1$ du chapitre VI,§3. Alors η opère sur $Q/Q_o \cong E$ comme une application semi-linéaire (appendice V). On notera μ l'automorphisme de corps de E associé à η. Ainsi, si $x \in E$, x^η est défini par l'opération de η sur Q/Q_o et l'isomorphisme $Q/Q_o \cong E$, tandis que x^μ est défini par l'opération de η sur KW et l'isomorphisme $KW \cong K_1W_1$.

Posons $\omega^2 = (0,\alpha)$. Soient $a \in K$ tel que $a \neq \alpha^{-\tau}$ et $b \in K$ tel que $b^{1+\theta} = \alpha + a^{-(1+\theta)}$. Alors d'après (2) du §2, on a :

$$(3)\quad \overline{f(\omega s^a)} = \overline{f(\omega^{-\mathfrak{z}} s^{a^{-1}})a^{-2}} = \mathfrak{z} a^{-2}\, \overline{f(\omega s^b)}$$

(Pour $\rho \in Q$, $\bar{\rho}$ désigne l'image de ρ dans $E \cong Q/Q_o$). D'après (2) et (3) du §2, on a pour $a \in K$:

$f(\omega^{-1}s^{a^{-1}}) = f(f(\omega^{-1})s^a)a^2\, s^a = f(g(\omega^{-1})s^a)^{h(\omega^{-1})^t}\, f(\omega^{-1})$, donc

$f(\omega^{\mathfrak{z}^{-1}} s^a)a^2\, s^a = f(\omega^{\mathfrak{z}} s^a)^{\mathfrak{z}^{-3}\eta}\, \omega^{\mathfrak{z}^{-1}}$, donc :

$$(4)\quad a^2\, \overline{f(\omega s^a)} = \mathfrak{z}^{-1}\, \overline{f(\omega s^a)}^\eta + \bar{\omega}$$

Supposons encore que $a \neq \alpha^{-\tau}$ et dans (4), remplaçons $\overline{f(\omega s^a)}$ par le deuxième membre de (3):

$$(5)\quad \mathfrak{z}\, \overline{f(\omega s^b)} = a^{-2\mu}\, \overline{f(\omega s^b)}^\eta + \bar{\omega}$$

L'égalité (4) est valable avec b à la place de a :

$$(6)\quad b^2\,\overline{f(\omega s^b)} = \mathfrak{S}^{-1}\,\overline{f(\omega s^b)}^{\eta} + \overline{\omega}$$

Des combinaisons linéaires convenables de (5) et (6) montrent alors que $a^{2\mu} + b^2 \neq 0$ et :

$$(7)\quad \overline{f(\omega s^b)} = \frac{a^{2\mu} + \mathfrak{S}}{\mathfrak{S}(a^{2\mu}+b^2)}\ \overline{\omega}$$

$$(8)\quad \overline{f(\omega s^b)}^{\eta} = \frac{b^2 + \mathfrak{S}}{b^2 a^{-2\mu}+1}\ \overline{\omega}$$

Ces égalités impliquent que :

$$(9)\quad \frac{(\mathfrak{S}^{-1}+a^{-2\mu})^{\mu}}{(1+b^2a^{-2\mu})^{\mu}} = \frac{b^2+\mathfrak{S}}{1+b^2a^{-2\mu}}$$

Donc $(\mathfrak{S}^{-1} + a^{-2\mu^2})/(b^2 + \mathfrak{S}) = \lambda \in F$ et $\lambda\mathfrak{S}^2 + (\lambda b^2 + a^{-2\mu^2})\mathfrak{S} + 1 = 0$.

Comme $\mathfrak{S}^{1+q} = 1$ et $\mathfrak{S} \notin F$, il en résulte que $\lambda = 1$ et que $b^2 + a^{-2\mu^2} = \mathfrak{S} + \mathfrak{S}^{-1}$. Les dénominateurs des deux membres de (9) sont alors égaux et $b^2a^{-2\mu} = (\mathfrak{S} + \mathfrak{S}^{-1} + a^{-2\mu^2})\,a^{-2\mu}$ est fixe par μ . Il en résulte que pour $X \in F - \{0, \alpha^{2\tau}\}$, on a :

$$(10)\quad (\mathfrak{S} + \mathfrak{S}^{-1} + X^{\mu})X = (\mathfrak{S} + \mathfrak{S}^{-1} + X^{\mu^2})X^{\mu}$$

Soit $X \in F - \{0, \alpha^{2\tau}, \alpha^{2\tau}+1\}$. En écrivant (10) avec $X+1$ à la place de X et en retranchant (10), on voit que $X^{\mu^2} = X$. Il en résulte que $\mu = 1$ car μ est d'ordre impair, et si $\mu \neq 1$, on a $|F| \geq 8$. Donc $\eta \in W$ et $h(\omega) \in W$. On peut alors conclure par le corollaire 1 de la proposition du §3 .

APPENDICE X

UN CAS PARTICULIER D'UN THÉORÈME DE HUPPERT

Nous démontrons ici une proposition qui est un cas particulier du théorème de B. Huppert sur les groupes de permutations doublement transitifs résolubles (voir par exemple [HB], chapitre XII, §7).

