Astérisque

THOMAS PETERFALVI

Le théorème de Bender-Suzuki I

Astérisque, tome 142-143 (1986), p. 141-233

<http://www.numdam.org/item?id=AST_1986__142-143__141_0>

© Société mathématique de France, 1986, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Société Mathématique de France
Astérisque 142-143 (1986)

LE THÉORÈME DE BENDER-SUZUKI I

Par Thomas Peterfalvi

0
0 0

INTRODUCTION

L'objet du théorème de H. Bender et M. Suzuki est la détermination des groupes finis G qui satisfont la condition suivante :

(*) G a un sous-groupe propre H tel que H soit d'ordre pair, mais que $H \cap H^x$ soit d'ordre impair pour tout $x \in G - H$.

Un tel sous-groupe de G a été appelé "stark eingebettet" par H. Bender.

Ce théorème montre en particulier qu'un groupe simple qui satisfait la condition (*) est nécessairement un groupe de type de Lie de rang 1 sur un corps fini de caractéristique 2.

Ce théorème est l'une des bases de la classification des groupes simples finis. Il intervient de deux manières dans cette classification.

D'abord, pour un 2-groupe Q, soit m(Q) le rang de Q, c'est-à-dire le maximum des rangs des sous-groupes abéliens élémentaires de Q. Soit G un groupe fini et P un 2-Sylow de G. Si k est un entier, posons $B_k(G,P) = < N_G(Q) \mid Q \subset P \text{ et } m(Q) \geq k >$. Dans la classification des groupes simples, le cas général est celui où $B_2(G,P) = G$. (On peut dans ce cas utiliser des "signalizer functors"). Le cas où $B_1(G,P) \neq G$ est le sujet du théorème de Bender-Suzuki, et celui où $B_1(G,P) = G$, mais $B_2(G,P) \neq G$ a été traité par M. Aschbacher.

Ensuite, pour la caractérisation d'un groupe connu G_o, on utilise en général des hypothèses sur la structure 2-locale d'un groupe G (c'est-à-dire sur les groupes $N_G(Q)$, où Q est un 2-sous-groupe non trivial de G), et on veut montrer que G est isomorphe à G_o. Pour cela, une des méthodes est de démontrer que si P est un 2-Sylow de G, $B_1(G,P)$ est isomorphe à G_o, puis invoquer le théorème de Bender-Suzuki pour démontrer que $B_1(G,P) = G$.

Les deux principales contributions à la démonstration du théorème de Bender-Suzuki sont les articles :

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

[B] H. BENDER : Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlässt. J. of Algebra 17 (1971), pp. 527-554.

Cependant ces articles font référence à des résultats antérieurs qui ne figurent pas dans les traités classiques sur les groupes finis, et pour avoir une démonstration complète, il faut, dans la situation actuelle, lire une dizaine d'articles, même en admettant certains théorèmes généraux comme celui de Feit-Thompson.

Ces résultats antérieurs comprennent les travaux de Zassenhaus [Abh. Math. Sem. Univ. Hamburg 11 (1936), pp. 17-40 et 187-220] (caractérisation de PSL(2,q) et étude des presque-corps) ; la détermination des groupes de Zassenhaus, qui a été faite par W. Feit et M. Suzuki en 1960-62 [W. Feit : Ill. J. of Math. 4 (1960), pp. 170-186, M. Suzuki : Ann of Maths. n°75 (1962), pp. 105-145] ; une caractérisation de PSL(2,q) par W. Feit [Amer. J. of Maths. 82 (1960), pp. 281-300] ; un article de G. Higman qui permet de déterminer les 2-groupes de Sylow d'un groupe G satisfaisant (*) [Ill. J. of Maths. 7 (1963), pp. 79-96] ; un article de C. Hering sur les groupes finis opérant de manière doublement transitive sur leurs involutions [Archiv der Math. 22 (1971), p. 456] ; enfin l'article de W. Kantor et G. Seitz : Finite groups with a split BN-pair of rank 1 - II [J. of Alg. 20 (1972), pp. 476-494] comporte un rectificatif à l'article principal de M. Suzuki.

D'autre part, le style des articles [S] et [B] est assez hétérogène. L'article de H. Bender est relativement concentré et très précis. La première partie de l'article de M. Suzuki est de lecture assez facile. La deuxième partie est plus difficile et contient quelques erreurs.

Ce travail est la première partie d'une rédaction de la démonstration du théorème de Bender-Suzuki. Une deuxième partie, qui apportera certaines simplifications à l'article [S] est en cours de rédaction.

Les trois premiers chapitres exposent l'article [B]. Dans le chapitre I, on montre que, avec la notation de (*), si G est de 2-rang ≥ 2, alors G opère de manière doublement transitive sur l'ensemble Ω des conjugués de H dans G. La démonstration est un peu simplifiée par la remarque, due à M.Enguehard et L. Puig, qu'il suffit d'étudier les p-sous-groupes maximaux fixant 3 points

de Ω au lieu des p-sous-groupes maximaux fixant 3 points dont un point donné. Dans le chapitre II, on démontre un résultat qui permet d'appliquer une hypothèse de récurrence à $N_G(X)$ si X est un sous-groupe $\neq 1$ de G qui fixe 3 points de Ω. Dans le chapitre III, on démontre que si G est de 2-rang ≥ 2 et si $O_{2'}(G) = 1$, alors H a un sous-groupe normal qui opère régulièrement sur $\Omega - \{H\}$. Cette dernière propriété, avec (*), est l'hypothèse de départ de [S].

Dans le chapitre IV, on démontre qu'un groupe d'ordre pair qui opère de manière doublement transitive sur ses involutions est de 2-rang 1, résultat qui est utilisé dans le chapitre III. Ce chapitre IV comprend un exposé de l'article de C. Hering cité ci-dessus, la démonstration d'un résultat antérieur de A. Wagner sur les groupes de collinéations doublement transitifs sur les points d'un espace projectif, et la démonstration d'un résultat de J.L. Alperin sur les extensions d'un 2-groupe par $GL(3, \mathbb{F}_2)$ dont à notre connaissance seul l'énoncé a été publié (les résultats de Wagner et d'Alperin sont utilisés dans l'article de Hering).

Les démonstrations de certains résultats auxiliaires sont reportées en appendices.

En plus des articles originaux, nous avons utilisé un manuscrit de C. Chevalley, un exposé de Y. Auffray au séminaire sur les groupes finis de Paris VII (1979) et un texte de M. Enguehard et L. Puig.

Théorèmes généraux utilisés.

Le théorème de Brauer-Suzuki : Soit G un groupe de 2-rang 1, c'est-à-dire ayant un sous-groupe d'ordre 2 mais pas de sous-groupe non cyclique d'ordre 4, et soit t une involution de G. On a $G = O_{2'}(G)C_G(t)$.

Référence : R. BRAUER and M. SUZUKI : On finite groups of even order whose 2 Sylow subgroup is a quaternion group, Proc. Nat. Acad. Sci. USA 45 (1959), pp. 1757-1759.

Le théorème de Feit-Thompson : Tout groupe d'ordre impair est résoluble.

Référence : W. FEIT and J.G THOMPSON : Solvability of groups of odd order. Pacific J. of Math. Vol 13 (1963), pp. 775-1029.

Le théorème ZJ de Glauberman : Soit p un nombre premier $\neq 2$. Tout p-groupe fini P a un sous-groupe caractéristique A(P) vérifiant les conditions suivan-

tes : si $P \neq 1$, $A(P) \neq 1$. Supposons que G soit un groupe fini résoluble dont P est un p-Sylow et que G n'ait pas de section (quotient d'un sous-groupe) isomorphe à SL(2,p), alors $O_{p'}(G)A(P)$ est un sous-groupe caractéristique de G.

Référence : G. GLAUBERMAN : A characteristic subgroup of a p-stable group. Canad. J. Math. 20 (1968), pp. 1101-1135, theorem A. Dans cet article, la condition faisant intervenir G n'est énoncée que si $O_{p'}(G) = 1$, mais le cas général s'en déduit facilement.

Pour les autres résultats utilisés, nous renvoyons aux livres :

B. HUPPERT : Endliche Gruppen I. (Springer Verlag, 1968).
I.M. ISAACS : Character theory of finite groups (Academic Press 1976).

Dans les chapitres II et III, on utilise en plus quelques propriétés élémentaires des groupes PSL(2,q), PSU(3,q), Sz(q) et à la fin du chapitre IV, on utilise la classification des 2-groupes de Suzuki (article de G. Higman), qui a été exposée dans un séminaire de Paris VII en 1979.

Notations.

L'élément neutre d'un groupe est noté 1, et un groupe réduit à l'élément neutre est aussi noté 1.

Les opérations d'un groupe sur un ensemble ou sur un groupe sont des opérations à droite, sauf mention du contraire.

"p-Sylow" est une abréviation de "p-sous-groupe de Sylow".

$\subset$ est l'inclusion au sens large.

Si X est une partie d'un groupe G, Inv(X) est l'ensemble des involutions de G qui appartiennent à X, et si t est une involution de G, J(X,t) est l'ensemble des éléments x de X tels que $x^t = x^{-1}$.

Si q est une puissance de 2, $\mathbb{F}_q$ est le corps à q éléments. Le groupe PSL(2,q) est défini dans Huppert, § 6 du chapitre II. Le groupe PSU(3,q) est le groupe qui est noté $PSU(3,q^2)$ dans Huppert, § 10 du chapitre II. Le groupe Sz(q) est le groupe de Suzuki défini sur $\mathbb{F}_q$. Pour une définition de ce groupe, voir par exemple R. CARTER : Simple groups of Lie type, Wiley & Sons, 1972 chapitre 13, ou l'exposé de Y. Auffray cité plus haut.

Les autres notations utilisées sont maintenant traditionnelles en théorie des groupes finis.

CHAPITRE I. LE THÉORÈME DE DOUBLE TRANSITIVITÉ

§ 1.- GÉNÉRALITES SUR LES GROUPES DE BENDER

(1) Définition.- Soit p un nombre premier. Un sous-groupe H d'un groupe fini G est appelé groupe de Bender pour p de G si l'ordre de H est divisible par p, et pour tout $x \in G - H$, l'ordre de $H \cap H^x$ est premier à p.

Soient G un groupe fini et H un groupe de Bender de G, p étant un nombre premier fixé.

(2) Si X est un sous-groupe de H d'ordre divisible par p, on a $N_G(X) \subset H$. Si x est un élément de H d'ordre divisible par p, on a $C_G(x) \subset H$.

(3) Tout p-Sylow de H est un p-Sylow de G.

(4) On a $N_G(H) = H$; l'opération de G sur l'ensemble des classes à droite de H dans G est donc équivalente à l'opération de G sur l'ensemble des conjugués de H (par automorphismes intérieurs).

Soient G un groupe fini et p un nombre premier divisant $|G|$.

(5) Soit P un p-Sylow de G. Posons $B(G,P) = < N_G(Q) \mid 1 \neq Q \subset P >$. Alors un sous-groupe H de G est un groupe de Bender pour p de G si et seulement si H contient un conjugué de B(G,P).

Les deux propriétés suivantes permettent de faire des raisonnements par récurrence sur les groupes ayant un groupe de Bender propre :

(6) Soit H un groupe de Bender pour p de G. Si X est un sous-groupe de G tel que $|X \cap H|$ soit divisible par p, alors $X \cap H$ est un groupe de Bender de X.

(7) Soit H un groupe de Bender pour p de G. a) Si X est un sous-groupe normal de G d'ordre divisible par p, on a $HX = G$. b) Si X est un sous-groupe normal de G tel que $|X|_p < |G|_p$, HX/X est un groupe de Bender de G/X.

(8) Soit G un groupe de p-rang 1. Alors un p-Sylow P de G a un unique sous-groupe Q d'ordre p, et $B(G,P) = N_G(Q)$.

(9) Soit G un groupe de p-rang ≥ 2. Si H est un groupe de Bender de G, on a $O_{p'}(G) \subset H$. Si H est un groupe de Bender propre de G, $O_{p'}(G) = \bigcap_{x \in G} H^x$.

Formulations équivalentes de la définition d'un groupe de Bender.

(10) a) Soit H un groupe de Bender pour p de G, et considérons G comme groupe opérant sur les classes à droite de H dans G. Alors tout élément d'ordre p de G a un point fixe et un seul.

b) Réciproquement, soit G un groupe d'ordre divisible par p qui opère transitivement sur un ensemble E de manière que tout élément d'ordre p de G ait un point fixe et un seul dans E. Alors le stabilisateur d'un point de E dans G est un groupe de Bender de G.

(11) Soit $\mathcal{S}$ l'ensemble des p-Sylow d'un groupe fini G d'ordre divisible par p. Soit R la relation d'équivalence sur $\mathcal{S}$ engendrée par la relation $S \cap S' \neq 1$ entre éléments de $\mathcal{S}$.

a) Si $\mathcal{C}$ est une classe d'équivalence de R et $S \in \mathcal{C}$, on a $B(G,S) = \{x \in G \mid \mathcal{C}^x = \mathcal{C}\}$, et $\mathcal{C}$ est l'ensemble des p-Sylow de B(G,S).

b) Pour que G admette un groupe de Bender propre, il faut et il suffit qu'il existe $\mathcal{S}_1$, $\mathcal{S}_2$ tels que $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, $\mathcal{S}_1 \neq \emptyset$, $\mathcal{S}_2 \neq \emptyset$, $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$ et tels que pour $S_1 \in \mathcal{S}_1$ et $S_2 \in \mathcal{S}_2$ on ait $S_1 \cap S_2 = 1$.

Démonstration des propriétés (2) - (11).

(2) Soit $X \subset H$ tel que $|X|$ soit divisible par p, et $y \in N_G(X)$. Puisque $X \subset H \cap H^y$, on a $y \in H$ par définition. La deuxième assertion en résulte puisque $C_G(x) \subset N_G(\langle x \rangle)$.

(3) Si P est un p-Sylow de H, on a $N_G(P) \subset H$ d'après (2), donc P est un p-Sylow de $N_G(P)$, donc est un p-Sylow de G.

(4) résulte immédiatement de (2).

(5) Soit H un groupe de Bender pour p de G. Soit P_1 un p-Sylow de H. D'après (3), $B(G,P_1)$ est défini et est conjugué à $B(G,P)$ dans G. D'après (2), $B(G,P_1) \subset H$.

Réciproquement, supposons $H \supset B(G,P)$. Alors $|H|$ est divisible par p. Soit $x \in G$ tel que $|H \cap H^x|$ soit divisible par p, et soit Q un p-Sylow de $H \cap H^x$. Montrons que $N_G(Q) \subset H$: il existe un p-Sylow P_1 de H tel que $Q \subset P_1$, et il existe $y \in H$ tel que $P_1 = P^y$. On a $N_G(Q) \subset B(G,P_1) = B(G,P)^y \subset H$, d'où notre assertion. De même $N_G(Q) \subset H^x$, donc $N_G(Q) \subset H \cap H^x$. Donc Q est un p-Sylow de $N_G(Q)$ donc un p-Sylow de G. Puisque Q et $Q^{x^{-1}}$ sont des p-Sylow de H, il existe $z \in H$ tel que $Q^z = Q^{x^{-1}}$. Alors $zx \in N_G(Q) \subset H$, donc $x \in H$ et H est donc bien un groupe de Bender pour p.

(6) résulte immédiatement de la définition.

(7) a) D'après (5), HX est un groupe de Bender de G, et $G \subset HX$ d'après (2).

b) On peut supposer que X est un p'-groupe d'après a). Alors $|HX/X|$ est divisible par p. Soit $\bar{x} \in G/X$ tel que l'ordre de $(HX/X) \cap (HX/X)^{\bar{x}}$ soit divisible par p. Alors $|(HX) \cap (HX)^x|$ est divisible par p, et HX étant un groupe de Bender de G d'après (5), $x \in HX$ donc $\bar{x} \in HX/X$.

(8) Un p-Sylow P de G a un sous-groupe central Q d'ordre p, qui est donc l'unique sous-groupe d'ordre p de P. Si Q_1 est un sous-groupe $\neq 1$ de P, Q_1 a un sous-groupe d'ordre p qui est l'unique sous-groupe Q d'ordre p de Q_1, donc $N(Q_1) \subset N(Q)$. Il en résulte que $B(G,P) = N_G(Q)$.

(9) Soit X un sous-groupe de type (p,p) de H. Comme X opère sur le p'-groupe $O_{p'}(G)$, on sait alors que $O_{p'}(G)$ est engendré par les $C(x) \cap O_{p'}(G)$ pour $x \in X^\#$. Comme $C_G(x) \subset H$ pour $x \in X^\#$ d'après (2), on a donc $O_{p'}(G) \subset H$. Si H est un groupe de Bender propre de G, $\bigcap_{x \in G} H^x$ est par définition un p'-sous-groupe normal de G, donc $O_{p'}(G) = \bigcap_{x \in G} H^x$.

(10) a) D'après (3) et la définition, un élément d'ordre p de G appartient à un unique conjugué de H, donc a un point fixe et un seul. L'assertion b) est évidente.

(11) a) Soit Q un sous-groupe non trivial de S, et $x \in N_G(Q)$. On a $S^x \cap S \neq 1$, donc $S^x \in \mathcal{C}$, d'où $\mathcal{C}^x \cap \mathcal{C} \neq \emptyset$. Il est clair que $\mathcal{C}^x$ est une classe d'équivalence de R, donc $\mathcal{C}^x = \mathcal{C}$. On a donc $B(G,S) \subset \{x \in G \mid \mathcal{C}^x = \mathcal{C}\}$.

Tout p-Sylow de B(G,S) est de la forme S^x, $x \in B(G,S)$. Comme $B(G,S) \subset \{x \in G \mid \mathcal{C}^x = \mathcal{C}\}$, on a $S^x \in \mathcal{C}$, donc l'ensemble des p-Sylow de B(G,S) est est inclus dans $\mathcal{C}$.

Soient S_1 un p-Sylow de B(G,S) et $S_2 \in \mathcal{S}$ tels que $S_1 \cap S_2 \neq 1$. Il existe $x \in G$ tel que $S_2 = S_1^x$, et on a $x \in B(G,S)$ car B(G,S) est un groupe de Bender de G, donc $S_2 \subset B(G,S)$. Il en résulte que l'ensemble des p-Sylow de B(G,S) est égal à $\mathcal{C}$.

Soit enfin $x \in G$ tel que $\mathcal{C}^x = \mathcal{C}$. Alors S^x est un p-Sylow de B(G,S), et il existe $y \in B(G,S)$ tel que $S^{xy} = S$. Alors $xy \in N_G(S) \subset B(G,S)$, donc $x \in B(G,S)$, ce qui prouve que $B(G,S) = \{x \in G \mid \mathcal{C}^x = \mathcal{C}\}$.

b) Soit S un p-Sylow de G. D'après (5), G a un groupe de Bender propre si et seulement si $B(G,S) \neq G$. D'après a) ceci est équivalent à $\mathcal{C} \neq \mathcal{S}$, $\mathcal{C}$ étant la classe d'équivalence de R contenant S.

§ 2.- LES INVOLUTIONS D'UN GROUPE ADMETTANT UN GROUPE DE BENDER PROPRE

Dans toute la suite, on appellera groupe de Bender d'un groupe fini un groupe de Bender pour le nombre premier 2. Dans les 3 premiers chapitres, on fera l'hypothèse :

(AO) *G est un groupe fini qui a un groupe de Bender propre.*

Notations.- Ω est une classe de conjugaison de groupes de Bender propres de G. On considère G comme groupe opérant (à droite) sur Ω par automorphismes intérieurs. Toute involution de G a alors un unique point fixe. Si u est une involution de G, on notera H(u) le point fixe de u. Pour toute partie E d'un groupe, on notera Inv(E) l'ensemble des involutions contenues dans E.

On pose $\mathcal{D} = \{H \cap H' \mid H \in \Omega, H' \in \Omega, H \neq H'\}$ et $n = |\mathrm{Inv}(H)|$ pour $H \in \Omega$: n est indépendant de H. Si X est un groupe fini, $Y \subset X$ et $u \in \mathrm{Inv}(X)$ on posera $J(Y,u) = \{y \in Y \mid y^u = y^{-1}\}$.

Proposition 1.- a) *Soient* $s,t \in \mathrm{Inv}(G)$ *tels que* $H(s) \neq H(t)$. *Alors* st *est d'ordre impair. Il existe une unique involution* u *de* G *telle que* $t = s^u$. *On a* $u \in \langle s,t \rangle$, $H(u) \neq H(s)$ *et* $H(u) \neq H(t)$.

b) $\mathrm{Inv}(G)$ *est une classe de conjugaison de* G. *Si* $H \in \Omega$, $\mathrm{Inv}(H)$ *est une classe de conjugaison de* H.

c) *Si* H, $H' \in \Omega$, *le nombre des involutions* u *telles que* $H^u = H'$ *est* n.

a) Soient $s,t \in \mathrm{Inv}(G)$ tels que $H(s) \neq H(t)$. Supposons que st soit d'ordre pair. Comme s et t inversent tout élément de $\langle st \rangle$, $\langle st \rangle$ a une involution u qui est centralisée par s et par t. Alors, d'après le § 1 (2), on a $H(s) = H(u) = H(t)$, ce qui est contraire à l'hypothèse. Donc st est d'ordre impair. D'après le théorème de Sylow, il existe $u \in \langle s,t \rangle$ tel que $s^u = t$. Si u n'est pas une involution, su est une involution car dans le groupe diédral $\langle s,t \rangle$, les éléments de $\langle s,t \rangle - \langle st \rangle$ sont des involutions. Donc en remplaçant éventuellement u par su, on peut supposer que u est une involution. Si $H(u) = H(s)$, on a $s^u \in H(s)$, d'où $H(t) = H(s)$, ce qui est contraire à l'hypothèse. Donc $H(u) \neq H(s)$. De même, puisque $t^u = s$, $H(u) \neq H(t)$. L'application : $u \mapsto s^u$ de $\mathrm{Inv}(G) - \mathrm{Inv}(H(s))$ dans lui-même est donc surjective, donc bijective.

b) Soit $H \in \Omega$. Comme $H \neq G$ et $N(H) = H$, on a $|\Omega| \geq 2$. Soit $H' \in \Omega$, $H' \neq H$. Alors $\mathrm{Inv}(H') \neq \emptyset$ et $\mathrm{Inv}(H') \cap \mathrm{Inv}(H) = \emptyset$ par définition. Donc $\mathrm{Inv}(G) - \mathrm{Inv}(H) \neq \emptyset$. D'après a) tout élément de $\mathrm{Inv}(H)$ est conjugué à tout élément de $\mathrm{Inv}(G) - \mathrm{Inv}(H)$. Il en résulte que $\mathrm{Inv}(G)$ est une classe de conjugaison de G. Soient $s,t \in \mathrm{Inv}(H)$. Si $x \in G$ est tel que $s^x = t$, on a $t \in H \cap H^x$, d'où $x \in H$, ce qui prouve que $\mathrm{Inv}(H)$ est une classe de conjugaison de H.

c) Si $H' = H$, $H^u = H'$ équivaut à $u \in H$. Supposons $H' \neq H$: soit $s \in \mathrm{Inv}(H)$. Si $u \in \mathrm{Inv}(G)$, on a $H^u = H' \iff s^u \in H' \iff s^u \in \mathrm{Inv}(H')$. Comme l'application $u \longmapsto s^u$ est une bijection de $\mathrm{Inv}(G) - \mathrm{Inv}(H)$ sur lui-même, le nombre des u tels que $s^u \in \mathrm{Inv}(H')$ est $|\mathrm{Inv}(H')| = n$.