Proposition. *Soit* D *un groupe d'ordre impair qui opère fidèlement sur un* q*-groupe abélien élémentaire* E *(*q *premier), et qui est transitif sur* $E^{\#}$. *Alors* F(D) *est cyclique et opère sans point fixe sur* E, *et* D/F(D) *est abélien.*

(Remarquer qu'avec les hypothèses de cette proposition, $E \rtimes D$ opère de manière doublement transitive sur E).

Lemme. *Soient* p *un nombre premier* $\neq 2$ *et* P *un* p*-groupe opérant fidèlement sur le* q*-groupe abélien élémentaire* E . *On suppose que* $|P_a|$ *est indépendant de* a *pour* $a \in E^{\#}$. *Alors* P *est cyclique et opère sans point fixe sur* E .

Démonstration du lemme : La loi de composition de E sera notée additivement et E sera considéré comme un $\mathbb{F}_q[P]$-module.

1) Supposons d'abord que $E = E_1 \oplus \ldots \oplus E_r$ où $r \geq 2$ et les E_i sont des sous-espaces de E permutés par P (c'est à dire $(E_i)g$ est l'un des E_j pour $g \in P$ et $1 \leq i \leq r$).

Soient $a \in E_1^{\#}$ et $b \in E_2^{\#}$. Si $x \in P_{a+b}$, on a $(a+b)x = ax + bx = a + b$. Comme P permute les E_i, il en résulte que $ax = a$ et $bx = b$,

ou $ax = b$ et $bx = a$. Mais puisque x est d'ordre impair, le deuxième cas est impossible. Donc $P_{a+b} = P_a \cap P_b$. Par hypothèse $|P_{a+b}| = |P_a| = |P_b|$, donc $P_a = P_b$. Ceci étant vrai pour tout $a \in E_1^{\#}$, P_a centralise E_1 . Puisque $P_a = P_b$ pour tout $b \in E_2^{\#}$, P_a centralise E_2 et de même, P_a centralise E_i pour $i > 1$. Donc P_a centralise E, d'où $P_a = 1$. D'après l'hypothèse, $P_a = 1$ pour tout $a \in E^{\#}$ et P opère sans point fixe sur E, donc P est cyclique.

2) Fin de la démonstration.

D'après 1) on peut supposer que P opère irréductiblement sur E . Supposons que P soit cyclique. ALors si $x \in P^{\#}$, $C_E(x)$ est un sous-espace de E stable par P et distinct de E, donc $C_E(x) = \{0\}$ et P opère sans point fixe sur E. On peut donc supposer que P n'est pas cyclique.

Alors d'après [H], chapitre III, (7-5), P a un sous-groupe normal R de type (p,p). Puisque P opère fidèlement et irréductiblement sur E, Z(P) est cyclique donc $|R \cap Z(P)| = p$ et P permute transitivement l'ensemble $\{T_i | i=1,\ldots,p\}$ des sous-groupes d'ordre p de R distincts de $R \cap Z(P)$. Puisque $C_E(R \cap Z(P))$ est un sous-espace de E invariant par P, on a $C_E(R \cap Z(P)) = \{0\}$. Soit $E_i = C_E(T_i)$. On sait alors que $E = \Sigma E_i$ et P opère sur l'ensemble des E_i .

Montrons que la somme des E_i est directe. Supposons que la somme $E_1 + \ldots + E_{k-1}$ soit directe, et soit $x \in E_k \cap (E_1 + \ldots + E_{k-1})$. On a $x = x_1 + \ldots + x_{k-1}$ où $x_i \in E_i$. Si $t \in T_k$, $xt = x_1t + \ldots + x_{k-1}t = x_1 + \ldots + x_{k-1}$. Comme t opère sur $E_i = C_E(T_i)$, il en résulte que t centralise x_i pour $i < k$, donc $R = \langle T_k, T_i \rangle$ centralise x_i . Donc $x_i = 0$ et $x = 0$, et la somme $E_1 + \ldots + E_k$ est directe.

Mais alors d'après 1), P est cyclique contrairement à l'hypothèse.

Démonstration de la proposition :

Soient $F = F(D)$, p un nombre premier impair et $P = O_p(F)$. Soient

$a,b \in E^{\#}$. Puisque $P \lhd D$ et D est transitif sur $E^{\#}$, P_a et P_b sont conjugués dans D. D'après le lemme, P est donc cyclique et opère sans point fixe sur E. Puisque $F = \Pi_p O_p(F)$, il en résulte que F est cyclique et opère dans point fixe sur E.

D'après les théorèmes de Feit-Thompson et de Fitting, $C_D(F) = F$, donc D/F est isomorphe à un sous-groupe de Aut(F) et par conséquent est abélien.

APPENDICE XI

SUR LES PRESQUE-CORPS

On dira qu'un ensemble fini F, muni de deux lois de composition + et . est un presque-corps si :

1. F est un groupe commutatif pour la loi + (l'élément neutre est noté 0).
2. $F - \{0\}$ est un groupe pour la loi . (l'élément neutre est noté 1).
3. On a $(a + b)c = ac + bc$ quels que soient $a,b,c \in F$.

H. Zassenhaus a classifié les presque-corps (finis) dans "Uber endliche Fastkörper", Abhandlungen Math. Sem. Hamburg Univ. 11 (1936), pp.187-221 , mais nous n'avons besoin ici que de certains résultats élémentaires.

Si F est un presque-corps, on posera $\mathcal{L}(F) = F \rtimes F^*$, où F^* est le groupe multiplicatif $F - \{0\}$ opérant par multiplication à droite sur F. Alors F^* opère régulièrement sur $F - \{0\}$. Réciproquement, si un groupe M opère sur un groupe abélien F, M étant régulier sur $F^\#$, on peut munir F d'une structure de presque-corps telle que $\mathcal{L}(F) \cong F \rtimes M$: il suffit de choisir un élément 1 de $F - \{0\}$ et de poser $(1x)(1y) = 1(xy)$ pour $x,y \in M$.

Soit F un presque-corps. Puisque F^* opère transitivement sur $F - \{0\}$, F est un f-groupe abélien élémentaire pour un nombre premier f, qu'on appelle la caractéristique de F.

Proposition 1. Soient L *un groupe de 2-rang 1,* M *un groupe de Bender propre de* L, t *une involution de* L-M , $D = M \cap M^t$. *On suppose que* L *opère fidèlement et de manière 2-transitive sur l'ensemble des conjugués de* M, *et que* D *a un complément normal* Q *dans* M. *Il existe alors un presque-corps* F, *un*

groupe Σ *d'automorphismes de* F *et un isomorphisme de* L *sur* $L(F) \rtimes \Sigma = (F \rtimes F^*) \rtimes \Sigma$ *qui identifie* Q *à* F^* *et* D *à* Σ

D'après l'appendice III, (2), $L = F \rtimes M = (F \rtimes Q) \rtimes D$ où F est un f-groupe abélien élémentaire qui opère régulièrement sur $A = \{M^x | x \in L\}$. Puisque Q opère régulièrement sur $A - \{M\}$, il opère régulièrement sur $F^\#$. On peut donc munir F d'une structure de presque-corps telle que $F \rtimes Q \cong F \rtimes F^*$. Le groupe D laisse fixe un élément de $F^\#$ (l'élément x tel que $M^x = M^t$) que l'on peut prendre comme élément 1 du presque-corps. De plus D opère fidèlement sur F, car il opère fidèlement sur A, et puisque D opère sur $F \rtimes Q$, D s'identifie donc à un groupe d'automorphismes du presque-corps F.

Les presque-corps $F_{r^2,2}$

Soit r une puissance d'un nombre premier impair, et $K = \mathbb{F}_{r^2}$. Pour $x, y \in K$, posons $x \circ y = xy$ si y est un carré dans le corps K, et $x \circ y = x^r y$ sinon. On vérifie alors que K, muni des lois de composition + et $\circ$ est un presque-corps. Ce presque-corps sera noté $F_{r^2,2}$.

Proposition 2. Soit F *un presque-corps (fini) dont le groupe multiplicatif a un sous-groupe cyclique d'indice 2. Alors* F *est un corps, ou bien il existe* r *tel que* F *soit isomorphe à* $F_{r^2,2}$. *De plus, dans ce deuxième cas,* $|Z(F^*)| = r - 1$.

Soit A le sous-groupe cyclique d'indice 2 de F^*. Supposons que A n'opère pas irréductiblement sur le groupe additif F. Alors $F = F_1 \oplus F_2$, $F_i \neq 0$ et A opère sans point fixe sur F_i, donc $|F_i| \geq |A| + 1$ et $|F| = 2|A| + 1 \geq (|A| + 1)^2$, ce qui est impossible. Donc A opère irréductiblement sur F.

Notons $\circ$ la multiplication du presque-corps F. D'après l'appendice V,

on peut définir sur F une multiplication . qui en fait un corps K ayant même addition et même élément 1 que F, et telle que pour $a \in A$ et $x \in F$, $x \circ a = xa$. De plus, pour $a \in F - \{0\}$, l'application $x \mapsto x \circ a$ est semi-linéaire, donc il existe un automorphisme σ_a de K tel que :

$$x \circ a = (1x) \circ a = x^{\sigma_a}(1 \circ a) = x^{\sigma_a} a .$$

On voit que $a \mapsto \sigma_a$ est un homomorphisme de F^* dans Aut(K) dont le noyau contient A. Si ce noyau est F^* , on a $F^* \cong K^*$ et F est un corps. Sinon, pour $a \in F^* - A$, σ_a est d'ordre 2, donc il existe r tel que $K = \mathbb{F}_{r^2}$, et $x^{\sigma_a} = x^r$. Comme A est aussi le sous-groupe d'indice 2 de K^* et $x \circ a = x^{\sigma_a} a$ pour $x \in F$, $a \in F^*$, on voit que $F \cong F_{r^2,2}$.

On a dans ce cas $Z(F^*) \subset A$, sinon F^* serait abélien et F serait un corps. Si $x \in A$ et $y \in F^* - A$, $x \circ y = x^r y$ et $y \circ x = yx$, donc $x \in Z(F^*)$ si et seulement si $x^r = x$, c'est à dire $x \in \mathbb{F}_r^*$.