Remarque.- Si les involutions de H commutent deux à deux (ce qui sera le cas si $O_{2'}(G) = 1$), le produit de deux involutions de G est soit d'ordre 2, soit d'ordre impair. Les groupes engendrés par une classe d'involutions possédant cette propriété ont été étudiés par Fischer et par Aschbacher. (Le théorème de Bender-Suzuki est utilisé dans le travail d'Aschbacher).

Lemme 1.- *Soit* X *un sous-groupe d'ordre impair de* $H \in \Omega$, *et soient* $u \in \mathrm{Inv}(H)$ *et* $t \in \mathrm{Inv}(G-H)$. *Alors on a* $|u^X| \geq |J(X,t)|$.

Il suffit de montrer que l'application : $x \longmapsto u^x$ de $J(X,t)$ dans u^X est injective. Si $u^x = u^y$ $(x,y \in J(X,t))$, on a $u^{xt} = u^{yt}$; xt et yt sont des involutions et $H(u) \neq H(u^{xt})$, sinon $xt \in H$ et $t \in H$, contrairement à l'hypothèse. D'après la proposition 1 a), on a $xt = yt$, d'où $x = y$.

Proposition 2.- *Soit* $D \in \mathcal{D}$. *a) Il existe* $H \in \Omega$ *et* $t \in \mathrm{Inv}(G-H)$ *tels que* $D = H \cap H^t$.

b) Soient H,t *comme dans a), et* $K = J(D,t)$. *Si* $u \in \mathrm{Inv}(H)$, *on a* $|u^D| = |t^D| = |K| = n$; D *opère transitivement sur* $\mathrm{Inv}(Ht)$ *et sur* $\mathrm{Inv}(H)$.

On a $D = H \cap H'$, $H,H' \in \Omega$, $H' \neq H$. D'après la prop. 1 c), il existe $t \in \mathrm{Inv}(G-H)$ tel que $H' = H^t$. Puisque D normalise H et H^t, D normalise l'ensemble $\mathrm{Inv}(Ht)$ des involutions qui transforment H en H^t. On a $J(H,t) \subset H \cap H^t = D$, donc $J(H,t) = K$. D'après l'appendice I, (1), on a $|t^D| = |K| = |J(H,t)| = |\mathrm{Inv}(Ht)|$, la dernière égalité provenant de ce que $u \longmapsto ut$ est une bijection de $\mathrm{Inv}(Ht)$ sur $J(H,t)$. Donc D opère transitivement sur $\mathrm{Inv}(Ht)$. De plus, d'après la prop. 1 c), $|\mathrm{Inv}(Ht)| = n$. D'après le lemme 1, on a $|u^D| \geq |K| = n$, donc $|u^D| = n$ et D opère transitivement sur $\mathrm{Inv}(H)$.

Lemme 2.- *Soient* H_1, H_2 *des éléments distincts de* Ω . *Soit* F *un sous-groupe de* G *tel que* $|F \cap H_1|$ *et* $|F \cap H_2|$ *soient pairs. Alors il existe* $t \in \mathrm{Inv}(F)$ *tel que* $H_2 = H_1^t$ *et* $F \cap H_1$ *et* $F \cap H_2$ *sont des groupes de Bender propres et distincts de* F, *conjugués dans* F.

Soient $u_1 \in \mathrm{Inv}(F \cap H_1)$ et $u_2 \in \mathrm{Inv}(F \cap H_2)$. Puisque $|H_1 \cap H_2|$ est impair, on a $u_2 \notin F \cap H_1$. En particulier, $F \cap H_1 \neq F \cap H_2$ et $F \cap H_1$ est un groupe de Bender propre de F (§ 1). D'après la prop. 1, il existe $t \in \mathrm{Inv}(F)$ tel que $u_1^t = u_2$. Alors $H_2 = H_1^t$ et $(F \cap H_2) = (F \cap H_1)^t$.

§ 3.- LES p-SOUS-GROUPES MAXIMAUX FIXANT 3 POINTS

Dans ce paragraphe et le suivant, p est un nombre premier fixé, $p > 2$.

Nous démontrons dans le § 4 que si G a un p-sous-groupe P tel que $|\Omega_P| = 2$, alors G est 2-transitif sur Ω. Pour cela, on prendra une partie $\{H,H'\}$ de cardinal 2 de Ω, et il suffira d'après l'appendice II, (4), de montrer que si Q est un p-Sylow de $H \cap H'$, alors $|\Omega_Q| = 2$. En supposant que $|\Omega_Q| \geq 3$, on pourra considérer un p-sous-groupe R de G tel que $Q \subset R$ et $|\Omega_R| \geq 3$, maximal pour ces propriétés. C'est pourquoi on étudie les p-sous-groupes maximaux de G qui fixent 3 points.

L'étude des p-sous-groupes P tels que $|\Omega_P| \geq 3$ est liée à l'étude des p-sous-groupes P tels qu'il existe $H \in \Omega_P$ tel que $|N_H(P)|$ soit pair. Si P vérifie cette dernière condition et si $|\Omega_P| \geq 2$, on a $|\Omega_P| \geq 3$ car si $H' \in \Omega_P$ est distinct de H et $t \in \mathrm{Inv}(N_H(P))$, on voit que $(H')^t$ est un élément de Ω_P distinct de H et de H'.

On démontrera dans la suite que si P est maximal parmi les p-sous-groupes de G qui fixent 3 points et si $H \in \Omega_P$, alors $|N_H(P)|$ est pair.

Proposition 1.- Soit P un élément maximal de l'ensemble des p-sous-groupes de G qui ont au moins 3 points fixes. Alors il existe $H \in \Omega$ tel que $P \subset H$ et tel que $|N_H(P)|$ soit pair.

Lemme 1.- Soit $D = H_1 \cap H_2$ $(H_1, H_2 \in \Omega,\ H_1 \neq H_2)$. Tout p-Sylow de D est normalisé par une involution de G qui échange H_1 et H_2.

D'après le § 2, prop. 2, il existe $t \in \mathrm{Inv}(G - H_1)$ tel que $H_2 = H_1^t$, et t normalise D. Comme $|D|$ est impair, t normalise un p-Sylow de D. D'après un théorème de Sylow, tout p-Sylow de D est normalisé par un conjugué u de t par un élément de D, et u échange H_1 et H_2.

Lemme 2.- Soit X un sous-groupe d'ordre impair de G tel que $N_G(X)$ soit de 2-rang ≥ 2. Alors $X \subset H(t)$ pour tout $t \in \mathrm{Inv}(N_G(X))$.

En effet, si $t \in \mathrm{Inv}(N_G(X))$, $H(t) \cap N_G(X)$ est un groupe de Bender de $N_G(X)$, et le lemme résulte du § 1, (9).

Lemme 3.- Soit P maximal parmi les p-sous-groupes de G qui ont au moins

3 points fixes, et $M = N_G(P)$. *Soient* H_1, H_2 *des éléments distincts de* Ω_P *tels qu'il existe* $x \in M$ *avec* $H_1^x = H_2$. *Alors il existe une involution de* M *qui échange* H_1 *et* H_2.

Si P est un p-Sylow de $H_1 \cap H_2$, il suffit d'appliquer le lemme 1. Sinon, d'après la maximalité de P, un p-Sylow de $M \cap H_1 \cap H_2$ n'a que 2 points fixes. D'après l'appendice II, (2), il existe $x \in M$ qui échange H_1 et H_2. Alors x est d'ordre pair, et il existe un entier k tel que x^k soit une involution. Comme une involution n'a qu'un point fixe, x^k ne peut fixer H_1 et H_2, donc les échange.

Démonstration de la proposition.- Posons $M = N_G(P)$. D'après le lemme 2, il suffit de considérer le cas où M est de 2-rang ≤ 1.

1er cas : les orbites de M dans Ω_P sont toutes de cardinal ≤ 2.

En particulier, M n'est pas transitif sur Ω_P. Soient $H_1, H_2 \in \Omega_P$ qui ne soient pas dans la même orbite sous M. D'après le lemme 1, P n'est pas un p-Sylow de $M \cap H_1 \cap H_2$. Donc un p-Sylow Q de $M \cap H_1 \cap H_2$ n'a que les deux points fixes H_1, H_2. Puisque $|\Omega_P| \geq 3$, il existe $H_3 \in \Omega_P$ distinct de H_1, H_2. Alors H_3 n'est pas un point fixe de Q, donc l'orbite de H_3 par Q est d'ordre $\geq p > 2$. Ce cas est donc impossible.

2ème cas : il existe une orbite de M dans Ω_P de cardinal ≥ 3.

Soient H_o, H_1, H_2 des éléments distincts de Ω_P qui sont dans la même orbite sous M. D'après le lemme 3, il existe des involutions t_1, t_2, t de M telles que $H_o^{t_1} = H_1$, $H_o^{t_2} = H_2$, $H_o^{t_1 t_2} = H_o^t$. En particulier, $|M|$ est pair donc M est de 2-rang 1. D'après le théorème de Brauer-Suzuki, $M/O_{2'}(M)$ a une seule involution, donc $t_1 t_2 \in O_{2'}(M)$. Alors $t_1 t_2 t \in H_o$ et l'image de $t_1 t_2 t$ dans $M/O_{2'}(M)$ est d'ordre 2, donc $t_1 t_2 t$ est d'ordre pair. Il en résulte que $|N_{H_o}(P)|$ est pair.

§ 4.- LES INTERSECTIONS p-RÉGULIÈRES

Lemme 1.- Soient $D \in \mathcal{D}$ *et* $H \in \Omega$ *tels qu'il existe* $H' \in \Omega$ *tel que* $D = H \cap H'$. *Les conditions suivantes sont équivalentes :*

a) il existe $u \in \mathrm{Inv}(H)$ *tel que* $|D \cap D^u|_p = |D|_p$.

b) *pour tout* $u \in \mathrm{Inv}(H)$, *on a* $|D \cap D^u|_p = |D|_p$.

c) *il existe un* p-*Sylow* P *de* D *tel que* $|N_H(P)|$ *soit pair.*

d) *pour tout* p-*Sylow* P *de* D, $|N_H(P)|$ *est pair.*

e) *il existe* $u \in \mathrm{Inv}(H)$ *et un* p-*sous-groupe* P *de* D *normalisé par* u *tel que* $|u^P| \geq n_p$.

Supposons ces conditions satisfaites. Si P *est* p-*Sylow de* D, *on a* $|\Omega_p| \geq 3$ *et si* u *est une involution de* H *qui normalise* P, *on a* $|u^P| = n_p$.

Si les conditions de ce lemme sont satisfaites, on dira que D est une intersection p-régulière relativement à H, et on écrira $(D,H) \in \mathscr{R}_p$.

D'après le § 2, si $u \in \mathrm{Inv}(H)$, on a $|u^D| = n$. D'après l'appendice I,(3), on a donc a) <==> c) <==> e). On a a) <==> b) car D est transitif sur Inv(H) et c) <==> d) car deux p-Sylow de D sont conjugués dans D. Si P est un p-Sylow de D et si ces conditions sont satisfaites, $|N_H(P)|$ est pair. On a alors $|\Omega P| \geq 3$ comme on l'a remarqué au § 3. Si $u \in \mathrm{Inv}(H)$ normalise P, on a $|u^P| = |u^D|_p = n_p$ d'après l'appendice I,(3)b).

Lemme 2.- *Soit* P *un élément maximal de l'ensemble des* p-*sous-groupes de* G *qui ont au moins 3 points fixes. Supposons que* P *contienne un* p-*Sylow d'un élément de* $\mathscr{D}$. *Alors si* H, H' *sont des éléments distincts de* Ω_p, $(H \cap H', H) \in \mathscr{R}_p$ *et* P *est un* p-*Sylow de* $H \cap H'$.

1) Supposons d'abord que $|N_H(P)|$ soit pair :

D'après l'hypothèse et le § 3, lemme 1, il existe $H_o \in \Omega$, $t \in \mathrm{Inv}(G - H_o)$ et un p-Sylow P_o de $H_o \cap H_o^t$ tels que $P_o^t = P_o$ et $P_o \subset P$. On a $|t^{P_o}| = n_p$ d'après l'appendice I,(3)b) et le § 2, prop. 2. D'après l'appendice I,(1), on a $|t^{P_o}| = |J(P_o,t)|$. Comme $P \supset P_o$, on a donc $|J(P,t)| \geq |J(P_o,t)| = n_p$.

1er cas : $t \notin H$. Soit $u \in \mathrm{Inv}(H)$ tel que $P^u = P$. D'après le § 2, lemme 1, on a $|u^P| \geq |J(P,t)|$, donc d'après ce qu'on vient de voir, $|u^P| \geq n_p$. D'après le lemme 1 e), il en résulte que $(H \cap H', H) \in \mathscr{R}_p$. D'après le lemme 1 et la maximalité de P, P est un p-Sylow de $H \cap H'$.

2ème cas : $t \in H$. On a $|t^{P_o}| = n_p$. En appliquant le lemme 1 e) avec t à la place de u et P_o à la place de P, on voit que $(H \cap H', H) \in \mathscr{R}_p$. On conclut comme dans le 1er cas.

2) Conclusion : D'après le § 3, il existe $H \in \Omega_p$ tel que $|N_H(P)|$ soit pair. D'après 1), pour tout $H' \in \Omega_p$ distinct de H, P est un p-Sylow de $H \cap H'$. D'après le § 3, lemme 1, il existe une involution de $N_G(P)$ qui échange H et H', donc $|N_{H'}(P)|$ est pair. On peut alors appliquer 1) à H, $H' \in \Omega_p$ distincts quelconques, d'où le lemme.

Proposition 1.- *a) Si* $\mathcal{R}_p = \emptyset$, G *opère de manière doublement transitive sur* Ω.

b) $\mathcal{R}_p = \emptyset$ *si et seulement s'il existe un* p*-sous-groupe* P *de* G *tel que* $|\Omega_P| = 2$.

Supposons $\mathcal{R}_p = \emptyset$. Soit $\{H,H'\}$ une partie de cardinal 2 de Ω, et P un p-Sylow de $H \cap H'$. Si $|\Omega_P| \geq 3$, le lemme 2 montre que $\mathcal{R}_p \neq \emptyset$, contrairement à l'hypothèse. Donc $\Omega_P = \{H,H'\}$ et G opère de manière doublement transitive d'après l'appendice II, (4).

Supposons $\mathcal{R}_p \neq \emptyset$. Si $(D_o,H_o) \in \mathcal{R}_p$ et Q_o est un p-Sylow de D_o, on a $|\Omega_{Q_o}| \geq 3$. D'après le lemme 2, il existe un p-sous-groupe Q de G tel que $|\Omega_Q| \geq 3$ et que pour tout $D \in \mathcal{D}$ avec $Q \subset D$, Q soit un p-Sylow de D. Soit S un p-Sylow de G tel que $Q \subset S$. Soient H, H' des éléments distincts de Ω_S. On a $Q \subset H \cap H'$ donc Q est un p-Sylow de $H \cap H'$, donc $Q = S$ et $|\Omega_S| \geq 3$. D'après le théorème de Sylow, on a donc $|\Omega_S| \neq 2$ pour tout p-Sylow S de G, et d'après l'appendice II, (1), $|\Omega_P| \neq 2$ pour tout p-sous-groupe P de G.

Proposition 2.- *Soient* $H \in \Omega$ *et* P *un élément maximal de l'ensemble des* p*-sous-groupes de* H *qui ont au moins 3 points fixes. Alors* P *est maximal parmi les* p*-sous-groupes de* G *qui ont au moins 3 points fixes et* $|N_H(P)|$ *est pair.*

1er cas : $\mathcal{R}_p = \emptyset$. Alors G est 2-transitif sur Ω d'après la prop. 1, donc P est maximal parmi les p-sous-groupes de G qui ont 3 points fixes et $N_G(P)$ est transitif sur Ω_P (appendice II, (6)). D'après le § 3, il existe $K \in \Omega_P$ tel que $|N_K(P)|$ soit pair, et d'après la transitivité de $N_G(P)$ il en résulte que $|N_H(P)|$ est pair.

2ème cas : $\mathcal{R}_p \neq \emptyset$. Soit R maximal parmi les p-sous-groupes de G qui contiennent P et fixent 3 points. Soit $K \in \Omega_R$ tel que $K \neq H$. On a $P \subset H \cap K$ et un p-Sylow de $H \cap K$ a 3 points fixes d'après la prop. 1. Donc P est un p-Sylow de $H \cap K$, et il existe $u \in N(P)$ qui échange H et K (§ 3, lemme 1). Alors $P \subset R^u \subset H$, donc

$P = R^u$ et $P = R$. De plus, P étant un p-Sylow de $H \cap K$, $|N_H(P)|$ est pair d'après le lemme 2.

Pour utiliser l'hypothèse de récurrence, nous aurons besoin du lemme suivant :

Lemme 3.- Supposons que G soit 2-transitif sur Ω. Soient $H, H' \in \Omega$ distincts, $D = H \cap H'$ et P un p-Sylow de D. Supposons que $|N_H(P)|$ soit impair. Alors $|\Omega_P| = 2$ et P est un p-Sylow de G.

Si $|\Omega_P| \geq 3$, P est maximal parmi les p-sous-groupes de G qui ont 3 points fixes, car $|D_1| = |D|$ pour tout $D_1 \in \mathcal{D}$ d'après la 2-transitivité de G. D'après la prop. 2, $|N_H(P)|$ est alors pair, contrairement à l'hypothèse. Donc $|\Omega_P| = 2$. D'après l'appendice II,(1), P est alors un p-Sylow de G.

§ 5.- LE THÉORÈME A. UTILISATION DE L'HYPOTHÈSE DE RÉCURRENCE

On commence ici la démonstration, par récurrence sur $|G|$ du théorème de double transitivité :

Théorème A.- Si G est de 2-rang ≥ 2, alors G opère de manière doublement transitive sur Ω.

On supposera dans la suite que :

(A1) G est de 2-rang ≥ 2.

(A2) Pour tout groupe F d'ordre $< |G|$, qui est de 2-rang ≥ 2 et qui a un groupe de Bender propre K, l'opération de F sur les conjugués de K est 2-transitive.

Dans ce paragraphe, on fixe $D \in \mathcal{D}$, $H \in \Omega$ et $t \in \mathrm{Inv}(G)$ tels que $D = H \cap H^t$.

Lemme 1.- a) $|N_H(D)|$ est impair.

b) il existe un nombre premier $p > 2$ tel que $(D,H) \notin \mathcal{R}_p$.

a) Soit u une involution de $N_H(D)$. Puisque D opère transitivement sur Inv(H) (§ 2), on a $\mathrm{Inv}(H) \subset \langle D, u \rangle$. Mais $\langle D, u \rangle = D \langle u \rangle$ est de 2-rang 1. Donc H n'a pas de sous-groupe de type (2,2) et puisque H contient un 2-Sylow de G, cela contredit (A1).

b) Supposons $(D,H) \in \mathscr{R}_p$ pour tout nombre premier $p > 2$. Soit $u \in \mathrm{Inv}(H)$. Four tout p premier, il existe un p-Sylow de D normalisé par u (§ 4, lemme 1). Puisque D est engendré par ces p-Sylow, u normalise D, ce qui contredit a).

Proposition 1.- Si D a un sous-groupe normal $A \neq 1$ qui est normalisé par t et par une involution de H, alors G opère de manière 2-transitive sur Ω.

Soit $N = N_G(A)$. Montrons qu'on peut appliquer l'hypothèse (A2) à $F = N/A$. On a $|F| < |G|$; on a $t \in N - (N \cap H)$, donc $N \cap H$ est un groupe de Bender propre de N et $(N \cap H)/A$ est un groupe de Bender propre de F (voir § 1) ; puisque $D \subset N$, $N \cap \mathrm{Inv}(H) \neq \emptyset$ et D opère transitivement sur Inv(H), on $\mathrm{Inv}(H) \subset N$; il en résulte que N et F sont de 2-rang ≥ 2.

D'après (A2), N opère de manière 2-transitive sur les conjugués de $N \cap H$ dans N.

Soit p un nombre premier > 2, tel que $(D,H) \notin \mathscr{R}_p$ (lemme 1), et soit P un p-Sylow de D. Par définition de $\mathscr{R}_p$, $|N_H(P)|$ est impair, donc (§ 4, lemme 3) P est un p-Sylow de N.

Si $|\Omega_p| = 2$, la conclusion résulte du §4 , prop. 1. Supposons donc que $|\Omega_p| \geq 3$. Soit S maximal parmi les p-sous-groupes de H contenant P, qui fixent 3 points. Puisque P est un Sylow de N, on a $S \cap N = P$. D'après le § 4, prop.2, il existe une involution u dans $N_H(S)$. Comme $\mathrm{Inv}(H) \subset N$, u normalise S et N, donc normalise $P = S \cap N$. Ainsi $|N_H(P)|$ est pair, contrairement à l'hypothèse.

Remarque : La proposition 1 est le seul endroit de la démonstration du théorème A où on utilise l'hypothèse de récurrence.

§ 6.- DÉMONSTRATION DU THÉORÈME DE DOUBLE TRANSITIVITÉ

Dans les propositions 1 et 2 qui suivent, p est encore un nombre premier impair quelconque. Dans la prop. 1, on montre que sous certaines conditions, un élément D de $\mathscr{D}$ a un sous-groupe caractéristique $\neq 1$ normalisé par une involution de H ($D = H \cap H'$, $H, H' \in \Omega$), ce qui permet d'appliquer la proposition du § 5. La démonstration utilise les théorèmes de Feit-Thompson et de Glauberman.

Lemme 1.- Soit X un p'-sous-groupe d'un groupe résoluble fini M . Si X est normalisé par un p-Sylow de M, alors $X \subset O_{p'}(M)$.