APPENDICE XII

LE THÉORÈME DE FEIT-SIBLEY

Nous démontrons dans cet appendice une forme du théorème de Feit-Sibley adaptée à nos besoins. Ce théorème a sa source dans les travaux de W. Feit, en particulier dans son article "On a class of doubly transitive permutation groups", Illinois J. Math, Vol. 4 (1960), pp. 170-186. Un cas laissé de côté dans cet article a été traité par D.A. Sibley dans "Coherence in finite groups containing a Frobenius section ", Illinois J. Math, Vol. 20 (1976), pp.434-442 . Un cas particulier (qui n'est pas suffisant pour notre application) est traité dans le livre d'Isaacs. Ce théorème a été généralisé par L. Puig dans "Structure locale et caractères", J. of Algebra, Vol. 56 (1979), pp. 24-42 .

Soient G un groupe fini, H un sous-groupe de G, $\mathcal{S}$ une partie de Irr(H) et τ une isométrie linéaire de $\mathbb{Z}[\mathcal{S}]^\circ$ dans $\mathbb{Z}[\mathrm{Irr}(G)]^\circ$ (voir [Is] pour les notations). Rappelons que $(\mathcal{S},\tau)$, ou $\mathcal{S}$ s'il n'y a pas d'ambiguïté sur τ, est dit cohérent si $|\mathcal{S}| \geq 2$ et si τ peut se prolonger en une isométrie linéaire de $\mathbb{Z}[\mathcal{S}]$ dans $\mathbb{Z}[\mathrm{Irr}(G)]$.

Le théorème de Feit-Sibley montre que sous certaines conditions particulières sur H et $\mathcal{S}$, $\mathcal{S}$ est cohérent, ce qui donne des informations sur les caractères de G à partir des caractères de H. On a d'abord :

Lemme 1. *a) Supposons que* $S = S_0 \cup \{\psi\}$, *que* (S_0, τ) *soit cohérent et qu'il existe* $\chi_0 \in S_0$ *tel que* $\chi_0(1) | \psi(1)$ *et* $2\chi_0(1)\psi(1) < \Sigma_{\chi \in S_0} \chi(1)^2$. *Alors* (S, τ) *est cohérent.*

b) Si $|S| \geq 2$ *et si tous les* $\chi \in S$ *ont même degré, alors* (S, τ) *est cohérent.*

Pour la démonstration, voir [Is], 7-14 et 7-15 .

Hypothèses et notations :

G est un groupe fini, $H = Q \rtimes D$ est un sous-groupe propre de G . On suppose que $(|D|, |Q|) = 1$ et que pour $x \in G-H$, on a $Q \cap Q^x = 1$ (Ces hypothèses impliquent que Q est un sous-groupe de Hall de G car si P est un groupe de Sylow $\neq 1$ de Q, $N_G(P) \subset H$).

$Q = S \times Q_1$, $|Q_1|$ et $|S|$ sont premiers entre eux, D opère sans point fixe sur Q_1 , Q_1 n'est pas un 2-groupe et S est nilpotent

$$S = \{\chi \in \mathrm{Irr}(H) \mid Q_1 \not\subset \mathrm{Ker}\ \chi\}$$

On pose $S' = [S,S]$, $Q' = [Q,Q]$, $d = |D|$ et si $R \subset Q$, $S(R) = \{\chi \in S \mid R \subset \mathrm{Ker}\chi\}$.

Lemme 2. *a) S est l'ensemble des* $\mathrm{Ind}_Q^H \phi$ *où* $\phi \in \mathrm{Irr}(Q)$ *et* $Q_1 \not\subset \mathrm{Ker}\phi$.

b) L'application $\psi \mapsto \mathrm{Ind}_H^G \psi$ *est une isométrie de* $\mathbb{Z}[S]^\circ$ *dans* $\mathbb{Z}[\mathrm{Irr}(G)]^\circ$.

a) Soit $\phi = \lambda\theta$ où $\lambda \in \mathrm{Irr}(S)$ et $\theta \in \mathrm{Irr}(Q_1)-\{1\}$. Si $x \in H$ est tel que $\phi^x = \phi$, alors $\theta^x = \theta$, donc $x \in Q$ car $Q_1 D$ est un groupe de Frobenius ([Is], 6-34). Donc le groupe d'inertie de ϕ dans H est Q , donc $\mathrm{Ind}_Q^H \phi$ est irréductible ([Is], 6-11). On a $Q_1 \not\subset \mathrm{Ker}\ \mathrm{Ind}_Q^H \phi$ car sur Q_1 , $\mathrm{Ind}_Q^H \phi$ prend les mêmes valeurs que $\mathrm{Ind}_{Q_1}^{Q_1 D} \theta$.

Si $\chi \in S$, $\mathrm{Res}_Q^H \chi$ a un constituant ϕ tel que $Q_1 \not\subset \mathrm{Ker}\ \phi$. Alors χ est un constituant de $\mathrm{Ind}_Q^H \phi$, donc $\chi = \mathrm{Ind}_Q^H \phi$.

b) résulte de [Is], 7-7 car les éléments de S s'annulent sur H-Q d'après a).