Supposons d'abord que $O_{p'}(M) = 1$. Par hypothèse, X est normalisé par $O_p(M)$ donc $[X,O_p(M)] \subset X \cap O_p(M) = 1$. Mais $C_M(O_p(M)) \subset O_p(M)$ (Huppert, chap. VI, (6.5)). Donc $X \subset O_p(M)$, d'où X =1. Dans le cas général, on a $XO_{p'}(M)/O_{p'}(M) = 1$ d'après le premier cas, donc $X \subset O_{p'}(M)$.

Ce lemme sera généralisé dans l'appendice IV.

Proposition 1.- Soient $(D,H) \in \mathcal{R}_p$ *et* $u \in \mathrm{Inv}(H)$. *On a* $O_{p'}(D \cap D^u) \subset O_{p'}(D)$. *Si* $O_{p'}(D \cap D^u) = O_{p'}(D)$, *alors* G *opère de manière doublement transitive sur* Ω.

Soit P un p-Sylow de D normalisé par u (§ 4, lemme 1). Comme $P \subset D \cap D^u$, $O_{p'}(D \cap D^u)$ est normalisé par P, et $O_{p'}(D \cap D^u) \subset O_{p'}(D)$ d'après le lemme 1 et le théorème de Feit-Thompson. Supposons que $O_{p'}(D \cap D^u) = O_{p'}(D)$. Soit A(P) le sous-groupe de P donné par le théorème ZJ de Glauberman. Montrons que $A = O_{p'}(D)A(P)$ vérifie les hypothèses de la proposition du § 5 :

. On a $A \neq 1$. En effet $D \neq 1$ d'après (A1), donc si $O_{p'}(D) = 1$, on a $P \neq 1$ d'où $A(P) \neq 1$.

. L'involution u normalise $O_{p'}(D) = O_{p'}(D \cap D^u)$ et P, donc A(P), donc u normalise A.

. On a $A \lhd D < t >$. Cela résulte du théorème ZJ de Glauberman, car $|D|$ étant impair, D est résoluble et n'a pas de section isomorphe à SL(2,p).

D'après la proposition du § 5, G opère de manière 2-transitive sur Ω.

Lemme 2.- Soient X *un groupe d'ordre impair,* $< u >$ *un groupe d'ordre 2 opérant sur* X, $M = X < u >$. *On suppose que* M *opère sur un groupe fini* Y *d'ordre premier à* $|M|$. *Alors* Y *est engendré par la réunion des sous-groupes* $C_Y(J(X,u))$ *et* $C_Y(v)$ *pour* $v \in \mathrm{Inv}(M)$.

Puisque $|Y|$ est impair, Y est résoluble. On raisonne par récurrence sur la longueur de la suite dérivée de Y. Si cette longueur est 0, Y=1. Sinon $Y_1 = [Y,Y]$ vérifie encore l'hypothèse et a une suite dérivée plus courte. Par hypothèse de récurrence, $Y_1 \subset Z$, où Z est le sous-groupe de Y engendré par $C_Y(J(X,u))$ et les $C_Y(v)$ pour $v \in \mathrm{Inv}(M)$. Il en résulte que $Z \lhd Y$. Puisque $< J(X,u) > \lhd X$ (appendice I,(4)) et Inv(M) est normal dans M, M opère sur Z donc sur Y/Z. Puisque $|Y|$ et $|M|$ sont premiers entre eux, on a

$C_{Y/Z}(\langle J(X,u)\rangle) = C_{Y/Z}(v) = Z/Z$ pour tout $v \in \mathrm{Inv}(M)$ [Huppert, Ch. I, théorème 18-6]. Il en résulte (appendice I,(1)) que tout $v \in \mathrm{Inv}(M)$ inverse les éléments de Y/Z. Si $x \in J(X,u)$, $x = (xu).u$ est le produit de deux involutions de M, donc centralise Y/Z. Donc $C_{Y/Z}(\langle J(X,u)\rangle) = Y/Z$ et $Y = Z$.

Proposition 2.- Soient P un élément maximal de l'ensemble des p-sous-groupes de G qui ont au moins 3 points fixes, $H \in \Omega_P$, u une involution de H qui normalise P mais ne le centralise pas et $K = J(P,u)$. Il existe alors un sous-groupe F de G tel que :

a) $F \cap H$ est un groupe de Bender propre de F

b) Si $s \in \mathrm{Inv}(F)$, alors $K \subset H(s)$ et $O_{p'}(H \cap H^s) \subset O_{p'}(H(s) \cap H \cap H^s)$.

1) Soient $H_1, H_2 \in \Omega$ tels que $K \subset H_1 \cap H_2$, et $s \in \mathrm{Inv}(H_1)$ tel que $K^s = K$. Supposons que $C_G(K) \cap H_2 \cap H_2^s \subset H_1$. Alors $O_{p'}(H_2 \cap H_2^s) \subset O_{p'}(H_1 \cap H_2 \cap H_2^s)$:

On peut appliquer le lemme 2 avec $Y = O_{p'}(H_2 \cap H_2^s)$, $X = \langle K\rangle$ et $M = X.\langle s\rangle$ (M opère bien sur Y car $K \subset H_2 \cap H_2^s$). Donc Y est engendré par $C_Y(K)$ et les $C_Y(v)$ pour $v \in \mathrm{Inv}(M)$. Puisque $M \subset H_1$ et $C_Y(K) \subset H_1$, il en résulte que $Y \subset H_1$. Donc :

$$O_{p'}(H_2 \cap H_2^s) \subset H_1 \cap H_2 \cap H_2^s \subset H_2 \cap H_2^s$$

et par conséquent $O_{p'}(H_2 \cap H_2^s) \subset O_{p'}(H_1 \cap H_2 \cap H_2^s)$.

2) Premier cas : $C_G(K) \not\subset H$. Posons $F_1 = C\langle u\rangle$ avec $C = C_G(K)$, qui est normalisé par u.

. $H \cap F_1$ est un groupe de Bender propre de F_1, car $u \in H \cap F_1$ et $C \not\subset H$.

. $|C|$ est impair : on a $u \notin C$, sinon u centraliserait K, donc P (appendice I, (1)). Or F_1 a une seule classe d'involutions car il a un groupe de Bender propre. Comme $C \lhd F_1$, il en résulte que C n'a pas d'involution.

Donc F_1 est de 2-rang 1. Soit F minimal parmi les sous-groupes de F_1 contenant strictement $H \cap F_1$. Alors $H \cap F = H \cap F_1$ est un groupe de Bender propre de F. Soit $s \in \mathrm{Inv}(F)$. Puisque F_1 a une seule classe d'involutions, s est conjugué à u par un élément de C, donc $K^s = K$ et $K \subset H(s)$.

Puisque $H \cap F$ est un sous-groupe maximal de F, on a d'après l'appendice III,(1) $F \cap H \cap H^s \subset F \cap H(s)$. Mais $F \cap H = F_1 \cap H$, donc $C \cap H \cap H^s \subset H(s)$. D'après 1) il en résulte que :

$$O_{p'}(H \cap H^s) \subset O_{p'}(H(s) \cap H \cap H^s).$$

3) Deuxième cas : $C_G(K) \subset H$. Posons $F = N_G(P)$. Alors $F \cap H$ est un groupe de Bender propre de F d'après la prop. 2 du § 4 et le lemme 2 du § 2. Soit $s \in \mathrm{Inv}(F - F \cap H)$. Alors s est conjugué à u dans $N_G(P)$, donc $P \subset H(s)$. D'après 1), $O_{p'}(H(s) \cap H(s)^u) \subset O_{p'}(H \cap H(s) \cap H(s)^u)$. Mais il existe une involution de G qui échange u et s (§ 2, prop. 1). Donc :

$$O_{p'}(H \cap H^s) \subset O_{p'}(H(s) \cap H \cap H^s).$$

Démontrons maintenant le théorème A. Remarquons que $n = |\mathrm{Inv}(H)| > 1$ d'après (A1) et que n est impair puisque $n = |J(D,t)|$ pour $D = H \cap H^t \in \mathcal{D}$. Soit p un diviseur premier de n. Si $\mathcal{R}_p = \emptyset$, G opère de manière doublement transitive sur Ω (§ 4, prop. 1). On suppose donc :

(A3) p est un diviseur premier de n et $\mathcal{R}_p \neq \emptyset$.

Remarque.- Si G est l'un des groupes qui figurent dans la conclusion du théorème de Bender-Suzuki, l'hypothèse (A3) ne peut être vraie que si $O_{2'}(G) \neq 1$. Nous verrons en effet que si $O_{2'}(G) = 1$ et $K = J(D,t)$ pour $D = H \cap H^t \in \mathcal{D}$, K est un groupe d'ordre n et un élément de $K^\#$ n'a que 2 points fixes.

D'après (A3) et le § 4, lemme 1, il existe P maximal parmi les p-sous-groupes de G ayant au moins 3 points fixes, et tel que P contienne un p-Sylow d'un élément de $\mathcal{D}$. Soient $H \in \Omega_p$ et $u \in \mathrm{Inv}(H)$ tel que $P^u = P$ (§ 4, lemme 2). Soit $K = J(P,u)$. On a $|K| = |u^P| = n_p$ (§ 4, lemmes 1 et 2), donc d'après le choix de p, u ne centralise pas P et on peut appliquer la proposition 2. Soit F le sous-groupe donné par cette proposition, et soit $s \in \mathrm{Inv}(F - F \cap H)$ tel que $O_{p'}(H \cap H(s))$ soit minimal (s existe d'après a) de la prop. 2). Soit $D = H \cap H(s)$.

. $(D,H(s)) \in \mathcal{R}_p$: En effet $|u^{<K>}| = |J(<K>,u)| = |K| = n_p$, donc $(D,H) \in \mathcal{R}_p$ d'après le § 4, lemme 1 e), et on a $(D,H(s)) \in \mathcal{R}_p$ car il existe une involution de G qui échange H et H(s).

. D'après les propositions 1 et 2, on a alors :

$$O_{p'}(H \cap H^s) \subset O_{p'}(D \cap D^s) \subset O_{p'}(D)$$

D'après la minimalité de $O_{p'}(H \cap H(s))$, il en résulte que $O_{p'}(D \cap D^s) = O_{p'}(D)$. D'après la proposition 1, G opère alors de manière doublement transitive sur Ω.

Voici trois conséquences immédiates du théorème A :

Corollaire 1.- *G opère transitivement sur l'ensemble des triplets* (H_1, H_2, u) *où* $H_1, H_2 \in \Omega$, $H_1 \neq H_2$ *et* $u \in \mathrm{Inv}(H_1)$.

Cela résulte de la double transitivité de G et du fait que $H_1 \cap H_2$ opère transitivement sur $\mathrm{Inv}(H_1)$, pour $H_1, H_2 \in \Omega$, $H_1 \neq H_2$ (prop. 2 du § 2).

Corollaire 2.- *G a une seule classe de groupes de Bender propres.*

Soient $H \in \Omega$ et S un 2-Sylow de H. Avec la notation du § 1, $B(G,S) \subset H$. D'après le théorème A, G opère de manière doublement transitive sur les conjugués de B(G,S), donc B(G,S) est un sous-groupe maximal de G. Il en résulte que $H = B(G,S)$.

Corollaire 3.- *Soit* $L = \langle \mathrm{Inv}(G) \rangle$. *Alors* $L \lhd G$, $|G/L|$ *est impair et* $L/O_{2'}(L)$ *est simple.*

Il est clair que $L \lhd G$. Soit $D = H_1 \cap H_2$ ($H_1, H_2 \in \Omega$, $H_1 \neq H_2$). D'après le § 2, lemme 2, $L \cap H_1$ et $L \cap H_2$ sont des groupes de Bender propres de L, conjugués dans L. Mais L est de 2-rang ≥ 2, donc est doublement transitif sur les conjugués de $L \cap H_1$ dans L. Il en résulte que $G = LD$, donc $|G/L|$ est impair. Comme L a une seule classe d'involutions, L n'a pas de sous-groupe normal propre d'ordre pair. Donc $L/O_{2'}(L)$ est simple.

CHAPITRE II.- LES SOUS-GROUPES DE G QUI FIXENT 3 POINTS

§ 1.- ÉNONCÉS DES THÉORÈMES B ET C

Nous commençons ici la démonstration du théorème de Bender-Suzuki, dont l'énoncé est :

Théorème B.- Soit G *un groupe de 2-rang* ≥ 2 *qui a un groupe de Bender propre. Alors il existe un sous-groupe* L *de* G *tel que* $O_{2'}(G) \subset L \lhd G$, $|G/L|$ *est impair, et* $L/O_{2'}(G)$ *est isomorphe à l'un des groupes* PSL(2,q), Sz(q) *ou* PSU(3,q) *où* q *est une puissance de* 2, $q > 2$. *De plus,* G *a une seule classe de groupes de Bender propres.*

Pendant la démonstration du théorème B, on supposera :

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

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

Nous démontrerons dans ce chapitre le théorème suivant :

Théorème C.- Soient H, H' *des éléments distincts de* Ω, *et soit* $u \in \mathrm{Inv}(H)$. *Si* $O_{2'}(G) = 1$, *alors tout sous-groupe de* $H \cap H'$ *qui est normalisé par* u *est centralisé par* u.

Ce théorème permettra, dans la plupart des cas, d'appliquer l'hypothèse de récurrence à $C_G(X)$, si X est un sous-groupe $\neq 1$ de G qui fixe au moins 3 points.

On voit facilement que le théorème C résulte de l'assertion : "Soient $H \in \Omega$ et p un nombre premier. S'il existe un p-sous-groupe de H fixant 2 points et normalisé mais non centralisé par une involution de H, alors $O_{2'}(G) \neq 1$". Nous démontrerons ceci en suivant la même démarche que pour la

démonstration du théorème A : Soient $D \in \mathcal{D}$, u une involution d'un point fixe de D, P un p-Sylow de $D \cap D^u$ normalisé par u. L'analogue du chapitre I, § 4 (cas $\mathcal{R}_p = \emptyset$) sera ici le cas où P n'est pas un p-Sylow de $PC_D(P)$. Dans le cas où P est un p-Sylow de $PC_D(P)$, on prouvera que $O_{p'}(D \cap D^u) \subset O_{p'}(D)$ en utilisant un théorème de Thompson et Bender (appendice IV). On pourra alors conclure comme dans le chapitre I, § 6, que D a un sous-groupe normal $A \neq 1$ normalisé par une involution de H et par une involution n'appartenant pas à H, puis appliquer l'hypothèse de récurrence à $N_G(A)$.

Pour démontrer le théorème C, nous n'aurons pas besoin de toute la force de l'hypothèse (B1), mais seulement de la conséquence suivante :

(B1-a) Soit F un groupe de 2-rang ≥ 2, d'ordre $< |G|$, et H un groupe de Bender propre de F. Alors les involutions de $H/O_{2'}(F)$ commutent deux à deux.

Lemme 1.- Soit $H \in \Omega$. Si les involutions de H commutent deux à deux, alors la conclusion du théorème C est vraie.

En effet, si X est un sous-groupe de $D = H \cap H'$ ($H' \in \Omega$, $H' \neq H$) normalisé mais non centralisé par $u \in \mathrm{Inv}(H)$, il existe $x \in X^{\#}$ tel que $x^u = x^{-1}$ (appendice I, (1)) et les involutions u et ux de H ne commutent pas car u.(ux) est d'ordre impair $\neq 1$.

Remarquons que, réciproquement, on ne peut pas déduire facilement (B1-a) du fait que la conclusion du théorème C est vraie pour $F/O_{2'}(F)$.

§ 2.- LEMMES PRÉLIMINAIRES

Lemme 1.- Soient $D = H \cap H'$ ($H, H' \in \Omega$, $H' \neq H$), $u \in \mathrm{Inv}(H)$, p un nombre premier > 2 et P un p-Sylow de $D \cap D^u$ normalisé par u.

a) G a une seule classe de p-sous-groupes maximaux fixant 3 points et P appartient à cette classe.

b) $N_G(P)$ opère de manière 2-transitive sur Ω_P et si $H_1 \in \Omega_P$, $N_G(P) \cap H_1$ est un groupe de Bender propre de $N_G(P)$.

c) Si $N_G(P)$ est de 2-rang 1, alors P est un p-Sylow de D.

d) Si P n'est pas un p-Sylow de $PC_G(P) \cap D$, alors u centralise P.

a) Soit Q maximal parmi les p-sous-groupes de G qui fixent 3 points. Si $H_1, H_2 \in \Omega_Q$ $(H_1 \neq H_2)$, il existe $v \in \mathrm{Inv}(H_1)$ qui normalise Q (chapitre I, § 4, prop. 2). Alors Q est un p-Sylow de $H_1 \cap H_2 \cap H_2^v$. Mais d'après le corollaire 1 du théorème A (chapitre I, § 6), $D \cap D^u$ est conjugué à $H_1 \cap H_2 \cap H_2^v$ dans G, donc P est conjugué à Q.

b) D'après a) et l'appendice II,(6), $N_G(P)$ opère de manière 2-transitive sur Ω_P. D'après le chapitre I, § 4, prop. 2 et § 2, lemme 2, $N_G(P) \cap H_1$ est un groupe de Bender propre de $N_G(P)$ pour $H_1 \in \Omega_P$.

c) Si $N_G(P)$ est de 2-rang 1, on peut appliquer l'appendice III,(1) d'après b), et on en déduit que $N_G(P) \cap D \subset N_G(P) \cap D \cap D^u$. Donc P est un p-Sylow de $N_D(P)$, donc un p-Sylow de D.

d) Soient H_1, H_2 des éléments distincts de Ω_P. D'après b) P n'est pas un p-Sylow de $PC(P) \cap H_1 \cap H_2$. D'après a) un p-Sylow de $PC(P) \cap H_1 \cap H_2$ n'a que 2 points fixes. D'après l'appendice II,(4), il en résulte que PC(P) opère de manière doublement transitive sur Ω_P. En particulier $|PC(P)|$ est pair, donc $|C(P)|$ est pair. D'après b) $N_G(P)$ n'a qu'une classe d'involutions, donc $u \in C(P)$.

Lemme 2.- Soient $H \in \Omega$, $t \in \mathrm{Inv}(G - H)$, $D = H \cap H^t$. *On suppose que* D *a un sous-groupe normal* $A \neq 1$ *normalisé par* t *et par une involution de* H. *Si les involutions de* H *ne commutent pas toutes deux à deux, alors* $O_{2'}(G) \neq 1$.

Soient $N = N_G(A)$ et $F = N_G(A)/A$. Comme dans le chapitre I, § 5, $N \cap H$ est un groupe de Bender propre de N, $\mathrm{Inv}(H) \subset N$ et l'hypothèse (B1-a) s'applique à F : les involutions de $(N \cap H)/O_{2'}(N)$ commutent deux à deux. Si E désigne le sous-groupe de H engendré par les $[u,v]$ où $u,v \in \mathrm{Inv}(H)$, on a donc $E \subset O_{2'}(N)$. En particulier $E \subset D$. Comme $E \lhd H$ et $E \subset D$, il résulte de la double transitivité de G que $E \subset \bigcap_{x \in G} H^x = O_{2'}(G)$. Donc si $E \neq 1$, alors $O_{2'}(G) \neq 1$.

Pour un p-groupe R, on notera A(R) le sous-groupe caractéristique de R donné par le théorème ZJ de Glauberman.

Lemme 3.- Soit F *un groupe de 2-rang* ≥ 2 *ayant un groupe de Bender propre* H. *On suppose que les involutions de* $H/O_{2'}(F)$ *commutent deux à deux. Soient* $t \in \mathrm{Inv}(F - H)$, $D = H \cap H^t$, p *un nombre premier* > 2 *et* R *un* p*-Sylow de* D. *Si* $O_{p'}(D) = 1$ *et s'il existe un* p*-sous-groupe de* D *normalisé mais non centralisé par une involution de* H, *alors* $\mathrm{Inv}(H) \subset N(A(R))$.

Soit E le sous-groupe de F engendré par Inv(H). Comme D opère sur Inv(H), ED est un groupe avec $E \lhd ED$.

1) $|ED : D|$ est une puissance de 2 :

On a $O_{2'}(F) \subset D$ (chapitre I, § 1) et $|ED : D| = |ED/O_{2'}(F) : D/O_{2'}(F)|$ divise $|EO_{2'}(F)/O_{2'}(F)|$. Mais par hypothèse, $EO_{2'}(F)/O_{2'}(F)$ est abélien élémentaire, donc d'ordre puissance de 2.

2) $O_{p'}(ED) = 1$:

Puisque $O_{p'}(D) = 1$, on a $O_{p'}(ED) \cap D = 1$, donc d'après 1) $|O_{p'}(ED)|$ est une puissance de 2. Donc si $O_{p'}(ED) \neq 1$, $O_{p'}(ED)$ contient une involution de H. Puisque D est transitif sur Inv(H), on a $Inv(H) \subset O_{p'}(ED)$. Mais alors si P est un p-sous-groupe de D normalisé par $u \in Inv(H)$, on a $[u,P] \subset P \cap O_{p'}(ED) = 1$, contrairement à l'hypothèse.

3) ED est résoluble et n'a pas de section isomorphe à SL(2,p) :

En effet, le quotient de 2 termes successifs de la suite :

$$1 \lhd O_{2'}(F) \lhd EO_{2'}(F) \lhd ED$$

est soit d'ordre impair, soit un 2-groupe abélien élémentaire. D'autre part, on sait qu'un 2-Sylow de SL(2,p) n'est pas abélien.

4) Conclusion :

D'après 1), R est un p-Sylow de ED. D'après 2),3) et le théorème ZJ de Glauberman, on a alors $A(R) \lhd ED$, ce qu'il fallait montrer.

§ 3.- DÉMONSTRATION DU THÉORÈME C

Soient $D = H \cap H'$ $(H,H' \in \Omega,\ H \neq H')$ et $u \in Inv(H)$. Pour démontrer le théorème C, il suffit de montrer que si u ne centralise pas $D \cap D^u$, alors $O_{2'}(G) \neq 1$. Si p est un nombre premier, il existe un p-Sylow de $D \cap D^u$ normalisé par u, et $D \cap D^u$ est engendré par ces p-Sylow quand p varie. Si u ne centralise pas $D \cap D^u$, il existe donc un p-Sylow P de $D \cap D^u$ normalisé mais non centralisé par u. On suppose donc :

(C1) p est un nombre premier et P un p-Sylow de $D \cap D^u$ normalisé mais non centralisé par u.

1) On a $O_{p'}(D \cap D^u) = O_{p'}(D)$:

D'après le § 2, lemme 1 d) et (C1), P est un p-Sylow de $PC_D(P)$; P normalise $O_{p'}(D \cap D^u)$ et D est résoluble. D'après le théorème de Thompson et Bender démontré dans l'appendice IV, il en résulte que $O_{p'}(D \cap D^u) \subset O_{p'}(D)$. D'après (C1) et le § 2, lemme 1,a), on peut appliquer la proposition 2 du chapitre I, § 6. On en déduit qu'il existe $s \in \mathrm{Inv}(G - H)$ tel que $O_{p'}(H \cap H^s) \subset O_{p'}(H(s) \cap H \cap H^s)$. D'après le chapitre I, § 6, corollaire 1, $H(s) \cap H \cap H^s$ est conjugué à $D \cap D^u$ dans G et $H \cap H^s$ est conjugué à D. On a donc $|O_{p'}(D)| \leq |O_{p'}(D \cap D^u)|$, d'où $O_{p'}(D \cap D^u) = O_{p'}(D)$.

Soit t une involution de G qui normalise P et telle que $D = H \cap H^t$. L'existence de t résulte du lemme 1 b) du § 2. On désignera par $\mathcal{P}$ l'ensemble des p-groupes Q qui ont les propriétés suivantes :

(P1) $P \subset Q \subset D$

(P2) $Q^t = Q$

(P3) $\mathrm{Inv}(N(P) \cap H) \subset N(A(Q))$.

(On note A(Q) le sous-groupe de Q donné par le théorème ZJ de Glauberman). On a $P \in \mathcal{P}$, de sorte que $\mathcal{P} \neq \emptyset$.

2) Si $O_{p'}(D) = 1$, un élément maximal de $\mathcal{P}$ est un p-Sylow de D :

Si $N_G(P)$ est de 2-rang ≤ 1, cela résulte du § 2, lemme 1 b) et c). On peut donc supposer que $N_G(P)$ est de 2-rang ≥ 2. Soit $Q \in \mathcal{P}$ tel que Q ne soit pas un p-Sylow de D et montrons qu'il existe $R \in \mathcal{P}$ tel que $Q \subsetneq R$.

Posons $F = N_G(A(Q))$. On a $t \in F$ d'après (P2) donc t normalise $F \cap D$. Soit R un p-Sylow de $F \cap D$ normalisé par t et tel que $Q \subset R$. On a $Q \neq R$, sinon comme $N_D(Q) \subset F$, Q serait un p-Sylow de $N_D(Q)$ donc de D.

Les conditions (P1) et (P2) sont bien satisfaites par R. Montrons que F vérifie les hypothèses du lemme 3 du § 2 : d'après (P3) pour Q, $F \cap H$ est de 2-rang ≥ 2 ; puisque $t \in F - F \cap H$, $F \cap H$ est un groupe de Bender propre de F ; d'après (C1), on a $P \neq 1$ donc $Q \neq 1$ et $A(Q) \neq 1$; il résulte alors de (B1-a) que les involutions de $(F \cap H)/O_{2'}(F)$ commutent deux à deux ; enfin on a $P \subset F \cap D$ et P est un p-Sylow de $PC_D(P)$ d'après (C1) et le lemme 1 d) du § 2, donc d'après le théorème de Thompson et Bender (appendice IV), on a $O_{p'}(F \cap D) \subset O_{p'}(D) = 1$. D'après le lemme 3 du § 2, on a donc $\mathrm{Inv}(F \cap H) \subset N(A(R))$, donc d'après (P3) pour Q, $\mathrm{Inv}(N(P) \cap H) \subset N(A(R))$, ce qui prouve (P3) pour R.

3) On a $O_{2'}(G) \neq 1$:

Soit $A = O_{p'}(D)$ si $O_{p'}(D) \neq 1$, et $A = A(Q)$ où Q est un p-Sylow de D tel que $Q \in \mathcal{P}$ si $O_{p'}(D) = 1$. On a alors $A \neq 1$ et A est caractéristique dans D d'après le théorème ZJ de Glauberman. De plus, u normalise A, d'après 1) si $A = O_{p'}(D)$ et d'après (P3) sinon. D'après (C1) et le lemme 1 du § 1, les involutions de H ne commutent pas toutes deux à deux. Les hypothèses du lemme 2 du § 2 sont donc satisfaites, d'où $O_{2'}(G) \neq 1$.

§ 4.- CONSÉQUENCES DU THÉORÈME C ET DE L'HYPOTHÈSE DE RÉCURRENCE

Si $O_{2'}(G) \neq 1$, il est clair, en appliquant (B1) à $F = G/O_{2'}(G)$, que G vérifie la conclusion du théorème B. On supposera désormais :

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

Dans la suite, on suppose fixé un élément H de Ω, $t \in \mathrm{Inv}(G - H)$ et on pose $D = H \cap H^t$, $V = C_D(t)$ et $K = J(D,t)$.

Nous allons démontrer quelques conséquences du théorème C. En particulier nous allons voir que l'hypothèse de récurrence peut s'appliquer dans certains cas à $C_G(X)$, où X est un sous-groupe $\neq 1$ de G qui fixe au moins 3 points.

Proposition 1.- Soit X un sous-groupe de G tel que $|\Omega_X| \geq 3$. a) Si $M \in \Omega_X$, $|C_M(X)|$ est pair.
b) Soit F un groupe tel que $\mathrm{Inv}\, C_G(X) \subset F \subset N_G(X)$. L'application $M \longmapsto F \cap M$ est une bijection de Ω_X sur une classe de groupes de Bender propres de F.

D'après le lemme 2 du chapitre I, § 2, a) implique b). Montrons a) par récurrence sur $|X|$. On peut supposer $X \neq 1$. Comme X est d'ordre impair, X est résoluble et il existe un nombre premier p tel que $Y = O^p(X) \subsetneq X$. Soit P un p-Sylow de X. On a $X = YP$. Posons $F_1 = C_G(Y)P$. Par hypothèse de récurrence $M \longmapsto F_1 \cap M$ est une bijection de Ω_Y sur une classe Ξ de groupes de Bender propres de F_1, et P est un p-sous-groupe de F_1 qui laisse au moins 3 points de Ξ fixes car $\Omega_X \subset \Omega_Y \cap \Omega_P$.

Soit $M \in \Omega_X$ et soit Q un élément maximal de l'ensemble des p-sous-groupes de $F_1 \cap M$ qui ont au moins 3 points fixes dans Ξ et qui contiennent P. D'après le chapitre I, § 4, prop. 2, il existe une involution u dans $N(Q) \cap F_1 \cap M$.

Puisque Q fixe au moins deux points de Ξ, donc au moins 2 points de Ω_Y, le théorème C montre que u centralise Q. Donc u centralise P. Comme $u \in F_1$ et et $|F_1/C_G(Y)|$ est une puissance de p, on a $u \in C_G(Y)$. Il en résulte que $u \in C_M(X)$.

Proposition 2.- *a) Il existe* $u \in \mathrm{Inv}(H)$ *tel que* $V = C_D(u)$.

b) Si X est un sous-groupe de D tel que $|\Omega_X| \geq 3$, *alors X est conjugué dans D à un sous-groupe de V.*

c) Si $x \in K - \{1\}$, *alors* $|\Omega_x| = 2$.

d) Si r est un diviseur premier de $|K|$, *D contient un r-Sylow de G.*

a) Les 3 points H, H^t et H(t) sont fixés par V. D'après la prop. 1, il existe $u \in \mathrm{Inv}(H)$ qui centralise V. On a $V \subset C_D(u)$. Mais d'après le chapitre I, § 2, prop. 2, $|V| = |C_D(u)| = |D|/|\mathrm{Inv}(H)|$. Donc $V = C_D(u)$.

b) D'après la prop. 1, il existe $v \in \mathrm{Inv}(H)$ tel que $X \subset C_D(v)$. Soit $u \in \mathrm{Inv}(H)$ tel que $V = C_D(u)$. Il existe $d \in D$ tel que $u = v^d$ (chapitre I, § 2). Alors $X^d \subset C_D(u) = V$.

c) Si $x \in K$, on a $|\Omega_x| \geq 2$. Supposons $|\Omega_x| \geq 3$. D'après la prop. 1, il existe $v \in \mathrm{Inv}(H)$ tel que $v^x = v$. Mais d'après le chapitre I, § 2, prop. 2, l'application $y \longmapsto v^y$ de K dans Inv(H) est bijective. Donc $x = 1$.

d) Soit R un r-Sylow de D normalisé par t. Si $R \subset V$, r ne divise pas $|K| = |D:V|$, ce qui est contraire à l'hypothèse. Donc $R \cap K \neq 1$. D'après c), $|\Omega_R| = 2$. D'après l'appendice II, (1), R est un r-Sylow de G.

LEMME 1.- *Si X est un sous-groupe de V, on a* $N_K(X) = \langle \mathrm{Inv}\ C_G(X) \rangle \cap K$.

Soit $k \in N_K(X)$. On a $k = t.(tk)$, $t \in \mathrm{Inv}\ C_G(X)$ et tk est une involution de $N_G(X)$. D'après la prop. 1, $N_G(X)$ a une seule classe d'involutions, donc $tk \in \mathrm{Inv}\ C_G(X)$.

Proposition 3.- *Soit X un sous-groupe de V. On suppose que X a un sous-groupe sous-normal* $Y \neq 1$ *tel que* $N_K(Y) \neq 1$. *Soit* $F = O^{2'}(C_G(X))$. *Alors :*

a) F opère de manière doublement transitive sur Ω_X *et* $N_G(X) = FN_V(X)$.

b) $N_H(X) = S \rtimes N_D(X)$ *où S est un 2-Sylow de* $F \cap H$.

Supposons de plus que $N_K(X) \neq 1$. *Alors*

c) $O_{2'}(F) = Z(F)$ *et* $F/Z(F)$ *est isomorphe à l'un des groupes* PSL(2,q), Sz(q), PSU(3,q) , *où* q *est une puissance de* 2, $q \geq 4$.

d) $N_K(X) = C_K(X)$ *est un sous-groupe cyclique d'ordre* $q - 1$.

1) Supposons d'abord que $N_K(X) \neq 1$.

a) Soit $F_1 = \langle \text{Inv } C_G(X) \rangle$. D'après le lemme 1, il existe $k \in F_1 \cap K - \{1\}$. En remplaçant éventuellement k par une de ses puissances, on peut supposer que k est d'ordre premier; il résulte alors de la prop. 1, de la prop. 2 c) et du chapitre I, § 4, prop. 1 que F_1 opère de manière doublement transitive sur Ω_X. Si $g \in N_G(X)$, il existe $f \in F_1$, tel que gf fixe H et H^t. Donc $N_G(X) = F_1 N_D(X)$ et $F_1 = F$. Comme $N_D(X) = N_K(X)N_V(X)$ (appendice I,(1)) et $N_K(X) \subset F$, on a $N_G(X) = FN_V(X)$.

c) Si F est de 2-rang 1, $F \cap D$ a 3 points fixes dans Ω_X d'après l'appendice III, (1), donc $F \cap K = 1$ d'après la prop. 2 c), et $N_K(X) = 1$, contrairement à l'hypothèse. Donc F est de 2-rang ≥ 2. D'après la prop. 1 et (B1), $F/O_{2'}(F)$ est isomorphe à l'un des groupes indiqués. On a $Z(F) \subset O_{2'}(F)$ car Z(F) centralise tout $H' \cap F$ $(H' \in \Omega_X)$, et réciproquement toute involution de F centralise $O_{2'}(F)$ d'après le théorème C, donc $O_{2'}(F) \subset Z(F)$ car $F = F_1 = \langle \text{Inv}(F) \rangle$.

b) Soit S un 2-Sylow de $F \cap H$. D'après la structure des groupes PSL(2,q), Sz(q), PSU(3,q), on a dans $\bar{F} = F/Z(F)$, $\overline{F \cap H} = \bar{S} \rtimes (\overline{F \cap D})$. En particulier $\bar{S} = O_2(\overline{F \cap H})$ est normal dans $N_H(X)/Z(F)$. Donc SZ(F) est normal dans $N_H(X)$ et $S = O_2(SZ(F))$ est normal dans $N_H(X)$. D'après a) on a $N_H(X) = (F \cap H)N_V(X) =$ $= SZ(F)N_D(X) = SN_D(X)$.

d) On a $N_K(X) = F \cap K$ (lemme 1). D'après la structure de $\bar{F} = F/Z(F)$, $J(\overline{F \cap D}, t)$ est un groupe cyclique d'ordre q-1. Si L est son image récirpoque dans F, L est donc un groupe abélien, et on a $C_L(t) = Z(F)$ et $J(L,t) = F \cap K$. Donc $F \cap K$ est un groupe, et $F \cap K \tilde{=} L/Z(F)$ est cyclique d'ordre $q - 1$.

2) Supposons que $N_K(X) = 1$.

En raisonnant par récurrence sur $|X|$, on peut supposer que X a un sous-groupe normal X_o tel que X_o satisfasse a) et b).

Soient $F_o = O^{2'}(C_G(X_o))$, $N_o = N_G(X_o)$, S_o le 2-Sylow de $F_o \cap H$. Par hypothèse on a $X \subset N_o$, N_o opère de manière doublement transitive sur Ω_{X_o}, et S_o est un

complément normal de $D \cap N_o$ dans $H \cap N_o$. De plus $\Omega_X \subset \Omega_{X_o}$. D'après l'appendice II, (7), $C_G(X) \cap S_o$, qui est inclus dans F, opère de manière transitive sur $\Omega_X - \{H\}$. Comme $t \in F - H \cap F$, il en résulte que F opère de manière doublement transitive sur Ω_X. On en déduit que $N_G(X) = FN_V(X)$ comme dans 1).

On a $F \subset C(X_o) \subset N_o$. D'après b) pour X_o, S_o est l'ensemble des 2-éléments de $N_o \cap H$, donc $S_o \cap F$ est l'ensemble des 2-éléments de $F \cap H$. Il en résulte que $S = S_o \cap F = O_2(F \cap H)$ est un 2-Sylow de $F \cap H$ et $S \lhd N_H(X)$. Comme $S = C(X) \cap S_o$ opère transitivement sur $\Omega_X - \{H\}$, on a $N_H(X) = SN_D(X)$.

L'assertion b) de la prop. 3 sera essentielle pour la suite. En voici une première application.

Proposition 4.- *a)* $C_V(K) = C_D(\mathrm{Inv}(H))$.

b) Si $C_V(K) \neq 1$, *alors* $H = C_H(\mathrm{Inv}(H))D$.

Soit $u \in \mathrm{Inv}(H)$ tel que $V = C_D(u)$ (prop. 2,a)). L'application $k \longmapsto u^k$ étant une bijection de K sur Inv(H) (chapitre I, § 2), on voit que $C_V(K) = C_D(u) \cap C(K)$ est l'ensemble des éléments de D qui centralisent Inv(H).

Supposons $C_V(K) \neq 1$ et soit X un groupe de Sylow $\neq 1$ de $C_V(K)$. D'après la prop. 3 b), on a $N_H(X) = S \rtimes N_D(X)$, où S est un 2-Sylow de $C_H(X)$. On a $\mathrm{Inv}(H) = \mathrm{Inv}\, N_H(X) \subset S$ et Inv(H) est central dans S puisque $K = N_K(X)$ opère transitivement sur Inv(H). Donc $S \subset C_H(\mathrm{Inv}(H))$. Cela prouve que : $N_H(X) \cap C_H(\mathrm{Inv}(H)) = S \rtimes (N_D(X) \cap C_D(\mathrm{Inv}(H)))$. Donc X est un groupe de Sylow de $C_H(\mathrm{Inv}(H))$. D'après l'argument de Frattini, on a $H = C_H(\mathrm{Inv}(H))N_H(X)$, mais $N_H(X) = SN_D(X) \subset C_H(\mathrm{Inv}(H))D$, d'où $H = C_H(\mathrm{Inv}(H))D$.

CHAPITRE III.- L'EXISTENCE D'UN COMPLÉMENT NORMAL DE D DANS H

§ 1.- ÉNONCÉ DU THÉORÈME D. RAPPELS SUR LES GROUPES DE CONTRÔLE

Nous gardons les notations et les hypothèses du dernier paragraphe du chapitre II. Dans ce chapitre, nous exposerons le § 6 de l'article de Bender, qui démontre que D a un complément normal dans H. On est alors ramené à la situation étudiée dans un article de Suzuki.

Théorème D.- D *a un complément normal dans* H.

Pour démontrer ce théorème, nous admettrons le résultat suivant de C. Hering : "Un groupe d'ordre pair qui opère de manière doublement transitive sur ses involutions est de 2-rang 1", qui sera démontré dans le chapitre suivant.

Soient W un groupe fini, E un sous-groupe de W, et p un nombre premier. Nous dirons que E est un groupe de p-contrôle dans W si :

1) E contient un p-Sylow de W.

2) Pour tout p-sous-groupe U de E et tout $x \in W$ tel que $U^x \subset E$, on a $x \in C_W(U)E$.

Cette notion est utilisée dans la recherche de compléments normaux. On a en particulier le lemme suivant :

Lemme 1.- Soient W *un groupe fini et* E *un sous-groupe de* W. *Soit* p *un nombre premier tel que* $O^p(E) \subsetneq E$. *Si* E *est un groupe de* p*-contrôle dans* W, *alors* $O^p(W) \subsetneq W$. *Plus précisément, si* y *est un* p*-élément de* E - [E,E] , *on a* $y \notin O^p(W)$.

Soit E_1 le plus petit sous-groupe normal de E tel que E/E_1 soit un p-groupe abélien, et soit T le transfert de W dans E/E_1 : si $Ex_1, \ldots, Ex_n$

sont les classes à droite de E dans W, T(w) est $e_1 e_2 \dots e_n E_1$ où $e_i = x_i w x_{i'}^{-1}$, i' étant l'indice tel que $Ex_i w = Ex_{i'}$. On sait que T est indépendant du choix des x_i et est un homomorphisme de W dans E/E_1 (Huppert, chapitre IV).

Soit y un p-élément de Ker T. Si y opère avec des orbites de cardinaux $r_1, \dots, r_k$ sur l'ensemble des classes à droite de E dans W, on a :

$$T(y) = \prod_{i=1}^{k} (x_i y^{r_i} x_i^{-1}) E_1$$

Ex_i étant un élément de l'orbite de cardinal r_i. D'après l'hypothèse de p-contrôle, on a $x_i y^{r_i} x_i^{-1} = (y^{r_i})^{v_i}$ où v_i est un élément de E. Comme E/E_1 est abélien,

$$T(y) = \prod_{i=1}^{k} (y^{r_i}) E_1 = y^n E_1 \qquad (n = |W:E|).$$

Puisque $y \in \text{Ker } T$, on a $y^n \in E_1$, et par hypothèse $(n,p) = 1$, donc $y \in E_1$.

Si y est un p-élément de $E - [E,E]$, $y \notin E_1$ donc $y \notin \text{Ker } T$. Mais $O^p(W) \subset \text{Ker } T$, donc $y \notin O^p(W)$.

D'autre part, si $O^p(E) \subsetneq E$, on a $E_1 \neq E$ et il existe un p-élément dans $E - E_1$ car la p-composante d'un élément de $E - E_1$ est dans $E - E_1$.

Pour pouvoir appliquer le lemme 1, nous utiliserons le critère suivant pour vérifier que E est un groupe de p-contrôle dans W :

Lemme 2.- Soit E un sous-groupe d'un groupe fini W. Soient p un diviseur premier de |E| et P un p-Sylow de E. On suppose que :

1) $N_W(P) = O_{p'}(C_W(P))N_E(P)$.

2) Pour tout sous-groupe non cyclique U de P, on a $N_W(U) = O_{p'}(C_W(U))N_E(U)$.

Alors E est un groupe de p-contrôle dans W.

L'hypothèse 1) du lemme montre que P est un p-Sylow de $N_W(P)$, donc de W. Il suffit donc de montrer que si U est un p-sous-groupe de E et $x \in W$ est tel que $U^x \subset E$, alors $x \in C_W(U)E$. On raisonne par récurrence sur $|P| - |U|$.

1) Supposons d'abord que $|U| = |P|$. D'après le théorème de Sylow, il existe $y \in E$ tel que $U^x = U^y$, d'où $xy^{-1} \in N_W(U)$. D'après l'hypothèse 1),

$xy^{-1} \in C_W(U)E$, d'où $x \in C_W(U)E$.

2) Soit S un p-Sylow de $N_E(U)$. Alors S est un p-Sylow de $N_W(U)$:

Si S est cyclique, on a $N_E(S) \subset N_E(U)$, donc S est un p-Sylow de $N_E(S)$, donc de E. Que S soit cyclique ou non, on a donc d'après les hypothèses 1) et 2) : $N_W(S) = O_{p'}(C_W(S))N_E(S)$. Comme $O_{p'}(C_W(S)) \subset N_W(U)$, on a $N_W(S) \cap N_W(U) \subset O_{p'}(C_W(S))N_E(U)$, ce qui prouve que S est un p-Sylow de $N_W(U)$.

3) Supposons que $|U| < |P|$ et que U ne soit pas cyclique.

Soient S un p-Sylow de $N_E(U)$ et S_1 un p-Sylow de $N_E(U^x)$. D'après 2) S et $S_1^{x^{-1}}$ sont des p-Sylow de $N_W(U)$, donc il existe $y \in N_W(U)$ tel que $S^y = S_1^{x^{-1}}$, c'est-à-dire $S^{yx} \subset E$. On a $|U| < |S|$, donc par hypothèse de récurrence $yx \in C_W(S)E$, d'où $x \in N_W(U)E$. Mais d'après l'hypothèse 2), $N_W(U) \subset C_W(U)E$, donc $x \in C_W(U)E$.

4) Supposons que $|U| < |P|$ et que U soit cyclique.

Soient encore S un p-Sylow de $N_E(U)$ et S_1 un p-Sylow de $N_E(U^x)$. Alors S et $S_1^{x^{-1}}$ sont des p-Sylow de $N_W(U)$. Puisque U est cyclique, $N_W(U)/C_W(U)$ est abélien et a un seul p-Sylow, donc $SC_W(U) = S_1^{x^{-1}} C_W(U)$. D'après le théorème de Sylow, il existe $y \in C_W(U)$ tel que $S^y = S_1^{x^{-1}}$. Alors $S^{yx} \subset E$ et par hypothèse de récurrence, $yx \in C_W(S)E \subset C_W(U)E$, donc $x \in C_W(U)E$.

Corollaire.- Soit E un sous-groupe d'un groupe fini W. Soit π l'ensemble des diviseurs premiers de $|E|$. On suppose que E est résoluble et que pour tout $p \in \pi$ et tout p-sous-groupe $U \neq 1$ de E, on a :

$$N_W(U) = O_{\pi'}(C_W(U))N_E(U).$$

Alors E est un sous-groupe de Hall de W et a un complément normal dans W.