Théorème. Si d *est impair,* S *est cohérent pour l'isométrie du lemme 2 b).*

Remarquons que $|S(Q')| \geq 2$ car $O_{2'}(Q_1) \rtimes D$ est un groupe de Frobenius d'ordre impair. D'après le lemme 1 b), $S(Q')$ est cohérent.

(1) *Supposons que* $|Q_1|$ *soit divisible par deux nombres premiers. Alors* $S(S')$ *est cohérent.*

On peut supposer que Q_1 n'est pas abélien. Soit $Q_2 \subset [Q_1,Q_1]$ tel que $Q_2 \lhd H$ et tel que $S(S'Q_2)$ soit cohérent. Soit $Q_3 \lhd Q_2$ tel que Q_2/Q_3 soit un facteur principal de H. Il suffit de montrer que $S(S'Q_3)$ est cohérent car alors, si on prend Q_2 minimal pour les conditions ci-dessus, on aura $Q_2 = 1$. Supposons que $S(S'Q_3)$ ne soit pas cohérent. D'après le lemme 1 a), il existe $\psi \in S(S'Q_3)$ tel que

$$\Sigma_{\chi \in S(S'Q_2)} \chi(1)^2 \leq 2d\psi(1)$$

On a $\Sigma_{\chi \in S(S'Q_2)} \chi(1)^2 = |H/S'Q_2| - |H/S'Q_1| = d|S/S'|(|Q_1/Q_2| - 1)$, d'où :

(1-1) $\quad |Q_1/Q_2| - 1 \leq 2\psi(1)$

Soit $Z/Q_3 = Z(Q_1/Q_3)$. On a $\psi(1) = d\phi(1)$ où $\phi \in \mathrm{Irr}(Q/S'Q_3)$, et d'après [Is], 2-30, on a $\phi(1)^2 \leq |Q/SZ|$, donc :

(1-2) $\quad \psi(1)^2 \leq d^2|Q/SZ| = d^2|Q_1/Z|$

Puisque Q_1 est nilpotent, on a $(Q_2/Q_3) \cap (Z/Q_3) \neq 1$, et Q_2/Q_3 étant un facteur principal de H, $Q_2 \subset Z$. De plus, puisque $|Q_1|$ a deux diviseurs premiers, on a $Q_2 \subsetneq Z$. D'après (1-1) et (1-2), on a :

$(|Q_1/Q_2| - 1)^2 \leq 4\, d^2|Q_1/Z|$, d'où :

$|Q_1/Q_2|(|Q_1/Q_2| - 2) < 4\, d^2|Q_1/Z|$, ou :

$|Z/Q_2|(|Q_1/Q_2| - 2) < 4\, d^2$.

Mais puisque D opère sans point fixe sur Q_1 et $Q_2 \subsetneq Z \subsetneq Q_1$, on a $|Z/Q_2| \geq d+1$ et $|Q_1/Q_2| \geq (d+1)^2$, donc $(d+1)^2 - 2 < 4d$, d'où $d \leq 2$ ce qui est impossible.

(2) *Supposons que $S(S')$ soit cohérent. Alors S est cohérent.*

On peut supposer que $S' \neq 1$. Comme dans (1), prenons $S_1 \subset S'$, $S_1 \lhd H$ tel que $S(S_1)$ soit cohérent, $S_2 \lhd S_1$ tel que S_1/S_2 soit un facteur principal de H, et supposons que $S(S_2)$ ne soit pas cohérent. Il existe alors $\psi \in S(S_2)$ tel que

$$d|S/S_1|(|Q_1| - 1) = \sum_{\chi \in S(S_1)} \chi(1)^2 \leq 2d\psi(1)$$

Soit $Z/S_2 = Z(S/S_2)$. Alors $S_1 \subset Z$ car S est nilpotent. On a $\psi(1) = d\phi(1)$ où $\phi \in \mathrm{Irr}(Q/S_2)$ et $\phi(1)^2 \leq |S/Z|.|Q_1/Z(Q_1)| \leq |S/S_1|.|Q_1/Z(Q_1)|$, d'où :

$$|S/S_1|(|Q_1| - 1)^2 \leq 4\, d^2 |Q_1/Z(Q_1)| \quad \text{et}$$

$$|S/S_1|.|Z(Q_1)|(|Q_1| - 2) < 4\, d^2$$

Mais puisque d est impair et D opère sans point fixe sur Q_1 , $|Z(Q_1)| \geq 2d+1$, donc $|S/S_1| < 4\, d^2/(4d^2-1) < 2$, ce qui est impossible.

D'après (1) et (2), on peut supposer désormais que Q_1 est un p-groupe non-abélien, p étant un nombre premier impair.