On voit que E est un sous-groupe de Hall de W en appliquant l'hypothèse dans le cas où U est de Sylow dans E. On peut supposer que $E \neq 1$ et raisonner par récurrence sur $|W|$. Soit $p \in \pi$ tel que $O^p(E) \subsetneq E$. D'après le lemme 2, E est de p-contrôle dans W, et d'après le lemme 1 il existe $W_1 \lhd W$, $W_1 \neq W$ tel que $|W/W_1|$ soit une puissance de p. On a $W = W_1E$ car E contient un p-Sylow de W. On voit que W_1 et $E_1 = E \cap W_1$ vérifient l'hypothèse de récurrence car $O_{\pi'}(C_W(U)) \subset W_1$ pour q premier et U un q-sous-groupe de E_1. Donc E_1 a un

complément normal dans W_1, qui est $O_{\pi'}(W_1)$ donc est normal dans W.

Pour démontrer que D a un complément normal dans H, il suffit d'après le lemme 1 de montrer que si $W \lhd H$ est tel que $WD = H$ et si $E = W \cap D$ est tel que p divise $|E : [E,E]|$, alors E est de p-contrôle dans W. En fait, on pourra démontrer les conditions 1), 2) du lemme 2 en utilisant l'hypothèse de récurrence pour N(P) et N(U) sauf si $P \subset V$ et P opère sans point fixe sur K. Pour traiter ce dernier cas, nous aurons besoin du lemme suivant :

Lemme 3.- Soit X *un sous-groupe* $\neq 1$ *de* V *tel que* $N_K(X) \neq 1$. *Soit* P *un sous-groupe* $\neq 1$ *de* V *tel que* P *normalise* X *et* P *opère sans point fixe sur* $N_K(X)$. *Alors* $p = |P|$ *est premier,* $|C_K(X)| = |\mathrm{Inv}\, N_H(X)| = 2^p - 1$, *et en posant* $V_1 = N_V(X)$, $K_1 = N_K(X)$, *on a* $V_1 = C_{V_1}(K_1) \lhd P$.

Soit S un 2-Sylow de $C_H(X)$ et $Q = \Omega_1(S)$. D'après le chapitre II, § 4, prop. 3, Q est un groupe abélien élémentaire d'ordre $|\mathrm{Inv}\, N_H(X)| + 1$ et $K_1 = C_K(X)$ est un groupe cyclique qui opère régulièrement sur $Q^\#$. On a $K_1 \lhd N_D(X)$ et $C_{V_1}(K_1) = C(Q) \cap N_D(X)$. De plus pour P_1 tel que $1 \neq P_1 \subset P$, on a $C_{K_1}(P_1) = 1$ donc $|C_Q(P)| = 2$. Le lemme résulte alors de l'appendice V appliqué à $U = N_D(X)/C_{V_1}(K_1)$ opérant sur Q.

§ 2.- APPLICATION DU CRITÈRE DE p-CONTRÔLE

Proposition 1.- Soient $W \lhd H$ *tel que* $H = WD$, $E = W \cap D$ *et* p *un diviseur premier de* $|E|$. *On a l'un des deux cas suivants :*

a) E *est un groupe de* p*-contrôle dans* W.

b) Il existe un p*-Sylow* P *de* E *tel que* $P \subset V$, P *opère sans point fixe sur* K *et* P *est cyclique.*

Soit U un p-sous-groupe de E. On a l'une des trois éventualités :

1) U n'a que 2 points fixes dans Ω.

2) U a 3 points fixes dans Ω et il existe un sous-groupe $U_1 \neq 1$ de U tel que $C_K(U_1) \neq 1$.

3) U a 3 points fixes dans Ω et U opère sans point fixe sur K.

Dans le cas 1), $N_W(U)$ opère sur $\Omega_U = \{H, H^t\}$ et laisse fixe H, donc $N_W(U) \subset H \cap H^t \cap W = E$.

Dans le cas 2), U_1 est sous-normal dans U et U est conjugué dans D à un sous-groupe de V, donc d'après le chapitre II, § 4, prop. 3 b), $N_H(U) = S \rtimes N_D(U)$ où $S = O_2(C_H(U))$. On a $S \subset W$ car $|H/W|$ est impair, donc $N_W(U) = S \rtimes N_E(U)$.

Dans le cas 3), U est cyclique d'après l'appendice I, (5)c).

On voit ainsi que les conditions 1) et 2) du § 1, lemme 2 sont vérifiées, sauf éventuellement si E a un p-Sylow P tel que $P \subset V$ et P opère sans point fixe sur K, et dans ce cas P est cyclique.

Corollaire. *Supposons que* $H = C_H(\mathrm{Inv}(H))D$. *Alors* D *a un complément normal dans* H. *En particulier, si* $C_V(K) \neq 1$, D *a un complément normal dans* H.

Soit $W \lhd H$ minimal tel que $H = WD$ et $W \subset C_H(\mathrm{Inv}(H))$, et supposons que $E = W \cap D \neq 1$. Puisque E est résoluble (théorème de Feit-Thompson), il existe un nombre premier p divisant $|E : [E,E]|$. Tout sous-groupe de $V \cap E$ centralise Inv(H), donc K et par conséquent le cas b) de la prop. 1 est impossible. Donc E est de p-contrôle dans W, et la minimalité de W est contredite par le § 1, lemme 1.

La deuxième assertion en résulte d'après le chapitre II, § 4, prop. 4.

Soit W minimal tel que $W \lhd H$ et $H = WD$, et soit $E = W \cap D$. Si $E \neq 1$, il existe un diviseur premier p de $|E : [E,E]|$ (Feit-Thompson) et E ne peut être de p-contrôle dans W d'après le § 1, lemme 1. On supposera donc, dans la suite de ce chapitre :

(D1) $W \lhd H$, $H = WD$, $E = W \cap D \neq 1$, $E' = [E,E]$, et pour tout diviseur premier p de $|E : E'|$, il existe un p-Sylow P de E tel que $P \subset V$, P opère sans point fixe sur K, et P est cyclique.

Lemme 1.- $K \subset E'$, $E^t = E$, *et tout élément de* $E \cap V - E' \cap V$ *opère sans point fixe sur* K.

On a $K \subset E'$ et $E^t = E$ d'après (D1) et l'appendice I, (5),d). Soit $x \in (E - E') \cap V$. L'image $\bar{x}$ de x dans E/E' est $\neq 1$, donc il existe un entier ℓ

tel que x^{ℓ} soit d'ordre premier p et p divise $|E/E'|$. D'après (D1), x^{ℓ} n'a pas de point fixe $\neq 1$ dans K, donc x n'en a pas non plus.

Remarque : Supposons que G soit l'un des groupes figurant dans la conclusion du théorème B, avec $O_{2'}(G) = 1$. Alors l'hypothèse $H = C_H(Inv(H))D$ du corollaire de la prop. 1 est vraie. L'hypothèse $C_V(K) \neq 1$ est vraie si G a un sous-groupe isomorphe à PSU(3,q). D'autre part, on voit comme dans le lemme 3 du § 1 que si G satisfait (D1), alors $V = C_V(K) \rtimes P$ où $|P| = p$ est premier. Ce cas se présente pour $G = G_o P$, $G_o = PSL(2,q)$, Sz(q) ou PSU(3,q), $q = 2^p$ et P est un groupe d'automorphismes d'ordre p de G_o induit par $Aut(\mathbb{F}_q)$.

Remarquons que si aucun élément de $D^{\#}$ ne centralise 2 involutions de H (c'est-à-dire, puisque $V \neq 1$ d'après (D1), si V est un complément de Frobenius dans D), on ne pourra pas appliquer la prop. 3 du chapitre II, §4. Ce cas existe réellement, pour $G = G_o P$, $G_o = PSL(2,q)$ ou Sz(q), $q = 2^p$ et P comme ci-dessus. On montrera dans ce cas, en utilisant la théorie des caractères, que H opère de manière doublement transitive sur Inv(H) ou bien que $H = C_H(Inv(H))D$.

§ 3.- CAS OÙ ON NE PEUT PAS APPLIQUER L'HYPOTHÈSE DE RÉCURRENCE

Proposition 1.- Supposons que pour tout X *tel que* $1 \neq X \lhd V$, *on ait* $C_K(X) = 1$. *Alors* E, *opérant sur* Inv(H), *est un groupe de Frobenius.*

1) K est un groupe abélien et $(|K|, |F(V)|) = 1$.

Pour tout diviseur premier q de $|F(V)|$, on a $C_K(O_q(V)) = 1$ donc $q \nmid |K|$. Donc $(|K|, |F(V)|) = 1$ et K est un groupe abélien d'après l'appendice I,(5)b).

2) Soit p un diviseur premier de $|E:E'|$. Alors p divise $|F(E \cap V)|$.

Soit P un sous-groupe d'ordre p de $E \cap V$ (voir (D1)). Soit $Q = F(E \cap V)$ et supposons que $p \nmid |Q|$. Puisque $C_K(P) = 1$ d'après (D1), le théorème de l'appendice VII montre que $K = C_K([Q,P])$, d'où $[P,Q] \subset C_V(K)$. Mais on a $C_V(K) = 1$ d'après l'hypothèse, donc $[P,Q] = 1$ et $P \subset Q$ d'après le théorème de Fitting.

3) $F(E \cap V)$ opère sans point fixe sur K.

Soit X maximal parmi les sous-groupes de $F(E \cap V)$ tels que $C_K(X) \neq 1$, et supposons que $X \neq 1$. Soit p comme dans 2) et P un sous-groupe d'ordre p de $F(E \cap V)$.

D'après (D1), $p \nmid |X|$. Puisque $F(E \cap V)$ est nilpotent, il en résulte que $P \subset C(X)$. On peut alors appliquer le lemme 3 du § 1. Si $V_1 = N_V(X)$, $K_1 = C_K(X)$, on a $V_1 = C_{V_1}(K_1) \rtimes P$. Comme $P \subset F(E \cap V) \cap V_1$, on a :

$$N_{F(E \cap V)}(X) = V_1 \cap F(E \cap V) = [C_{V_1}(K_1) \cap F(E \cap V)] \rtimes P.$$

D'après la maximalité de X, il en résulte que $N_{F(E \cap V)}(X) = X \rtimes P$. Comme $F(E \cap V)$ est nilpotent, cela implique que $X = O_{p'}(F(E \cap V))$, donc $X \lhd V$, ce qui contredit l'hypothèse.

4) Conclusion

Puisque $F(E \cap V)$ est nilpotent d'ordre impair, 3) implique que $F(E \cap V)$ est cyclique. D'après le théorème de Fitting, $(E \cap V)/F(E \cap V)$ est isomorphe à un sous-groupe de Aut $F(E \cap V)$, donc est abélien. On a donc $[E \cap V, E \cap V] \subset F(E \cap V)$. Mais $E = K(V \cap E)$, $K \subset E'$ et $K \lhd E$ (§ 2, lemme 1 et appendice I,(4)) d'où $E' = K[V \cap E, V \cap E]$. Il en résulte que $E' \cap V = [V \cap E, V \cap E] \subset F(E \cap V)$. Donc $E' \cap V$ opère sans point fixe sur K. D'après le lemme 1 du § 2, $E \cap V$ opère sans point fixe sur K, donc E est un groupe de Frobenius de complément $E \cap V$.

Proposition 2.- Supposons que E, opérant sur Inv(H), soit un groupe de Frobenius. Alors la conclusion du théorème D est vraie.

Les éléments $\neq 1$ de K ne fixent aucune involution de H et $|E| = |K||V \cap E|$ car $K \subset E$ (§ 2, lemme 1). Donc K est le noyau de Frobenius de E et K opère régulièrement sur Inv(H). Puisque t inverse les éléments de K, K est un groupe abélien. Pour $k \in K^{\#}$, k n'a que 2 points fixes dans Ω (chapitre II, § 4, prop. 2), donc $C_W(k) \subset C_H(k) \subset D$, d'où $C_W(k) \subset E$ et $C_W(k) = K$. D'après le théorème de l'appendice VI, on a $W = C_W(\mathrm{Inv}(H))N_W(K)$ ou bien W opère de manière 2-transitive sur Inv(H). Mais puisque $\mathrm{Inv}(H) \subset W$, W est de 2-rang ≥ 2 et W ne peut opérer de manière 2-transitive sur Inv(H) d'après le résultat de Hering (voir § 1), donc $W = C_W(\mathrm{Inv}(H))N_W(K)$. On a $N_W(K) \subset D$ car $\Omega_K = \{H, H^t\}$, donc $H = WD = C_H(\mathrm{Inv}(H))D$. La conclusion résulte alors du corollaire de la prop. 1 du § 2.

Corollaire.- Si $E' \cap V = 1$ ou si pour tout X tel que $1 \neq X \lhd V$, on a $C_K(X) = 1$, alors la conclusion du théorème D est vraie.

En effet, E opérant sur Inv(H) est alors un groupe de Frobenius, d'après

le lemme 1 du § 2 si $E' \cap V = 1$, et d'après la prop. 1 dans le deuxième cas.

§ 4.- STRUCTURE DE D

On raisonne désormais par l'absurde. On suppose que W est minimal tel que $W \lhd H$ et $H = WD$, mais que $E = W \cap D \neq 1$. Alors l'hypothèse (D1) est satisfaite et de plus, d'après le corollaire de la prop. 1 du § 2 et le corollaire de la prop. 2 du § 3 :

(D2) Il existe X tel que $1 \neq X \lhd V$ et $C_K(X) \neq 1$, on a $C_V(K) = 1$ et $E' \cap V \neq 1$.

Remarque : Si G est l'un des groupes apparaissant dans la conclusion du théorème B, avec $O_{2'}(G) = 1$, alors $V/C_V(K)$ est cyclique, donc les hypothèses $C_V(K) = 1$ et $E' \cap V \neq 1$ sont contradictoires. On voit aussi que pour un tel G les hypothèses (D1), $C_V(K) = 1$ et il existe X tel que $1 \neq X \subset V$ et $C_K(X) \neq 1$ sont contradictoires.

On considère dans la suite un diviseur premier p de $|E : E'|$ et un sous-groupe P d'ordre p de $V \cap E$, qui existe d'après (D1).

Lemme 1.- a) Il existe un sous-groupe $A \neq 1$ *de* V *tel que* $V = A \rtimes P$ *et* $|C_K(A)| = 2^p - 1$.

b) Pour tout sous-groupe B *tel que* $1 \neq B \subset A$ *et* P *normalise* B, *on a* $C_K(B) = C_K(A)$.

c) $N_D(P) = C_A(P) \times P$ *et* $D = \langle K \rangle A \rtimes P$.

d) P *est un* p*-Sylow de* D *et* $E = E' \rtimes P$.

D'après (D1), P opère sans point fixe sur K. Soit X comme dans (D2). D'après le lemme 3 du § 1, on a $V = C_V(K_1) \rtimes P$, où $K_1 = N_K(X) \neq 1$. Soit $A = C_V(K_1)$. On a $A \neq 1$ d'après (D2). Soit B un sous-groupe normalisé par P tel que $1 \neq B \subset A$. Puisque B centralise $K_1 \neq 1$, on peut appliquer le lemme 3 du § 1 avec B à la place de X. On en déduit que $|C_K(B)| = 2^p - 1$. Cela prouve a) et b).

D'après l'appendice I, (5) c), $N_D(P) \subset V$, donc $N_D(P) = C_A(P) \times P$. Puisque $\langle K \rangle \lhd D$ et $D = KV$, on a $\langle K \rangle A \lhd D$ et $D = \langle K \rangle AP$. Puisque P opère sans point

fixe sur K, $p \nmid |K|$ donc $p \nmid |<K>|$ (appendice I,(5)) donc $|<K>A|_p = |A|_p < |D|_p$, donc $P \not\subset <K>A$ d'où $D = <K>A \rtimes P$.

Supposons que P ne soit pas un p-Sylow de D. D'après c) un p-Sylow de D n'est pas cyclique. D'après la prop. 1 du § 2 (avec $W = H$), D est de p-contrôle dans H. D'après c) et le lemme 1 du § 1, $P \not\subset O^p(H)$, donc $P \not\subset O^p(W)$. Comme $H = O^p(W)D$, la minimalité de W est contredite.

D'après c) il existe M tel que $E = M \rtimes P$. Si $E' \neq M$, $|E : E'|$ aurait un diviseur premier $q \neq p$, et d'après (D1) il existerait un q-sous-groupe $Q \neq 1$ de $E \cap V$ qui opère sans point fixe sur K. Alors $Q \subset A$ donc Q centralise $C_K(A) \neq 1$ ce qui est absurde, d'où d).

Proposition 1.- Soit π l'ensemble des diviseurs premiers r de $|D|$ tels que $r \neq p$ et $r \nmid |K|$. Alors $C_A(P)$ est un π-sous-groupe de Hall de D et $K[A,P]P$ est un complément normal de $C_A(P)$ dans D.

1) $C_A(P)$ est un sous-groupe de Hall de $N_H(P)$ et a un complément normal dans $N_H(P)$.

Soit U un sous-groupe $\neq 1$ de $C_A(P)$. On a $C_K(U) \neq 1$ car $U \subset A$, donc d'après le chapitre II, § 4, prop. 3 b), $N_H(U \times P) = O_2(C_H(U \times P)) \rtimes N_D(U \times P)$, c'est-à-dire d'après le lemme 1, c) et d) :

$$(*) \qquad N_H(U) \cap N_H(P) = [O_2(C_H(U \times P)) \times P] \rtimes N_{C_A(P)}(U).$$

Il suffit alors d'appliquer le corollaire du lemme 2 du § 1.

2) Si $C_A(P) \neq 1$, alors P n'est pas un p-Sylow de H.

Soit U un groupe de Sylow $\neq 1$ de $C_A(P)$. D'après 1), U est un groupe de Sylow de $N_H(P)$ et $N_H(U) \cap N_H(P) \subset C_H(P)$. D'après l'argument de Frattini, $N_H(P) = C_H(P)[N_H(U) \cap N_H(P)] \subset C_H(P)$. Si P est un p-Sylow de H, W a un p-complément normal d'après le théorème de Burnside, et la minimalité de W est contredite.

3) Soit R un groupe de Sylow de $C_A(P)$. Alors $|R|$ divise $p - 1$.

D'après 1), il existe un p-Sylow P_1 de $N_H(P)$ qui est normalisé par R. On peut supposer que $R \neq 1$, donc $P \subsetneq P_1$ d'après 2). L'égalité (*) de 1) montre que pour U tel que $1 \neq U \subset R$, on a $C_H(U) \cap P_1 = P$, donc R opère sans point fixe sur P_1/P.

Le groupe $N_H(P)$ est un groupe de Bender propre de $N_G(P)$ (chapitre II, § 4, prop. 1), $N_G(P)$ est 2-transitif sur Ω_P (appendice II,(5)) et $N_G(P)$ est de 2-rang 1 car $|N_K(P)| = |\mathrm{Inv}\, N_H(P)| = 1$. Si N est le noyau de l'opération de $N_G(P)$ sur Ω_P, il résulte alors de l'appendice III,(5) que $P_1 N/N$ est cyclique et, P étant un p-Sylow de D, P_1/P est cyclique.

Puisque R opère sans point fixe sur le groupe $\Omega_1(P_1/P)$ d'ordre p, $|R|$ divise p-1.

4) $C_A(P)$ est un π-groupe.

On sait que $p \nmid |C_A(P)|$ (lemme 1,d)). Soit d'autre part r un nombre premier tel que $r \mid |A|$ et $r \mid |K|$. Soit R un r-Sylow de A normalisé par P. D'après la décomposition de K en réunion d'orbites sous R, r divise $|C_K(R)|$, donc (lemme 1 b)), r divise $2^p - 1$. Il en résulte que 2 est d'ordre p dans $(\mathbb{Z}/r\mathbb{Z})^*$, donc $p \leq r - 1$ et d'après 3) r ne divise pas $|C_A(P)|$.

5) $C_A(P)$ est un sous-groupe de Hall de D.

Soient $r \in \pi$ et R un r-Sylow de A normalisé par P. D'après l'appendice I, (5)a), $|<K>|$ est premier à $|RP|$, et on peut appliquer le théorème de l'appendice VII à RP opérant sur $<K>$. D'après 4) et le lemme 1 c), $|C_D(P)|$ est premier à $|K|$, donc à $|<K>|$, et on a par conséquent $C_{<K>}(P) = 1$. Donc $<K>$ est centralisé par $[R,P]$. D'après (D2) on a donc $[R,P] = 1$ et $R \subset C_A(P)$.

6) Conclusion.

D'après 5) et l'appendice I,(5) b), $[A,P]$ est un complément normal de $C_A(P)$ dans A. Alors $<K>[A,P]P$ est un π-complément normal dans D, et $<K>[A,P] = K[A,P]$ car $<K> \cap V \subset O_{\pi'}(A) = [A,P]$.

Proposition 2.- a) $E = K[A,P]P$, $E' = K[A,P]$, $E' \cap V = [A,P]$.

b) *E' est un groupe nilpotent, est un sous-groupe de Hall de G, et* $|E'|$ *a les mêmes diviseurs premiers que* $|K|$.

c) $|K| = r^a(2^p - 1)$ *où a est un entier* ≥ 1 *et r un diviseur premier de* $2^p - 1$.

d) $F(V) = E' \cap V$ *et* $F(V)$ *est un r-Sylow de V.*

a) Puisque $E \lhd D$, d'après l'argument de Frattini et le lemme 1 c), on a $D = EN_D(P) = EC_A(P)$. On a donc $K[A,P]P \subset E$ d'après la prop. 1. D'après le

lemme 1 d), il en résulte que $E = K[A,P]P$, $E' = K[A,P]$ et $E' \cap V = [A,P]$.

b) D'après la prop. 1, $C_A(P) \cap E' = 1$, donc $C_{E'}(P) = 1$. D'après le théorème de Thompson sur le noyau des groupes de Frobenius, E' est nilpotent. Il résulte de a) et de la prop. 1 que E' est un sous-groupe de Hall de D tel que $|E'|$ ait les mêmes diviseurs premiers que $|K|$, et E' est de Hall dans G d'après le chapitre II, §4, prop. 2d).

c) D'après (D2), $E' \cap V \neq 1$. Soit r un diviseur premier de $|E' \cap V|$ et R le r-Sylow de $E' \cap V$. D'après b), on a $E' = S_1 \times S_2$ où $S_1 = O_r(E')$, $S_2 = O_{r'}(E')$ et $R \subset S_1$. Soit $K_i = J(S_i,t)$. Puisque t normalise S_i et $K \subset E'$, on a $K = K_1 \times K_2$. D'après le lemme 1 b), on a $|C_K(R)| = 2^p - 1$. On a $C_K(R) = C_{K_1}(R) \times K_2$, donc $|K|/(2^p - 1) = |K_1|/|C_{K_1}(R)|$ est une puissance de r. D'après l'hypothèse $C_V(K) = 1$, on a $Z(S_1) \cap V = 1$, donc $1 \neq Z(S_1) \subset C_{K_1}(R)$, donc r divise $|C_K(R)| = 2^p - 1$. D'autre part, si $|K| = 2^p - 1$, alors R centralise K, contrairement à l'hypothèse $C_V(K) = 1$. Donc $|K| > 2^p - 1$.

d) Il résulte de la démonstration de c) que $|E' \cap V|$ a un seul diviseur premier r. Alors $R = E' \cap V$ est un r-Sylow de V d'après b) et $R \lhd V$ donc $R \subset F(V)$. Soit Q tel que $F(V) = R \times Q$. Puisque $R = [A,P] \neq 1$, $P \not\lhd V$ donc $P \cap F(V) = 1$ et $Q \subset A$. Donc Q centralise $C_K(R) = C_K(A)$. Puisque $C_{S_1}(R) = Z(R)C_{K_1}(R)$ (appendice I, (1)), Q centralise $C_{S_1}(R)$. D'après le lemme 4 de l'appendice IV appliqué à $R \times Q$ opérant sur S_1, Q centralise S_1. Puisque Q centralise $C_K(R)$, il en résulte que Q centralise K, et on a donc $Q = 1$ d'après l'hypothèse $C_V(K) = 1$.

§ 5.- FIN DE LA DÉMONSTRATION

On garde les notations p, P, A, r du § 4.

Proposition 1.- $p \geq 7$.

Supposons que $p = 3$ ou 5. Alors $2^p - 1 = 7$ ou 31 est premier et d'après le § 4, prop. 2 c), $|K| = r^{a+1}$ où r est premier et $a \geq 1$. Soit $U = \langle \mathrm{Inv}(H) \rangle$.

1) On a $U \cap E' \neq 1$.

Supposons en effet que $U \cap E' = 1$. D'après le § 4, prop. 2 b), E' est un

r-Sylow de G donc U est un r'-groupe. Il existe alors un 2-Sylow S de U normalisé par E'. Puisque $K \subset E'$ opère transitivement sur Inv(H), il en résulte que $Inv(H) \subset Z(S)$, donc U est abélien élémentaire et $|U| = 2^b$ pour un entier $b \geq 2$. Comme $|Inv(H)| = |K|$, on a alors $2^b = r^{a+1} + 1$, donc $r^{a+1} \equiv -1 \pmod 4$, donc a est pair. Mais alors $(r^{a+1} + 1)/(r + 1)$ est un nombre entier impair qui divise 2^b, donc $a = 0$, ce qui est impossible.

2) $W = U$.

D'après la proposition 2 b) du § 4, $U \cap E'$ est un r-Sylow de U donc d'après l'argument de Frattini, $H = UN_H(U \cap E')$. Si $U \cap E'$ a 3 points fixes dans Ω, on a $U \cap E' \subset V$ (chapitre II, § 4, prop. 2) et comme $U \cap E' \lhd D$, $K = N_K(U \cap E') = C_K(U \cap E')$ (chapitre II, § 4, lemme 1). D'après l'hypothèse $C_V(K) = 1$, on a $U \cap E' = 1$, ce qui contredit 1). Donc $U \cap E'$ n'a que 2 points fixes dans Ω et par conséquent $N_H(U \cap E') \subset D$. Donc $H = UD$. Comme $|H/W|$ est impair, on a $U \subset W$, et d'après la minimalité de W, $U = W$.

3) Conclusion.

Puisque $K \subset E' \subset W$, Inv(H) est une classe de conjugaison de W, et $|Inv(H)| = |K|$ est puissance d'un nombre premier. On peut alors appliquer le théorème suivant de Burnside :

Soit $\mathcal{C}$ une classe de conjugaison d'un groupe fini $W \neq 1$ tel que $|\mathcal{C}|$ soit puissance d'un nombre premier. Alors il existe $N \lhd W$ tel que $N \neq W$ et tel que l'image de $\mathcal{C}$ dans W/N soit contenue dans Z(W/N).

[Pour la démonstration, voir Isaacs, théorème (3-9)].

Soit $N \lhd W$ tel que $N \neq W$ et tel que l'image de Inv(H) dans W/N soit contenue dans Z(W/N). D'après 2), W/N est alors un 2-groupe abélien élémentaire $\neq 1$, et comme les involutions de H sont conjuguées dans W, $|W/N| = 2$ et $Inv(H) \cap N = \emptyset$. Il en résulte que W est de 2-rang 1, ce qui est absurde.

Dans la dernière partie de la démonstration, on montrera que $N_H(P)$ normalise F(V). En appliquant l'hypothèse de récurrence à $N_G(F(V))$, cela permettra de voir que D est de p-contrôle dans H, contredisant la minimalité de W. Pour voir que $N_H(P)$ normalise F(V), on construit un sous-groupe N de G, formé d'éléments fortement réels, tel que $N_H(P)$ normalise N et F(V) soit un sous-groupe caractéristique de $C_H(N)$.

Lemme 1.- Soit X *un sous-groupe tel que* $P \subset X \subset V$ *et* $N_H(P) \subset N_H(X)$. *Alors* $X = P$.

On a $X = (X \cap A) \rtimes P$. Supposons $X \cap A \neq 1$. Alors d'après le chapitre II, § 4, prop. 3, on a $N_H(X) = O_2(C_H(X)) \rtimes N_D(X)$. Puisque $N_H(P) \subset N_H(X)$, $O_2(C_H(X)) \subset C_H(P)$ et $N_D(P) \subset N_D(X)$, il en résulte que $N_H(P) = O_2(C_H(X)) \rtimes N_D(P)$. D'après le § 4 lemme 1, c) et d), P est donc un p-Sylow de H et $N_H(P) = C_H(P)$. D'après le théorème de Burnside, W a un quotient d'ordre p, et la minimalité de W est contredite.

On utilisera les propriétés suivantes des groupes PSL(2,q), Sz(q), (q puissance de 2).

1°.- Si S est un 2-Sylow de PSL(2,q) ou Sz(q) et $x \in S$, on a $x^4 = 1$.

2°.- Soient u, v des involutions de L = PSL(2,q) (resp. L = Sz(q)) telles que $[u,v] \neq 1$. Alors $C_L(uv)$ est un groupe cyclique d'ordre $q \pm 1$ (resp. $q \pm \sqrt{2q} + 1$) dont les éléments sont inversés par u.

Proposition 2.- Soit u *l'involution de* $C_H(V)$ *et soit* $M = \{x \in C_G(ut) \mid x^t = x^{-1}\}$.

a) L'ordre f *de* ut *est 3 ou 5.*

b) Pour $x \in M - \{1\}$, *on a* $\Omega_x = \emptyset$, $(|M|, |F(V)|) = 1$, *et* M *est un groupe abélien.*

c) $N_H(P)$ *normalise* M.

d) $O_{f'}(M) \neq 1$ *et* P *opère sans point fixe sur* $O_{f'}(M)$.

a) Soit $F = O^{2'}(C_G(V))$. Puisque $V = A \rtimes P$ et $C_K(A) \neq 1$, d'après la prop. 3, § 4 du chapitre II, $F \cap H$ a un seul 2-Sylow S et S opère de manière régulière sur $\Omega_V - \{H\}$.

Soit $F_o = O^{2'}(C_G(A))$. D'après la prop. 3, § 4 du chapitre II, $F_o/Z(F_o)$ est isomorphe à l'un des groupes PSL(2,q), Sz(q) ou PSU(3,q). Ce dernier cas est d'ailleurs exclu car, P ne centralisant pas A (§ 4, prop. 2), on a $F_o \cap V = F_o \cap A \subset Z(F_o)$, donc le fixateur de 3 points de Ω_A dans $F_o/Z(F_o)$ est réduit à l'identité. Si S_o est le 2-Sylow de $C_H(A)$, on a donc $S_o^4 = 1$. Comme $F \subset F_o$, on a $S \subset S_o$. Donc S est un 2-groupe qui n'a qu'une involution, tel que $S^4 = 1$. Il en résulte que S est cyclique d'ordre 2 ou 4, ou quaternionien d'ordre 8. Par conséquent, $|\Omega_V| = |S| + 1 = 3, 5$ ou 9.

Soit Z le noyau de l'opération de F sur Ω_V. D'après l'appendice III,2), $F/Z = \bar{Q} \rtimes ((F \cap H)/Z)$ où $\bar{Q}$ est un f-groupe abélien élémentaire pour un nombre premier f, et $|\bar{Q}| = |\Omega_V|$ donc f = 3 ou 5.

D'après l'appendice III,(4), on a $\bar{u}\,\bar{t} \in \bar{Q}$ dans F/Z, donc $(ut)^f \in Z$. Or t centralise Z d'après le théorème C, donc $(ut)^f$ est inversé par t et centralisé par t, donc $(ut)^f = 1$, et ut est d'ordre f.

b) On a $\Omega_{ut} = \emptyset$. En effet, si $ut \in H_1$ avec $H_1 \in \Omega$, alors $ut \in J(H_1,t)$ et $t \notin H_1$ car $H(u) \neq H(t)$. D'après le chapitre I, § 6, corollaire 1, ut est conjugué à un élément de K, donc f divise $|<K>|$. D'après le § 4, prop. 2 b) et c), f divise $2^p - 1$, donc $f \equiv 1 (\mathrm{mod}.p)$. Cela est impossible d'après a).

Si $x \in M - \{1\}$, on a $\Omega_x = \emptyset$. En effet, si $|\Omega_x| \geq 2$, il existe $H_1 \in \Omega$ tel que $t \notin H_1$ et $x \in H_1$. Alors $x \in J(H_1,t)$ et d'après la prop. 2, § 4, du chapitre II, $|\Omega_x| = 2$. On a donc $|\Omega_x| \leq 2$. Supposons que $|\Omega_x| = 1$ ou 2. Alors ut est un élément d'ordre impair qui centralise x, donc doit laisser fixe le point ou les 2 points de Ω_x. Cela est absurde car $\Omega_{ut} = \emptyset$.

Puisque t opère sur le groupe $C_G(ut)$ et $C(t) \cap C(ut) \subset C(u) \cap C(t) \subset V$, on a $C_{C(ut)}(t) = V$ et, t étant d'ordre 2, $|C_G(ut)|$ est donc impair. D'après l'appendice I,(5), appliqué à $X = C_G(ut)$, il suffit que $(|M|, |F(V)|) = 1$ pour que M soit un groupe abélien. Si $(|M|, |F(V)|) \neq 1$, r divise $|M|$ (§ 4, prop. 2,d)), donc un r-Sylow de $C_G(ut)$ normalisé par t n'est pas centralisé par t, donc M a un élément x d'ordre r. Mais D contient un r-Sylow de G (§ 4, prop. 2,b), donc x a 2 points fixes, contrairement à ce qu'on a vu dans le paragraphe précédent.

c) Précisons la structure de $N_G(P)$. D'après la prop. 1, § 4 du chapitre II, $N_H(P)$ est un groupe de Bender propre de $N_G(P)$, qui est de 2-rang 1 car $|N_K(P)| = |\mathrm{Inv}\, N_H(P)| = 1$. Le noyau de l'opération de $N_G(P)$ sur Ω_P est P d'après le lemme 1, et $N_G(P)$ opère de manière doublement transitive sur Ω_P d'après l'appendice II,(5). D'après l'appendice III,(2), il existe alors un sous-groupe Q tel que $P \subset Q \subset N_G(P)$ et $N_G(P)/P = Q/P \rtimes N_H(P)/P$. Comme $ut \notin H$, on a $\bar{u} \neq \bar{t}$ dans $N_G(P)/P$ et $\bar{u}\,\bar{t}$ est d'ordre f. Donc Q/P est un f-groupe abélien élémentaire dont les éléments sont inversés par u (appendice III,(2) et (4)). On a donc $C_Q(u) = P$. On a $f \neq p$ d'après a) et la prop. 1. Donc $Q = P \times J(Q,u)$ et $J(Q,u) \tilde{=} Q/P$ d'après l'appendice I,(5)b).

On a $ut \in Q$ donc $ut \in J(Q,u)$, d'où $J(Q,u) \subset M$, et M étant un groupe abélien

M est donc l'ensemble des éléments de $C_G(J(Q,u))$ inversés par u. Or, $J(Q,u) = O_{f}(Q)$ est normal dans $N_G(P)$ et $N_H(P)$ centralise u car u est la seule involution de $N_H(P)$. Puisque $N_H(P)$ normalise J(Q,u) et u, $N_H(P)$ normalise M.

d) On a vu dans a) que si $F_o = O^{2'}(C_G(A))$, $L = F_o/Z(F_o)$ est isomorphe à PSL(2,q) ou Sz(q), et on a $q = 1 + |C_K(A)| = 2^p$. Soient $T_1/Z(F_o) = C_L(ut)$ et $T = J(T_1,u)$. Alors $T_1/Z(F_o)$ est cyclique d'ordre $q \pm 1$ ou $q \pm \sqrt{2q} + 1$ et ses éléments sont inversés par u. Comme $T_1/Z(F_o)$ est cyclique et $Z(F_o)$ est central dans T_1, T_1 est abélien, donc T est un sous-groupe. Puisque u inverse les éléments de $T_1/Z(F_o)$, on a $C_{T_1}(u) = Z(F_o)$, d'où $T_1 = Z(F_o) \times T$ et $T \tilde{=} T_1/Z(F_o)$. On va montrer que $O_{f'}(T) \subset M$ et $O_{f'}(T) \neq 1$, ce qui prouvera que $O_{f'}(M) \neq 1$.

On a $ut \in T$ et T est abélien, donc ut centralise $O_{f'}(T)$, donc $O_{f'}(T) \subset M$.

Soit $U = T \cap N_G(P)$. Alors UP/P est un sous-groupe d'ordre impair de $N_G(P)/P$ dont les éléments sont inversés par u, donc avec la notation de c), $UP/P \subset Q/P$ (appendice III,(4)), et $U \subset J(Q,u)$. On a vu dans c) que J(Q,u) est un f-groupe abélien élémentaire, donc T étant cyclique, on a $|U| = f$. On voit que pour $p > 3$ et $q = 2^p$, aucun des nombres $q \pm 1$, $q \pm \sqrt{2q} + 1$ ne peut être égal à $f = 3$ ou 5. Donc $U \neq T$ et par conséquent $P \not\subset C_G(T)$. Mais P normalise A et centralise u et t, donc $P \subset N_G(T)$. Donc $|N_G(T)/C_G(T)|$ est divisible par p et $p > f$ (prop. 1). Il en résulte que T n'est pas un f-groupe cyclique, d'où $O_{f'}(T) \neq 1$.

Les éléments de $C_M(P)$ sont des éléments d'ordre impair de $N_G(P)$ inversés par u, donc comme ci-dessus, $C_M(P) \subset J(Q,u)$, donc $C_M(P)$ est un f-groupe et P opère sans point fixe sur $O_{f'}(M)$.

Proposition 3.- $N_H(P) \subset N_H(F(V))$.

Soit $N = O_{f'}(M)$. D'après la prop. 2 c), $N_H(P)$ normalise N, et il suffit de montrer que F(V) est un sous-groupe caractéristique de $C_H(N)$.

Puisque $C_{C(ut)}(t) = V$ et $M = J(C(ut),t)$, V normalise M donc F(V) normalise N et le groupe $F(V) \rtimes P$ opère sur N. De plus P opère sans point fixe sur N et sur F(V) et $(|N|, |F(V)|) = 1$ (prop. 2 d) et b) et § 4, prop. 1 et 2). D'après le théorème de l'appendice VII, N est centralisé par $[F(V),P] = F(V)$. Donc $F(V) \subset C_H(N)$.

Supposons que $C_H(N)$ n'ait qu'un ou deux points fixes dans Ω. D'après

la prop. 2 d), $N \neq 1$ et si $x \in N^{\#}$, x est d'ordre impair et centralise $C_H(N)$ donc fixe le ou les points fixes de $C_H(N)$, ce qui contredit la prop. 2 b). Donc $C_H(N)$ fixe au poins 3 points de Ω.

D'après le chapitre II, § 4, prop. 2, il existe donc $g \in G$ tel que $F(V) \subset C_H(N) \subset V^g$. D'après le § 4, prop. 2, $F(V)$ est le seul r-Sylow de V, donc le seul r-Sylow de V^g, d'où $F(V) = O_r(C_H(N))$.

Contradiction finale.- D'après la prop. 3, $N_H(P) \subset N_H(PF(V))$, ce qui contredit le lemme 1.

CHAPITRE IV

LES GROUPES QUI OPÈRENT DE MANIÈRE DOUBLEMENT TRANSITIVE SUR LEURS INVOLUTIONS

§ 1.- UNE PROPOSITION DE WAGNER

Le but de ce chapitre est de démontrer le théorème suivant, qui a été utilisé dans la démonstration du théorème D :

THÉORÈME E.- Soit G *un groupe d'ordre pair qui opère de manière doublement transitive sur* Inv(G), *par conjugaison. Alors* G *est de 2-rang 1.*

Ce théorème a été démontré par C. Hering (Archiv der Math. 22, 1971, p. 456). La démonstration se base sur une proposition de A. Wagner (On collineation groups of projective spaces I, Math. Z. 76, 1961, p. 411) et sur un résultat de J.L. Alperin, annoncé dans "Sylow 2-subgroups of rank 3" (Finite groups 72, North Holland Publishing Company).

A. Wagner a étudié les groupes de collinéations doublement transitifs sur les points d'un espace projectif, et a en particulier démontré :

Proposition.- Soit V *un espace vectoriel de dimension* $n \geq 3$ *sur* $\mathbb{F}_2$. *Soit* G *un sous-groupe de* GL(V) *qui opère de manière doublement transitive sur* $V - \{0\}$. *Soit* U *un sous-espace de dimension 3 de* V. *Alors* $N_G(U)/C_G(U)$ *est isomorphe à* Aut(U).

Pour $X \subset V$, on note $N_G(X)$ ou G_X le sous-groupe des éléments de G qui laissent X invariant, $C_G(X)$ le sous-groupe des éléments de G qui laissent chaque point de X invariant, et on notera $\bar{G}_X = N_G(X)/C_G(X)$ que l'on identifie à un groupe de permutations de X.

Lemme 1.- Soit V *un espace vectoriel de dimension* $n \geq 2$ *sur* $\mathbb{F}_2$, $N = |V| - 1$, $v_1, \ldots, v_N$ *les points de* $V - \{0\}$, $H_1, \ldots, H_N$ *les hyperplans de* V. *Alors la matrice d'incidence* $A = (a_{ij})_{1 \leq i,j \leq N}$, *définie par* $a_{ij} = 1$ *si* $v_i \in H_j$, $a_{ij} = 0$ *sinon, est inversible*

Soit $A.{}^tA = (b_{ij})$. D'après la définition de A, b_{ij} est le nombre des hyperplans H de V tels que $v_i \in H$ et $v_j \in H$. Donc :

$$b_{ii} = \alpha = 2^{n-1} - 1 \quad \text{et} \quad b_{ij} = \beta = 2^{n-2} - 1 \quad \text{pour} \quad j \neq i.$$

On voit alors que $(\det A)^2 = \det(b_{ij}) = (\alpha - \beta)^{N-1}[\alpha + (N-1)\beta] \neq 0$, donc $\det A \neq 0$.

Lemme 2.- Soit V *un espace vectoriel de dimension* ≥ 2 *sur* $\mathbb{F}_2$. *Soit* G *un sous-groupe de* GL(V).

a) Le caractère de G *considéré comme groupe de permutations de* $V - \{0\}$ *est égal au caractère de* G *considéré comme groupe de permutations de l'ensemble des hyperplans de* V.

b) Le nombre d'orbites de G *sur* $V - \{0\}$ *est égal au nombre d'orbites de* G *sur l'ensemble des hyperplans de* V.

Gardons les notations du lemme 1. Soit $g \in G$. Soit P(g) la matrice de permutation de g opérant sur $V - \{0\}$: $P(g) = (p_{ij})_{1 \leq i,j \leq N}$, $p_{ij} = 1$ si $g(v_i) = v_j$, $p_{ij} = 0$ sinon. Soit Q(g) la matrice de permutation de g opérant sur l'ensemble des hyperplans de V, définie de manière analogue. On a

$$(P(g) \,.\, A)_{ik} = a_{jk} \qquad \text{avec } j \text{ tel que} \qquad g(v_i) = v_j$$

$$(A \,.\, Q(g))_{ik} = a_{i\ell} \qquad \text{avec } \ell \text{ tel que} \qquad g(H_\ell) = H_k$$

et $a_{jk} = 1 \iff v_j \in H_k \iff v_i \in H_\ell \iff a_{i\ell} = 1$.

Donc $P(g).A = A.Q(g)$ et d'après le lemme 1, $Q(g) = A^{-1}P(g)A$, d'où $\mathrm{Tr}\, Q(g) = \mathrm{Tr}\, P(g)$. Cela démontre a).

b) se déduit de a) car si G est un groupe de permutations de caractère χ, on sait que le nombre d'orbites de G est $[\chi, 1_G] = (1/|G|) \sum_{g \in G} \chi(g)$.

Lemme 3.- Soit G *un groupe fini opérant transitivement sur deux ensembles finis* A *et* B. *Si* $|A|$ *et* $|B|$ *sont premiers entre eux et si* $a \in A$, G_a *opère transitivement sur* B.

C'est une autre formulation de Huppert, chapitre I, lemme 2-13.

Démonstration de la proposition.- On suppose que les hypothèses de la proposition sont satisfaites. Soit $X = \langle a,b \rangle$ un sous-espace de dimension 2 de U. On note $\mathcal{V}^k$ l'ensemble des sous-espaces de V de dimension k, $\mathcal{V}^k_a$ (resp. $\mathcal{V}^k_X$) l'ensemble des éléments de $\mathcal{V}^k$ qui contiennent a (resp. X), $\mathcal{H} = \mathcal{V}^{n-1}$, $\mathcal{H}_a = \mathcal{V}^{n-1}_a$, $\mathcal{H}_X = \mathcal{V}^{n-1}_X$.

1) G_a opère transitivement sur $\mathcal{H}_a$ et sur $\mathcal{H} - \mathcal{H}_a$:

Par hypothèse, G_a a deux orbites sur $V - \{0\}$, donc deux orbites sur $\mathcal{H}$ d'après le lemme 2.

2) $G_{a,X}$ opère transitivement sur $\mathcal{H} - \mathcal{H}_a$:

D'après la double transitivité de G, G_a opère transitivement sur $\mathcal{V}^2_a$. On a $|\mathcal{V}^2_a| = 2^{n-1} - 1$. D'après 1), G_a opère transitivement sur $\mathcal{H} - \mathcal{H}_a$ et $|\mathcal{H} - \mathcal{H}_a| = (2^n - 1) - (2^{n-1} - 1) = 2^{n-1}$. D'après le lemme 3, il en résulte que $G_{a,X}$ opère transitivement sur $\mathcal{H} - \mathcal{H}_a$.