(3) *Soit $1 \neq Z \lhd H$ tel que $Z \subset Z(Q_1)$. Alors $X = S - S(Z)$ est cohérent.*

Montrons d'abord que $X_1 = X \cap S(S')$ est cohérent. On a $|X_1| \geq 2$ car $Z \neq 1$ et si $\chi \in X_1$, $\overline{\chi} \neq \chi$ (la restriction de χ au sous-groupe $Q_1 D$ d'ordre impair étant irréductible). Soit $X_1 = \{\chi_1, \ldots, \chi_r\}$, $\chi_1(1) \leq \ldots \leq \chi_r(1)$. Puisque χ_i est l'induit à H d'un caractère ϕ_i de $\mathrm{Irr}(S/S' \times Q_1)$, $\chi_i(1)$ est de la forme dp^{k_i} , k_i entier. On a pour $i > 1$:

$$\Sigma_{1 \leq j < i} \chi_j(1)^2 = |H/S'| - |H/S'Z| - \Sigma_{i \leq j \leq r} \chi_j(1)^2 \ .$$

Le membre de gauche de cette égalité est divisible par d^2 , et le membre de droite par $\phi_i(1)^2$ car $\phi_i(1)^2 \leq |Q_1/Z(Q_1)| \leq |Q_1/Z|$ d'après [Is], 2-30 . Donc :

(3-1) Pour $1 < i \leq r$, $\chi_i(1)^2$ divise $\Sigma_{1\leq j<i}\ \chi_j(1)^2$

Soit k le plus grand indice tel que $\chi_k(1) = \chi_1(1)$. on a $k \geq 2$ car $\overline{\chi_1} \neq \chi_1$ et $\{\chi_1,\ldots, \chi_k\}$ est cohérent (lemme 1b)). Supposons $k < r$. Pour $i > k$, on a d'après (3-1) :

$$2\chi_1(1)\chi_i(1) < p\chi_1(1)\chi_i(1) \leq \chi_i(1)^2 \leq \Sigma_{1\leq j<i}\ \chi_j(1)^2$$

D'après le lemme 1, il en résulte que χ_1 est cohérent.

Pour montrer (3), on peut alors supposer que $S' \neq 1$. Soient comme dans (2) $S_1 \subset S'$, $S_1 \lhd H$ tel que $\chi \cap \mathcal{S}(S_1)$ soit cohérent, et $S_2 \lhd S_1$ tel que S_1/S_2 soit un facteur principal de H. Supposons que $\chi \cap \mathcal{S}(S_2)$ ne soit pas cohérent. Un élément ψ de $\chi \cap \mathcal{S}(S_2)$ est de la forme $\mathrm{Ind}_Q^H(\lambda\theta)$, $\lambda \in \mathrm{Irr}(S/S_2)$, $\theta \in \mathrm{Irr}(Q_1)$, $Z \not\subset \mathrm{Ker}\theta$. Comme $\mathrm{Ind}_Q^H(1.\theta) \in \chi_1$, il en résulte que $\chi_1(1)$ divise $\psi(1)$. D'après le lemme 1 a), il existe donc $\psi \in \chi \cap \mathcal{S}(S_2)$ tel que

$$d|S/S_1|.|Q_1/Z|(|Z| - 1) = \Sigma_{\chi\in\chi\cap\mathcal{S}(S_1)}\ \chi(1)^2 \leq 2\chi_1(1)\psi(1)$$

On a $\chi_1(1)^2 \leq d^2|Q_1/Z(Q_1)| \leq d^2|Q_1/Z|$ et puisque $S_1/S_2 \subset Z(S/S_2)$, $\psi(1)^2 \leq d^2|S/S_1|.|Q_1/Z|$. Il en résulte que :

$$d^2|S/S_1|^2|Q_1/Z|^2(|Z| - 1)^2 \leq 4\ d^4|S/S_1||Q_1/Z|^2 \quad \text{ou :}$$

$$|S/S_1|(|Z| - 1)^2 \leq 4\ d^2$$

Mais puisque D opère sans point fixe sur Z, $|Z| \geq 2d + 1$, donc $|S/S_1| \leq 1$ ce qui est impossible.

(4) Notations.

Soit $\mathcal{Y} = \mathcal{S}(Q') = \{\eta_1 ,\ldots, \eta_m\}$. Soit $Z = [Q_1,Q_1] \cap Z(Q_1)$; puisque

Q_1 est supposé non abélien, $Z \neq 1$. Soit $\mathcal{X} = \mathcal{S} - \mathcal{S}(Z) = \{\chi_1, \ldots, \chi_n\}$, $\chi_1(1) \leq \ldots \leq \chi_n(1)$ et posons $\chi_i(1) = a_i\chi_1(1)$. Alors a_i est entier (voir (3)). On a $\mathcal{X} \cap \mathcal{Y} = \emptyset$ et on sait que $\mathcal{X}$ et $\mathcal{Y}$ sont cohérents, c'est à dire qu'il existe $e_i \in \pm\mathrm{Irr}(G)$ $(1 \leq i \leq n)$ et $e'_j \in \pm\mathrm{Irr}(G)$ $(1 \leq j \leq m)$ tels que

$$\mathrm{Ind}_H^G(\chi_i - a_i\chi_1) = e_i - a_ie_1 \quad (2 \leq i \leq n)$$

$$\mathrm{Ind}_H^G(\eta_j - \eta_1) = e'_j - e'_1 \quad (2 \leq j \leq m)$$

(5) *Quels que soient* i,j , *on a* $[e_i, e'_j] = 0$.