3) $G_{a,b}$ opère transitivement sur $\mathcal{H}_a \cap (\mathcal{H} - \mathcal{H}_X)$:

Soient $H_1, H_2 \in \mathcal{H}_a \cap (\mathcal{H} - \mathcal{H}_X)$. Alors $b \notin H_1$ et $b \notin H_2$. D'après 2) il existe $g \in G_{b,X}$ tel que $g(H_1) = H_2$. Comme $g(H_1 \cap X) = H_2 \cap X$ et $H_1 \cap X = H_2 \cap X = \langle a \rangle$, g laisse fixe a, donc $g \in G_{a,b}$.

4) Le nombre d'orbites de $G_{a,b}$ sur $\mathcal{V}^3_X$ est égal au nombre d'orbites de $G_{a,b}$ sur $\mathcal{V}^2_a - \{X\}$:

Le nombre d'orbites de $G_{a,b}$ sur $\mathcal{V}^3_X$

= le nombre d'orbites de $G_{a,b}$ sur $\mathcal{H}_X$ (lemme 2b) appliqué à V/X)
= le nombre d'orbites de $G_{a,b}$ sur $\mathcal{H}_a$ moins 1 (d'après 3))
= le nombre d'orbites de $G_{a,b}$ sur $\mathcal{V}^2_a$ moins 1 (lemme 2 b) appliqué à $V/\langle a \rangle$)

5) $G_{a,b,U}$ opère transitivement sur l'ensemble des $Y \in \mathcal{V}^2_a - \{X\}$ tels que $Y \subset U$:

$Y \longmapsto Y + X$ est une application de $\mathcal{V}^2_a - \{X\}$ sur $\mathcal{V}^3_X$. De plus, si Y_1 et $Y_2 \in \mathcal{V}^2_a - \{X\}$ sont dans la même orbite sous $G_{a,b}$, il en est de même de $Y_1 + X$ et $Y_2 + X$. D'après 4), il en résulte que, réciproquement, si $Y_1 + X$ et $Y_2 + X$ sont dans la même orbite sous $G_{a,b}$, il en est de même de Y_1 et Y_2.
En particulier, si $Y_1, Y_2 \in \mathcal{V}^2_a - \{X\}$ sont tels que $Y_1 \subset U$, $Y_2 \subset U$, on a

$Y_1 + X = Y_2 + X = U$, donc il existe $g \in G_{a,b}$ tel que $g(Y_1) = Y_2$. Comme $g(Y_1 + X) = Y_2 + X$, on a $g \in G_{a,b,U}$.

6) Conclusion :

Soit (a,b,c) une base de U. D'après 5), il existe $g \in G_{a,b,U}$ tel que $g(< a,c >) = < a,c + b >$, donc $g(c) = c + b$ ou $g(c) = a + c + b$.

Donc, pour tout sous-espace X de dimension 2 de U, et pour tout $a \in X - \{0\}$, $\bar{G}_U$ contient l'une des deux transvections d'hyperplan X et de vecteur différent de 0 et de a. Ceci étant vrai pour tout $a \in X - \{0\}$, $\bar{G}_U$ contient au moins deux transvections non triviales d'hyperplan X, donc les 3 transvections non triviales d'hyperplan X.

Donc $\bar{G}_U$ contient toutes les transvections. Comme GL(U) est engendré par les transvections, on a $\bar{G}_U = GL(U)$.

Remarque : Plus généralement, si V est un espace vectoriel de dimension $n \geq 3$ sur un corps fini, si G est un groupe de collinéations opérant de manière doublement transitive sur l'espace projectif $\mathcal{P}(V)$ et si U est un sous-espace de dimension 3 de V, G induit un groupe de collinéations de $\mathcal{P}(U)$ qui contient PSL(U). On s'est limité ici au cas où le corps est $\mathbb{F}_2$ pour simplifier l'étape 6) de la démonstration.

Par contre, la proposition ne se généralise pas au cas où U est supposé de dimension 4. Il existe en effet un sous-groupe de $GL(4, \mathbb{F}_2)$ qui opère de manière doublement transitive sur $\mathbb{F}_2^4 - \{0\}$ et qui est isomorphe à $\mathcal{A}_7$.

§ 2.- RÉDUCTION A UN CAS PARTICULIER

Proposition.- Supposons qu'il existe un groupe de 2-rang ≥ 2 qui opère de manière doublement transitive sur ses involutions. Il existe alors un groupe G et un sous-groupe normal V de G tels que :

a) V *est abélien élémentaire d'ordre* $\neq 2$ *et* $Inv(G) = V^{\#}$.

b) $C_G(V)$ *est un 2-groupe.*

c) $G/C_G(V) \tilde{=} Aut(V)$.

On supposera dans ce paragraphe :

(E1) G est un groupe fini de 2-rang ≥ 2 qui opère de manière doublement transitive sur ses involutions

(E2) Tout groupe d'ordre pair $< |G|$ qui opère de manière doublement transitive sur ses involutions est de 2-rang 1.

1) Les involutions de G engendrent un sous-groupe normal abélien élémentaire V de G :

D'après l'hypothèse, il existe deux involutions distinctes de G qui commutent. D'après la double transitivité de G, les involutions de G commutent deux à deux. Donc $V = \mathrm{Inv}(G) \cup \{1\}$ est un sous-groupe abélien élémentaire normal de G.

2) Soit X un sous-groupe d'ordre impair de G. Alors $N_V(X) = C_V(X)$:

En effet, $[N_V(X), X] \subset V \cap X = 1$.

3) Soit U un sous-groupe d'ordre 4 de V. Alors $C_G(U)$ est un 2-groupe :

Soit P un p-Sylow de $C_G(U)$ pour un nombre premier $p \neq 2$. En considérant G comme un groupe opérant sur Inv(G), P est un p-Sylow du fixateur de deux points. D'après l'appendice II,(5), $N_G(P)$ opère donc de manière doublement transitive sur $C(P) \cap V^{\#}$. D'après 1) et 2), il en résulte que $N_G(P)$ (donc aussi $N_G(P)/P$) opère de manière doublement transitive sur ses involutions. De plus, $U \subset N_G(P)$, donc $N_G(P)/P$ est de 2-rang ≥ 2. D'après (E2) il en résulte que $|N_G(P)/P| \geq |G|$, donc $P = 1$.

4) Le cas où $|V| = 4$:

Dans ce cas, $|V^{\#}| = 3$ et $G/C_G(V) \tilde{=} \mathfrak{S}_3$. Si X est un 3-Sylow de G, on a donc $XC_G(V) \lhd G$ et $C_V(X) = 1$. D'après l'argument de Frattini, $G = C_G(V)N_G(X)$. Comme $|G/C_G(V)|$ est pair, $|N_G(X)|$ est pair, donc $N_V(X) \neq 1$. D'après 2), $C_V(X) \neq 1$, ce qui est absurde.

5) Le cas où $|V| \geq 8$:

Soit U un sous-groupe d'ordre 8 de V. D'après la proposition du § 1, $N_G(U)/C_G(U) \tilde{=} \mathrm{Aut}(U)$. D'après 3), il suffit donc de montrer que $U = V$.

Si $K = \mathbb{F}_8$, le groupe des applications $x \mapsto \lambda x^{2^i}$ $(\lambda \in K^*,\ 0 \leq i \leq 2)$ est un groupe de Frobenius d'ordre 7×3. Donc $N_G(U)/C_G(U)$ contient un groupe de Frobenius $F_1/C_G(U)$ d'ordre 7×3. Comme $C_G(U)$ est un 2-groupe, $C_G(U)$ a un complément F dans F_1 d'après le théorème de Zassenhaus. Soit $F = S \rtimes X$, $|S| = 7$, $|X| = 3$. D'après 3) on a $|C_V(X)| \leq 2$ et $|C_V(S)| \leq 2$. Comme $|U^{\#}| = 7$,

$C_U(X) \neq 1$ donc $|C_V(X)| = |C_U(X)| = 2$. Puisque X normalise $C_V(S)$ et $|C_V(S)| \leq 2$, X centralise $C_V(S)$, donc :

$$C_V(S) \subset C_V(X) \subset U.$$

D'après le théorème de l'appendice VII, V est engendré par $C_V(S)$ et les $C_V(X^s)$ pour $s \in S$, donc $V = U$.

§ 3.- LE CAS OU $C_G(V)$ EST ABÉLIEN

Pour démontrer le théorème E, il reste à montrer qu'il n'existe pas de groupe G qui satisfasse les conditions de la proposition du § 2. Il suffit de montrer :

Proposition 1.-Soient G un groupe fini et $V \lhd G$ *tels que :*

a) V *est abélien élémentaire d'ordre 8*

b) $C = C_G(V)$ *est un 2-groupe et* $\mathrm{Inv}(C) = V^{\#}$.

c) $G/C \tilde{=} \mathrm{Aut}(V)$.

Il existe alors une involution appartenant à $G - C$ *et* C *est abélien.*

J.L. Alperin a en fait déterminé les groupes G qui satisfont les hypothèses de cette proposition. Ces hypothèses lui étaient suggérées par l'étude des groupes simples de 2-rang 3.

Dans ce paragraphe, nous démontrerons :

Proposition 2.- Supposons qu'on ait les hypothèses de la proposition 1 et de plus que C *soit abélien. Il existe alors une involution appartenant à* $G - C$.

Si C est d'exposant 2^n, C est abélien de type $(2^n, 2^n, 2^n)$ car sinon $1 \neq C^{2^{n-1}} \subsetneq V$ et G/C ne pourrait opérer transitivement sur $V^{\#}$, contrairement à l'hypothèse c). Dans la suite de la démonstration, on suppose que $\mathrm{Inv}(G) = V^{\#}$ et que la proposition 2 est vraie pour les groupes d'ordre $< |G|$.

1) Pour $x \in G$, on note $\bar{x} + 1$ l'endomorphisme $c \longmapsto c^x c$ de C. Soit $x \in G - C$ tel que $x^2 \in C$. Pour tout $c \in C$, on a $(xc)^2 = x^2 c^x c \neq 1$ donc $x^2 \notin \mathrm{Im}(\bar{x} + 1)$.

2) Posons $C_k = C^{2^{n-k}}$ $(0 \le k \le n)$. Si $n \ge 2$, l'application $x \longmapsto x^2$ induit un isomorphisme de G/C-modules : $C_2/C_1 \to C_1 = V$. Donc G/V vérifie encore les hypothèses de la proposition 2. D'après l'hypothèse de récurrence, il existe $x \in G - C$ tel que $x^2 \in V^{\#}$. Ceci est aussi vrai si $n = 1$. Puisque $G/C \tilde{=} GL(3, \mathbb{F}_2)$ a une seule classe d'involutions, pour tout $x \in G - C$ tel que $x^2 \in C$ il existe $c \in C$ tel que $(xc)^2 \in V^{\#}$.

3) Soit (v_1, v_2, v_3) une base de V sur $\mathbb{F}_2$. Pour toute matrice inversible $(\alpha_{ij})_{1 \le i,j \le 3}$ à coefficients dans $\mathbb{F}_2$, il existe $x \in G$ tel que :

$$v_j^x = \prod_{i=1}^{3} v_i^{\alpha_{ij}} \qquad (1 \le j \le 3).$$

Soient s et $t \in G$ correspondant respectivement aux matrices :

$$s : \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \qquad t : \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

On a $s^2 \in C$ et $t^2 \in C$. D'après 2) on peut supposer que $s^2 \in V^{\#}$. Comme s^2 est un point fixe de s dans $V^{\#}$, on a $s^2 \in \langle v_1, v_2 \rangle$ et d'après 1) $s^2 \notin \langle v_2 \rangle$. En remplaçant éventuellement s par sv_3, on peut donc supposer que :

(3.1) $\qquad s^2 = v_1$.

4) Soient $a = st$ et $b = a^2$. Alors a et b correspondent respectivement aux matrices :

$$a : \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \qquad b : \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Posons $c_1 = b^2$. On a $c_1 \in C^{\#}$. Soit $m \ge 1$ tel que c_1 soit d'ordre 2^m. Puisque $c_1^{2^{m-1}}$ est un élément de $V^{\#}$ qui est centralisé par a, on a :

(4.1) $\qquad c_1^{2^{m-1}} = v_1$

Supposons $m = 1$. Alors $b^2 = c_1 = v_1 \in \mathrm{Im}(\bar{b} + 1)$, ce qui contredit 1). Donc

(4.2) $\qquad m \ge 2$.

5) Soit $u = c_1^s c_1$. Dans G/C, $\bar{s}^2 = \bar{t}^2 = 1$ et a centralise $c_1 = a^4$, donc

$$u^s = c_1 c_1^s = u, \quad u^t = c_1^{st} c_1^t = c_1 c_1^t, \quad u = (c_1 c_1^t)^t = c_1^t c_1 = u^t .$$

Supposons $u \neq 1$. Il existe $k \geq 0$ tel que $u^{2^k} \in V^{\#}$. Comme u^{2^k} est un élément de V centralisé par s et par t, on a $u^{2^k} \in \mathrm{Ker}(\bar{s}+1) \cap \mathrm{Ker}(\bar{t}+1) \cap V = \langle v_1 \rangle$ donc $u^{2^k} = v_1$. Mais $u = c_1^s c_1 \in \mathrm{Im}(\bar{s}+1)$, donc $v_1 \in \mathrm{Im}(\bar{s}+1)$. Comme $s^2 = v_1$, cela contredit 1), donc $u = 1$ et

$$(5.1) \qquad c_1^s = c_1^t = c_1^{-1}$$

6) Soit $c_3 \in C_m$ tel que $c_3^{2^{m-1}} = v_3$ et soit $c_2 = c_3^s c_3$. En élevant cette égalité à la puissance 2^{m-1} on voit que $c_2^{2^{m-1}} = v_2$, donc $C_m = \langle c_1 \rangle \times \langle c_2 \rangle \times \langle c_3 \rangle$. On a $c_2^s = (c_3^s c_3)^s = c_3 c_3^s = c_2$. Ainsi s opère sur C_m selon les formules :

$$(6.1) \qquad c_1^s = c_1^{-1}, \quad c_2^s = c_2, \quad c_3^s = c_2 c_3^{-1} .$$

Pour un endomorphisme u de C, posons $\mathrm{Im}_{C_m}(u) = \mathrm{Im}(u|_{C_m})$ et $\mathrm{Ker}_{C_m}(u) = \mathrm{Ker}(u|_{C_m})$. D'après (6.1), on a :

$$(6.2) \qquad \mathrm{Im}_{C_m}(\bar{s}+1) = \langle c_2 \rangle \quad \text{et} \quad \mathrm{Ker}_{C_m}(\bar{s}-1) = \langle c_2, v_1 \rangle .$$

7) Puisque G/C a une seule classe d'involutions, il résulte de (6.2) que si $\bar{x}$ est une involution de G/C :

$$(7.1) \qquad \mathrm{Im}_{C_m}(\bar{x}+1) \text{ est cyclique d'ordre } 2^m, \mathrm{Ker}_{C_m}(\bar{x}-1) \text{ est de type } (2^m,2)$$
$$\text{et } \mathrm{Im}_{C_m}(\bar{x}+1) \subset \mathrm{Ker}_{C_m}(\bar{x}-1).$$

En particulier, puisque $c_1^b = c_1$ et $v_2^b = v_2$, on a $\mathrm{Ker}_{C_m}(\bar{b}-1) = \langle c_1, v_2 \rangle$, et $\mathrm{Im}_{C_m}(\bar{b}+1)$ est un sous-groupe cyclique d'ordre 2^m de $\langle c_1, v_2 \rangle$, donc :

$$\mathrm{Im}_{C_m}(\bar{b}+1) = \langle c_1 \rangle \quad \text{ou} \quad \langle c_1 v_2 \rangle .$$

Mais d'après 1) $b^2 = c_1 \notin \mathrm{Im}(\bar{b}+1)$, donc :

$$(7.2) \qquad \mathrm{Im}_{C_m}(\bar{b}+1) = \langle c_1 v_2 \rangle .$$

8) Pour compléter la description de l'opération de $\langle \bar{s}, \bar{t} \rangle$ sur C_m, on doit

considérer c_2^t et c_3^t. Posons $d = c_2^t c_2$. Alors $d^{2^{m-1}} = v_2^t v_2 = v_1$, donc il existe des entiers k_1, k_2, k_3 définis modulo 2^{m-1} tels que :

$$d = c_1^{2k_1+1} c_2^{2k_2} c_3^{2k_3} .$$

Remarquons que toutes les relations de 5), 6), 7) restent valables si on remplace c_1 par $c_1^{2k_1+1}$ (on n'utilisera plus la relation $b^2 = c_1$). Après ce remplacement, on peut donc supposer $k_1 = 0$. Puisque $d \in \mathrm{Im}_{C_m}(\bar{t}+1)$, on a $\mathrm{Im}_{C_m}(\bar{t}+1) = \langle d \rangle$ d'après (7.1). Il existe donc un entier k tel que $c_3^t = c_3^{-1} d^k$. Ainsi :

$$(8.1) \qquad c_2^t = c_2^{-1} d, \quad c_3^t = c_3^{-1} d^k, \quad d = c_1 c_2^{2k_2} c_3^{2k_3} .$$

9) On écrit les relations entre k, k_2, k_3 déduites de $\bar{t}^2 = 1$, de $c_2^b c_2 \in \mathrm{Im}_{C_m}(\bar{b}+1) = \langle c_1 v_2 \rangle$ et de $c_3^b c_3 \in \mathrm{Im}_{C_m}(\bar{b}+1) = \langle c_1 v_2 \rangle$.

On a d'abord $d^t = (c_2^t c_2)^t = c_2 c_2^t = d$ ou :

$$c_1^{-1}(c_1 c_2^{2k_2-1} c_3^{2k_3})^{2k_2} (c_1^k c_2^{2kk_2} c_3^{2kk_3-1})^{2k_3} = c_1 c_2^{2k_2} c_3^{2k_3}$$

En identifiant les exposants de c_1 dans les deux membres, on a

$$-1 + 2k_2 + 2kk_3 \equiv 1 \pmod{2^m} \quad \text{ou :}$$

$$(9.1) \qquad k_2 + kk_3 - 1 \equiv 0 \pmod{2^{m-1}}.$$

Ensuite, les relations (5.1), (6.1), (8.1) permettent de calculer $c_2^b c_2$ et $c_3^b c_3$. On trouve que $c_2^b c_2 = c_1^{x_1} c_2^{x_2} c_3^{x_3}$ et $c_3^b c_3 = c_1^{y_1} c_2^{y_2} c_3^{y_3}$ où :

$$x_1 = 2k_2 + 2k_3(1-k)$$

$$x_2 = (2k_2 - 1)^2 + 2k_3(2k_2 - 1 - 2kk_2) + 1$$

$$y_1 = -k + (1-k)(2k_2 + 2k_3 - 2kk_3 + 1)$$

$$y_2 = (2k_2 - 1 - 2kk_2)(2k_2 + 2k_3 - 2kk_3)$$

Comme $c_2^b c_2 \in \langle c_1 v_2 \rangle$ mais x_1 est pair, on a $x_2 \equiv 0 \pmod{2^m}$. De plus, d'après

(9.1) on a $2kk_3 \equiv 2(1 - k_2) \pmod{2^m}$, d'où :

$$(2k_2 - 1)^2 + 2k_3(2k_2 - 1) + 4(k_2 - 1)k_2 + 1 \equiv 0 \pmod{2^m}$$

ou $2(2k_2 - 1)^2 + 2k_3(2k_2 - 1) \equiv 0 \pmod{2^m}$, donc :

(9.2) $\quad k_3 \equiv 1 - 2k_2 \pmod{2^{m-1}}$.

On a $y_1 \equiv 1 - 2k \equiv 1 \pmod 2$. Comme $c_3^b c_3 \in \langle c_1 v_2 \rangle$ il en résulte que $y_2 \equiv 2^{m-1} \pmod{2^m}$, donc puisque $m \geq 2$:

(9.3) $\quad k_2 + k_3 - kk_3 \equiv 2^{m-2} \pmod{2^{m-1}}$.

Mais d'après (9.1) et (9.2), on a :

$$k_2 + k_3 - kk_3 \equiv k_2 + (1 - 2k_2) + (k_2 - 1) \equiv 0 \pmod{2^{m-1}} .$$

Donc (9.3) est impossible et on a la contradiction voulue.

§ 4.- LE CAS OÙ $C_G(V)$ N'EST PAS ABÉLIEN

Pour finir la démonstration de la proposition 1 du § 3, il reste à démontrer que si G satisfait les hypothèses de cette proposition, alors $C = C_G(V)$ est abélien. Supposons donc que G soit un groupe qui satisfasse les hypothèses de la proposition 1 du § 3, mais que C ne soit pas abélien. Alors un sous-groupe d'ordre 7 de G opère régulièrement sur $V^\# = \mathrm{Inv}(C)$, donc C est un 2-groupe de Suzuki avec $\Omega_1(C) = V$.

On sait que $G/C \tilde{=} \mathrm{Aut}(V) \tilde{=} GL(3, \mathbb{F}_2)$ est un groupe simple, et $C_G(C) \subset C_G(V) = C$ donc Aut(C) n'est pas résoluble.

D'après la proposition 1 de l'appendice VIII, C n'est donc pas un 2-groupe de Suzuki de type $A(3,\phi)$ (rappelons que pour un 2-groupe de Suzuki de type $A(n,\phi)$, ϕ est un automorphisme d'ordre impair $\neq 1$ de $\mathbb{F}_{2^n}$). D'après la structure des 2-groupes de Suzuki, C/V est alors un $\mathbb{F}_2$-espace vectoriel de dimension 6. De plus $G/C \tilde{=} GL(3, \mathbb{F}_2)$ opère naturellement sur C/V.

Si C/V avait un sous-$\mathbb{F}_2[G/C]$-module de dimension 1 sur $\mathbb{F}_2$, il existerait $x \in C - V$ tel que $\bar{x} \in C/V$ soit invariant par G/C. Alors $x^2 \in V^\#$ serait invariant par $G/C \tilde{=} \mathrm{Aut}(V)$, ce qui est absurde.

D'après l'appendice IX, toute $\mathbb{F}_2$-représentation irréductible de $GL(3, \mathbb{F}_2)$ est de degré 1, 3 ou 8. Il en résulte que C/V a un sous-$\mathbb{F}_2[G/C]$-module simple de dimension 3 sur $\mathbb{F}_2$.