Puisque Ind_H^G est une isométrie sur $\mathbb{Z}[\mathcal{S}]^\circ$, on a $[e_i - a_ie_1, e'_2 - e'_1] = 0$ pour $2 \leq i \leq n$. Soit $\lambda = [e_i - a_ie_1, e'_1] = [e_i - a_ie_1, e'_2]$. Si $\lambda \neq 0$, alors $a_i = 1$, $\lambda = \pm 1$ et $e_i - e_1 = \lambda(e'_1 + e'_2)$. Mais $e_i(1) - e_1(1) = 0$ et $e'_1(1) - e'_2(1) = 0$, d'où $e'_1(1) = 0$, ce qui est absurde. Donc $\lambda = 0$, $e_i \neq \pm e'_1$ et $e_1 \neq \pm e'_1$.

(6) *Posons* $\chi_1(1) = ad$. *Il existe* $\lambda \in \mathbb{Z}$ *et* $v \in \mathbb{Z}[\mathrm{Irr}(G)]$ *tels que*

$$\mathrm{Ind}_H^G(\chi_1 - a\eta_1) = -ae'_1 + \lambda\Sigma_{i=1}^m e'_i + v \quad , [v, e'_i] = 0 \quad (1 \leq i \leq m) \quad .$$

Si λ *est divisible par* a, *alors* $\mathcal{S}$ *est cohérent*

La première assertion résulte de ce que $[\mathrm{Ind}_H^G(\chi_1 - a\eta_1), \mathrm{Ind}_H^G(\eta_i - \eta_1)] = a$ pour $i > 1$. Supposons que $\lambda = ax$, $x \in \mathbb{Z}$. On a

$$1 + a^2 = [\chi_1 - a\eta_1, \chi_1 - a\eta_1] = [v,v] + a^2(x-1)^2 + (m-1)x^2a^2$$

donc $(x-1)^2 + (m-1)x^2 \leq 1 + 1/a^2$, et $a > 1$ car $\mathcal{X} \cap \mathcal{Y} = \emptyset$. Donc $x = 0$, ou $x = 1$ et $m = 2$. Le deuxième cas se ramène au premier en remplaçant e'_1, e'_2 par $-e'_2, -e'_1$. On peut donc supposer que $x = 0$, d'où $\lambda = 0$, $[v,v] = 1$ et $\mathrm{Ind}_H^G(\chi_1 - a\eta_1) = v - ae'_1$. On a $-1 = [\mathrm{Ind}_H^G(\chi_2 - \chi_1), \mathrm{Ind}_H^G(\chi_1 - a\eta_1)] = [e_2, v] - [e_1, v]$, donc $v = e_1$ ou $v = -e_2$. Dans le deuxième cas, $n = 2$ car sinon $-a_3 = [\mathrm{Ind}_H^G(\chi_3 - a_3\chi_1), \mathrm{Ind}_H^G(\chi_1 - a\eta_1)] = 0$, et on se ramène

au premier cas en remplaçant e_1, e_2 par $-e_2, -e_1$. Donc $\mathrm{Ind}_H^G(\chi_1 - a\eta_1) = \pm(e_1 - ae_1')$. Alors $X \cup Y$ est cohérent car Ind_H^G coïncide avec l'isométrie $\chi_i \mapsto e_i$, $\eta_j \mapsto e_j'$ sur $\mathbb{Z}[X]^\circ$, sur $\mathbb{Z}[Y]^\circ$ et sur $\chi_1 - a\eta_1$, qui engendrent $\mathbb{Z}[X \cup Y]^\circ$.

Soient $X_1 = X \cap S(S')$ et $\psi \in S(S') - (X_1 \cup Y)$. Comme dans (3-1), $\psi(1)^2$ divise $\Sigma_{\chi \in X_1} \chi(1)^2 = |H/S'| - |H/S'Z|$, d'où :

$$2\eta_1(1)\psi(1) \leq p\eta_1(1)\psi(1) \leq \psi(1)^2 \leq \Sigma_{\chi \in X_1} \chi(1)^2 < \Sigma_{\chi \in X_1 \cup Y} \chi(1)^2 .$$

D'après le lemme 1 a), il en résulte que $S(S')$ est cohérent, et d'après (2), S est cohérent.

(7) *Soit* $\psi \in \mathrm{Irr}(G)$ *tel que* ψ *soit constant sur* $Z^\#$. *Alors si* $z \in Z^\#$, $\psi(z) \equiv \psi(1)$ *mod.*$|Q|$.

Remarquons que $\psi(z) \in \mathbb{Z}$ car ψ est constant sur $Z^\#$. Soient K_s les classes de conjugaison de G ($s = 0,1,2,\ldots$), et K_s la somme des éléments de K_s dans l'algèbre du groupe G. Soit ω l'homomorphisme de $Z\mathbb{C}[G]$ dans $\mathbb{C}$ associé à ψ : $\omega(K_s) = \psi(K_s)/\psi(1)$. On a

(7-1) $\omega(K_i)\omega(K_j) = \Sigma_s a_{ijs}\, \omega(K_s)$, où $K_iK_j = \Sigma_s a_{ijs} K_s$

Soient i et j tels que $K_i \cap Z^\# \neq \emptyset$ et $K_j \cap Z^\# \neq \emptyset$. Montrons que :

(7-2) $\psi(1)\omega(K_i)\omega(K_j) \equiv \Sigma_{s, K_s \cap Z \neq \emptyset} \psi(1) a_{ijs}\, \omega(K_s)$ mod.$|Q|$

(On écrit $x \equiv y$ mod.$|Q|$ si x, y et $(x-y)/|Q|$ sont des entiers algébriques).

Supposons que $K_s \cap Z = \emptyset$. Soient $u \in K_i$, $v \in K_j$ tels que $uv \in K_s$, et $w \in Q^\#$. Si $u^w = u$ et $v^w = v$, on a $u \in C_G(w) \subset H$ et $v \in C_G(w) \subset H$, donc $u \in K_i \cap H$ et $v \in K_j \cap H$. Puisque $Z \lhd H$ et Q est à intersections triviales dans G, $K_i \cap H \subset Z$ et $K_j \cap H \subset Z$, donc $uv \in Z$, contrairement à l'hypothèse. Il en résulte que Q opère sans point fixe sur $\{(u,v) \mid u \in K_i, v \in K_j, uv \in K_s\}$ de cardinal $a_{ijs}|K_s|$. Si $x \in K_s$, $|Q|$ divise donc

$a_{ijs}|K_s|\psi(x) = \psi(1)a_{ijs}\omega(K_s)$. Cela prouve (7-2).

Soit $K_o = \{1\}$. Pour $K_s \cap Z^\# \neq \emptyset$, $\alpha = \omega(K_s)$ est indépendant de s par hypothèse. La congruence (7-2) donne donc :

(7-3) $\psi(1)\alpha^2 \equiv \psi(1)(a_{ijo} + a_{ij}\alpha) \mod.|Q|$, avec $a_{ij} \in \mathbb{N}$.

Puisque d est impair, on peut supposer que $K_1 \cap Z^\# \neq \emptyset$ et $K_2 = (K_1)^{-1}$. En appliquant (7-3) à $(i,j) = (1,1)$ puis $(i,j) = (1,2)$, on obtient :

(7-4) $\psi(1)a_{11}\alpha \equiv \psi(1)(|G:Q| + a_{12}\alpha) \mod.|Q|$

En appliquant ceci à $\psi = 1_G$, on voit que $|G:Q|a_{11} \equiv |G:Q| + a_{12}|G:Q| \mod.|Q|$ d'où $a_{11} \equiv 1 + a_{12} \mod.|Q|$ car Q est un sous-groupe de Hall de G, et (7-4) devient :

$$\psi(1)(1 + a_{12})\alpha \equiv \psi(1)(|G:Q| + a_{12}\alpha) \mod.|Q|$$

d'où $\psi(1)\alpha \equiv \psi(1)|G:Q| \mod.|Q|$. Mais si $z \in Z^\#$, $\alpha = |G:Q|\psi(z)/\psi(1)$, donc $|G:Q|\psi(z) \equiv |G:Q|\psi(1) \mod.|Q|$ et il en résulte que $\psi(z) \equiv \psi(1) \mod.|Q|$.

(8) *Conclusion.*

D'après (5) et (6), on a

$[\mathrm{Res}_H^G e_1' , \chi_i - a_i\chi_1] = 0$ pour $i \geq 2$ et $[\mathrm{Res}_H^G e_1' , \chi_1 - a\eta_1] = \lambda - a$, donc

$$\mathrm{Res}_H^G e_1' = (\lambda + a\mu) \Sigma_{i=1}^n a_i\chi_i + \chi'$$

où χ' est un caractère de H tel que $[\chi',\chi_i] = 0$ pour tout i et $\mu = [\mathrm{Res}_H^G e_1', \eta_1] - 1$. On a $\Sigma_{i=1}^n a_i\chi_i = \frac{1}{da}(\rho_H - \rho_{H/Z})$, ρ_X désignant le caractère régulier d'un groupe X. D'autre part, puisqu'aucune composante irréductible de χ' n'appartient à X , on a $Z \subset \mathrm{Ker}\chi'$. Il en résulte que pour $z \in Z^\#$,

$$e_1^!(z) - e_1^!(1) = (\lambda+a\mu)(-\frac{|H|}{da}) = -|Q|(\frac{\lambda}{a}+\mu) .$$

D'après (7), a divise alors λ et la conclusion résulte de (6).

Remarque. Si d est pair et $|\mathcal{S}| \geq 2$, la conclusion du théorème est encore vraie. En effet, dans ce cas Q_1 est abélien, et $|Q_1| > d+1$ ou $S \neq 1$. On voit alors que $\mathcal{S}(Q') = \mathcal{S}(S')$ est cohérent, et si $\mathcal{S}$ n'est pas cohérent, $S' \neq S$ et $|S/S'|.|Q_1|(|Q_1| - 2) < 4d^2$ (voir (2)). Mais $|Q_1| \geq d+1$, d'où $|S/S'| < 4\ d^2/(d^2-1) < 6$, ce qui est impossible, $|S/S'| = 4$ étant exclu par l'hypothèse $(|D|,|Q|) = 1$.

Thomas Peterfalvi
U.E.R. de Mathématique et Informatique
Université Paris 7
2 , Place Jussieu ,
75251 Paris cedex 05