Soit C_1/V un tel sous-module. Alors C_1 est un 2-groupe de type $A(3,\phi)$ où ϕ est d'ordre impair. Comme $C_G(C_1) \subset C_G(V) = C$ et $G/C \tilde{=} GL(3, \mathbb{F}_2)$, $Aut(C_1)$ n'est pas résoluble. D'après la proposition 1 de l'appendice VIII, on a donc $\phi = 1$. D'après la description des 2-groupes de Suzuki, il en résulte que C est de type $B(3,1,\varepsilon)$ ou $C(3,\varepsilon)$, et Aut(C) n'est pas résoluble. De plus, dans le deuxième cas, G/C laisse stable C_1 qui est le sous-groupe noté P_1 dans la proposition 4 de l'appendice VIII. Cela n'est pas possible d'après les propositions 3 et 4 de l'appendice VIII.

APPENDICE I

LEMMES SUR L'OPÉRATION D'UN ÉLÉMENT D'ORDRE d DANS UN GROUPE

Hypothèses : M est un groupe fini, d un nombre premier, t un élément d'ordre d de M, X un d'-sous-groupe de M normalisé par t. On pose $V = C_X(t)$ et $K = \{[t,x]/x \in X\}$.

(1) a) On a $|t^X| = |K| = |X : V|$.

b) Supposons $d = 2$. Alors $K = \{x \in X/x^t = x^{-1}\}$ et l'application $(x,y) \longmapsto xy$ (resp. $(x,y) \longmapsto yx$) est une bijection de $V \times K$ sur X.

Soit p un nombre premier.

(2) Il existe un p-Sylow de X normalisé par t, deux p-Sylow de X normalisés par t sont conjugués par un élément de V, et tout p-sous-groupe de X normalisé par t est contenu dans un p-Sylow de X normalisé par t.

(3) Soit Y un d'-sous-groupe de M.

a) Si P est un p-Sylow de $\bigcap_{u \in <t>} Y^u$ normalisé par t, on a $|C_P(t)| = |C_Y(t)|_p$.

b) Si P est un p-Sylow de Y normalisé par t, on a $|t^P| = |t^Y|_p$.

c) Soit P un p-sous-groupe de Y normalisé par t tel que $|t^P| \geq |t^Y|_p$. Alors P est contenu dans un p-Sylow de Y normalisé par t et on a $|t^P| = |t^Y|_p$ et $|\bigcap_{u \in <t>} Y^u|_p = |Y|_p$.

d) Les conditions suivantes sont équivalentes : (i) $|\bigcap_{u \in <t>} Y^u|_p = |Y|_p$. (ii) Y a un p-Sylow normalisé par t. (iii) Il existe un p-sous-groupe P de Y normalisé par t tel que $|t^P| \geq |t^Y|_p$.

(4) V et t normalisent K, $<K> \lhd X$, $X = <K>V$, $K = \{[t,x]/x \in <K>\}$ et $|<K>| = |K| . |V \cap <K>|$.

(5) Supposons X résoluble. Alors :

a) $|\langle K\rangle|$ et $|K|$ ont les mêmes diviseurs premiers.

b) Si $(|K|,|F(V)|) = 1$, alors K est un sous-groupe de X, complément normal de V.

c) Soit U un p-sous-groupe de V. Si $C_K(U) = 1$, alors $N_X(U) \subset V$. Si U opère sans point fixe sur K (c'est-à-dire $k^u \neq k$ pour $u \in U - \{1\}$ et $k \in K - \{1\}$), alors U est cyclique ou quaternionien généralisé.

d) Soient $E \lhd X$ et P un p-Sylow de E tel que $P \subset V$ et $C_K(P) = 1$. Alors $K \subset [E,E]$ et $E^t = E$.

Démonstrations :

(1) On a $|t^X| = |X : V|$ et l'application $u \longmapsto t^{-1}u$ est une bijection de t^X sur K, d'où a). Supposons $d = 2$. Soit $K_1 = \{x \in X \mid x^t = x^{-1}\}$. On vérifie que $K \subset K_1$. Soient $x_1, x_2 \in V$ et $y_1, y_2 \in K_1$ tels que $x_1y_1 = x_2y_2$. Alors $y_1^2 = ((x_1y_1)^t)^{-1}(x_1y_1) = ((x_2y_2)^t)^{-1}(x_2y_2) = y_2^2$, donc $|X|$ étant impair, $y_1 = y_2$, d'où $x_1 = x_2$. L'application $(x,y) \longmapsto xy$ de $V \times K_1$ dans X est donc injective. D'après a) on a donc $K = K_1$ et l'application est aussi surjective. On procède de même pour l'autre application.

(2) Le nombre des p-Sylow de X est premier à d, donc il existe un p-Sylow de X normalisé par t. Soient P et Q deux p-Sylow de X normalisés par t, et $x \in X$ tel que $Q^x = P$; t et t^x appartiennent à $N(P) \cap (X \langle t \rangle) = N_X(P)\langle t \rangle$. D'après le théorème de Sylow, il existe donc $y \in N_X(P)$ tel que $t^{xy} \in \langle t \rangle$. On a $[xy,t] \in \langle t \rangle \cap X = 1$, donc $xy \in V$ et $Q^{xy} = P$. Soit enfin P maximal parmi les p-sous-groupes de X normalisés par t. Il existe un p-Sylow de $N_X(P)$ normalisé par t, donc P est un p-Sylow de $N_X(P)$, donc de X.

(3) a) Soit Q un p-Sylow de $C_Y(t)$ tel que $C_P(t) \subset Q$. On a $Q \subset \bigcap_{u \in \langle t \rangle} Y^u$ donc Q est contenu dans un p-Sylow P' de $\bigcap_{u \in \langle t \rangle} Y^u$ normalisé par t. Il existe $z \in C(t)$ tel que $P' = P^z$. On a donc $|C_{P'}(t)| = |(C_P(t))^z| = |C_P(t)|$. Puisque $C_P(t) \subset Q \subset C_{P'}(t)$, il en résulte que $C_P(t) = Q$ et $|C_P(t)| = |C_Y(t)|_p$.

b) On a $|P| = |Y|_p = |t^P||C_P(t)|$ et $|Y| = |t^Y||C_Y(t)|$. Or P est un p-Sylow de $\bigcap_{u \in \langle t \rangle} Y^u$, donc d'après a) $|C_P(t)| = |C_Y(t)|_p$. Il résulte alors des égalités ci-dessus que $|t^P| = |t^Y|_p$.

c) On a $P \subset \bigcap_{u \in <t>} Y^u$ donc P est contenu dans un p-Sylow Q de $\bigcap_{u \in <t>} Y^u$ normalisé par t. Par hypothèse, $|t^Y|_p \leq |t^P| \leq |t^Q|$, d'où $|Y|_p = |t^Y|_p |C_Y(t)|_p \leq$ $\leq |t^Q||C_Y(t)|_p$. D'après a), on a $|t^Q||C_Y(t)|_p = |t^Q||C_Q(t)| = |Q|$, donc $|Y|_p \leq |Q|$. Donc Q est un p-Sylow de Y et les inégalités ci-dessus sont des égalités.

d) (i) $\Longrightarrow$ (ii) d'après (2), (ii) $\Longrightarrow$ (iii) d'après b), (iii) $\Longrightarrow$ (i) d'après c).

(4) Il est clair que V et t normalisent K. On a $<K> \lhd X$ d'après l'identité $[t,x]^y = [t,y]^{-1}[t,xy]$ $(x,y \in X)$; t centralise $X/<K>$ et X est un d'-groupe d'où $X = <K>V$. Soit $K_1 = \{[t,x]/x \in <K>\}$. D'après (1)a), $|<K>| = |K_1||V \cap <K>|$, donc $|X| = |<K>||V|/|V \cap <K>| = |K_1||V|$, d'où $|K_1| = |K|$. Comme $K_1 \subset K$, on a $K_1 = K$.

(5) a) Soit p un nombre premier. Si $p \mid |K|$, alors $p \mid |<K>|$ d'après (4). Réciproquement, supposons que $p \nmid |K|$. D'après le théorème de Hall, le nombre des p'-groupes de Hall de X est $\neq 0$ et premier à d. Il existe donc un p'-groupe de Hall R de X tel que $R^t = R$. Pour montrer que $p \nmid |<K>|$, il suffit de montrer que $K \subset R$. Soit $K_1 = \{[t,x]/x \in R\}$. D'après (1), $|R| = |R \cap V| \,.|K_1|$, donc $|X|_p |R \cap V| \,.|K_1| = |X| = |V| \,.|K|$. Mais $|X|_p$ $|R \cap V|$ divise $|V|$ car $p \nmid |K|$, et on a $K_1 \subset K$. Il en résulte que $|V| = |X|_p |R \cap V|$ et $|K_1| = |K|$, d'où $K = K_1 \subset R$.

b) D'après a), $(|<K>|, |F(V)|) = 1$, donc $[V \cap <K>, F(V)] \subset <K> \cap F(V) = 1$. D'après le théorème de Fitting, $V \cap <K> \subset F(V)$, d'où $V \cap <K> = 1$. D'après (4), on a donc $<K> = K$ et $X = KV$.

c) Supposons $C_K(U) = 1$. D'après a) et la décomposition de K en réunion d'orbites sous U, $<K>$ est un p'-groupe. On a donc $[N_K(U), U] \subset U \cap <K> = 1$, donc $N_K(U) = C_K(U) = 1$, et pour $x \in N_X(U)$, $[t,x] \in N_X(U) \cap K = 1$, ce qui prouve que t centralise $N_X(U)$.

Supposons que U opère sans point fixe sur K et que $U \neq 1$. Alors $<K>$ est un p'-groupe comme ci-dessus. Soit q un diviseur premier de $|K|$ et Q un q-Sylow de $<K>$ normalisé par U. Alors Q n'est pas inclus dans V car $|<K>| = |K| \,.|<K> \cap V|$. Donc $N_Q(V \cap Q) \supsetneq V \cap Q$. D'après la première assertion de c), pour $u \in U^\#$ on a $C_X(u) \subset V$, donc U opère sans point fixe sur $N_Q(V \cap Q)/(V \cap Q)$. Cela prouve que U est cyclique ou quaternionien généralisé [Huppert, chapitre V, th. 8.7].

d) D'après l'argument de Frattini, $X = EN_X(P)$. D'après c) $N_X(P) \subset V$, donc t centralise X/E, donc $K \subset E$. Puisque t centralise $X/\langle K \rangle$ et $\langle K \rangle \subset E$, on a $E^t = E$. D'après (4), $K = \{[t,x]/x \in E\}$ et on a $[E,E]P \lhd E$ car $E/[E,E]$ est abélien. En répétant l'argument ci-dessus avec E à la place de X et $[E,E]P$ à la place de E, on voit que t centralise $E/[E,E]$, donc $K \subset [E,E]$.

APPENDICE II

LEMMES DE DOUBLE TRANSITIVITÉ

Hypothèses : X est un groupe fini opérant sur un ensemble fini E, p est un nombre premier, a, b sont des éléments distincts de E, $H = X_a$, $D = X_a \cap X_b$. Pour $Y \subset X$, on note E_Y l'ensemble des points fixes de Y dans E.

(1) Soit P un p-sous-groupe de X tel que $E_P = \{a,b\}$. Il existe alors un p-Sylow Q de H tel que $P \subset Q$ et $E_Q = \{a,b\}$. Si de plus $p > 2$, alors Q est un p-Sylow de X.

(2) Supposons que $\{a,b\}$ soit l'ensemble des points fixes d'un p-sous-groupe de X et qu'il existe $x \in X$ tel que $b = a^x$. Il existe alors un élément de X qui échange a et b.

(3) Supposons que pour tout $c \in E - \{a\}$, $\{a,c\}$ soit l'ensemble des points fixes d'un p-sous-groupe de X, et que X ne laisse pas a fixe. Alors X opère de manière 2-transitive sur E.

(4) Si $|E| \geq 3$ et si toute partie de cardinal 2 de E est l'ensemble des points fixes d'au moins un p-sous-groupe de X, alors X opère de manière 2-transitive sur E.

Pour (5), (6), (7), on suppose de plus que X opère de manière 2-transitive sur E.

(5) Si P est un p-Sylow de D, alors $N_X(P)$ est 2-transitif sur E_P.

(6) Soit P un élément maximal de l'ensemble des p-sous-groupes de H qui fixent au moins 3 points. Alors P est maximal dans l'ensemble des p-sous-groupes de X qui fixent au moins 3 points, et $N_X(P)$ est 2-transitif sur E_P.

(7) On suppose que D a un complément normal Q dans H. Si Y est un sous-groupe de D qui fixe au moins 3 points de E, $C_Q(Y)$ opère de manière régulière sur $E_Y - \{a\}$, $C_H(Y) = C_Q(Y) \rtimes C_D(Y)$ et $C_X(Y)$ opère de manière 2-transitive sur E_Y.

Démonstrations :

(1) Soit Q un p-Sylow de D tel que $P \subset Q$. On a $\{a,b\} \subset E_D \subset E_Q \subset E_P = \{a,b\}$ donc $E_Q = \{a,b\}$. $N_H(Q)$ opère sur l'ensemble $\{a,b\}$ des points fixes de Q et laisse fixe a, donc $N_H(Q) \subset D$. Alors Q est un p-Sylow de $N_H(Q)$, donc de H. Si $p > 2$, N(Q) opère sur $\{a,b\}$ donc $|N(Q) : N(Q) \cap D| \leq 2$, donc Q est un p-Sylow de N(Q), donc de X.

(2) Soient Q un p-Sylow de H tel que $E_Q = \{a,b\}$ et $x \in X$ tel que $b = a^x$. Alors Q et Q^x sont des p-Sylow de X_b, et il existe donc $y \in X_b$ tel que $Q^{xy} = Q$. Puisque xy normalise Q, xy laisse stable $\{a,b\} = E_Q$ et on $a^{xy} = b^y = b$ d'où $b^{xy} = a$.

(3) Soit $c \in E - \{a\}$. Soient Q et R des p-Sylow de H tels que $E_Q = \{a,b\}$ et $E_R = \{a,c\}$ (cf. (1)). Il existe $x \in H$ tel que $Q^x = R$, d'où $\{a,b\}^x = \{a,c\}$ et $b^x = c$. Donc H est transitif sur $E - \{a\}$ Comme X ne laisse pas a fixe, X est 2-transitif sur E.

(4) résulte immédiatement de (3).

(5) Soient $c,d \in E_P$, $c \neq d$. Soit $x \in X$ tel que $a^x = c$, $b^x = d$. D'après la 2-transitivité de X, P et P^x sont des p-Sylow de $X_c \cap X_d$. Soit $y \in X_c \cap X_d$ tel que $P^{xy} = P$. Alors $xy \in N_X(P)$, $a^{xy} = c$ et $b^{xy} = d$.

(6) Si P est un p-Sylow de D, $N_X(P)$ est 2-transitif sur E_P d'après (5). Supposons que P ne soit pas un p-Sylow de D. Alors pour $c \in E_P - \{a\}$, P n'est pas un p-Sylow de $H \cap X_c$, d'après la 2-transitivité de X, donc un p-Sylow de $N_X(P) \cap H \cap X_c$ n'a que 2 points fixes. Soient $c,d \in E_P - \{a\}$, $c \neq d$. Alors P n'est pas un p-Sylow de $X_c \cap X_d$, donc si Q est un p-Sylow de $N(P) \cap X_c \cap X_d$ contenant P, on a $P \subsetneq Q$. D'après la maximalité de P, $Q \not\subset H$, donc N(P) ne laisse pas a fixe. D'après (3), N(P) opère donc de manière 2-transitive sur E_P.

La transitivité de N(P) sur E_P entraîne que P est maximal parmi les p-sous-groupes de X qui fixent 3 points. Soit en effet Q un p-sous-groupe de X qui fixe 3 points, tel que $P \subset Q$. Si $c \in E_Q$, alors $c \in E_P$ et il existe $x \in N(P)$ tel que $a = c^x$. Alors $P \subset Q^x \subset H$, d'où $P = Q^x$ et $P = Q$.

(7) D'après l'hypothèse, Q opère de manière régulière sur $E - \{a\}$. Soit

$c \in E_Y - \{a\}$. Il existe $x \in Q$ tel que $b^x = c$. Si $y \in Y$, on a $c^y = c$ et $b^x = (b^x)^y = (b^y)^{y^{-1}xy} = b^{y^{-1}xy}$, d'où $x = y^{-1}xy$ et $x \in C_Q(Y)$. Cela prouve que $C_Q(Y)$ opère de manière transitive, donc régulière sur $E_Y - \{a\}$ et que $C_H(Y) = C_Q(Y) \rtimes C_D(Y)$. L'hypothèse étant indépendante de $a, b \in E_Y$ et puisque $|E_Y| \geq 3$, $C_X(Y)$ opère de manière doublement transitive sur E_Y.

APPENDICE III

SUR LES GROUPES DE 2-RANG 1

Hypothèses : F est un groupe fini opérant transitivement sur un ensemble fini A, F est de 2-rang 1, $H = F_a$ (pour un $a \in A$) est un groupe de Bender propre de F, et H est un sous-groupe maximal de F ; $t \in \mathrm{Inv}(F - H)$ et $D = H \cap H^t$.

(1) On a $H \cap H^t = N \cap H(t)$.

On suppose maintenant de plus que F opère fidèlement sur A.

(2) Il existe un nombre premier f et un f-groupe abélien élémentaire Q tels que $F = Q \rtimes H$ et $C_H(Q) = 1$.

(3) H a une seule involution u et D est centralisé par u et par t.

(4) Si u, v sont des involutions distinctes de F, $uv \in Q$ et uv est d'ordre f. L'ensemble des éléments d'ordre impair de F inversés par u est Q.

(5) Supposons que F soir 2-transitif sur A, et soit p un nombre premier tel que $p \nmid |D|$. Alors un p-Sylow R de H opère sans point fixe sur Q et si p est impair, R est cyclique.

Démonstrations :

(1) On peut supposer que F opère fidèlement sur A car H, H^t et H(t) contiennent le noyau de l'opération. Alors d'après (3), D centralise t donc $D \subset H(t)$ et t centralise $H \cap H(t)$ donc $H \cap H(t) \subset H^t$.

(2) Soit $u \in \mathrm{Inv}(H)$. D'après le théorème de Brauer-Suzuki, $F = O_{2'}(F)C_F(u)$ et puisque $C_F(u) \subset H$, $F = O_{2'}(F)H$. Puisque $O_{2'}(F)$ est résoluble $\neq 1$, il a un sous-groupe caractéristique abélien élémentaire $Q \neq 1$, par exemple $\Omega_1 Z O_f(O_{2'}(F))$ pour f convenable. Alors $Q \lhd F$. Si $Q \subset H$, alors $Q \subset \bigcap_{x \in F} H^x = 1$, ce qui est absurde. Donc $Q \not\subset H$ et $F = HQ$; Q est donc transitif sur A. Si $x \in C_H(Q)$, x laisse fixe a^y

pour $y \in Q$, donc $x \neq 1$. On a donc $C_H(Q) = 1$, et en particulier $H \cap Q = 1$.

(3) Si $u,v \in \mathrm{Inv}(H)$, on $C_F(u) \subset H$ et $C_F(v) \subset H$, donc $C_Q(u) = C_Q(v) = 1$. Les éléments de Q sont inversés par u et v (appendice I,(1)), donc $uv \in C_H(Q)$, d'où $uv = 1$ et $u = v$.

On a $|\mathrm{Inv}(H)| = |u^D| = |t^D| = 1$ (chapitre I, § 2, prop. 2) donc u et t centralisent D.

(4) D'après (2) et (3), F/Q n'a qu'une involution, donc si u et v sont des involutions de F, $uv \in Q$. On a vu dans (3) que u inverse les éléments de Q. Si x est un élément $\neq u$ de F inversé par u, on a $x = u(ux) \in Q$.

(5) Si $x \in R^{\#}$, x n'est pas conjugué à un élément de D, donc le nombre de points fixes de x est ≤ 1. Donc l'ensemble des points fixes de x est $\{a\}$. Il en résulte que $C_F(x) \subset H$ d'où $C_Q(x) = 1$.

APPENDICE IV

UN THÉORÈME DE THOMPSON ET BENDER

Si M est un groupe résoluble, on sait que M vérifie la propriété suivante : soit Q le sous-groupe de M contenant $O_{p'}(M)$ tel que $Q/O_{p'}(M) = O_p(M/O_{p'}(M))$ (p étant un nombre premier). On a $C_G(Q/O_{p'}(M)) \subset Q$ [Huppert, chapitre VI, lemme 6-5]. Un groupe fini qui vérifie cette propriété est dit p-contraint.

Nous allons démontrer le théorème suivant, qui généralise le lemme 1 du chapitre I, § 6 :

Théorème.- Soit p *un nombre premier impair. Soient* M *un groupe fini p-contraint et* P *un* p*-sous-groupe de* M *tel que tout élément d'ordre* p *de* $C_M(P)$ *soit dans* P. *Si* X *est un* p'*-sous-groupe de* M *normalisé par* P, *alors* $X \subset O_{p'}(M)$.

Remarque : Si P est un p-Sylow de $PC_M(P)$, P contient tout p-élément de $C_M(P)$, car $P \lhd PC_M(P)$.

Bender a démontré ce théorème dans "Uber den grössten p'-Normalteiler in p-auflösbaren Gruppen" [Arch. Math. 18 (1967), p. 15] . Thompson en avait auparavant démontré une forme légèrement plus faible dans "Fixed points of p-groups acting on p-groups" [Math. Z. 86 (1964), p. 12].

Lemme 1.- Soit X *un* p'*-groupe opérant sur un* p*-groupe* Q.

a) On a $[Q,X] = [[Q,X],X]$.

b) Si Q *est abélien, on a* $Q = [Q,X] \times C_Q(X)$.

Pour la démonstration, voir Huppert, chapitre III, 13-3 et 13-4. Comparer b) à l'appendice I,(1).

Lemme 2.- Soit p *un nombre premier. Soient* U *un groupe fini et* X *un* p'*-sous-groupe normal de* U. *On suppose que* U *opère sur un* p*-groupe* Q *de manière que* X *ne centralise pas* Q, *mais centralise tout sous-groupe propre de* Q *normalisé par* U. *Alors* Q/Z(Q) *est abélien élémentaire.*

Puisque U normalise Q et X, [Q,X] est un sous-groupe de Q normalisé par U. Comme X ne centralise pas Q, on a d'après le lemme 1 $[[Q,X],X] = [Q,X] \neq 1$. Donc X ne centralise pas [Q,X]. Il résulte donc de l'hypothèse que $[Q,X] = Q$.

Soit $\Phi(Q)$ le groupe de Frattini de Q. On a $Q \neq 1$, donc $\Phi(Q) \subsetneq Q$ et $\Phi(Q)$ est normalisé par U. Il résulte de l'hypothèse que $[X,\Phi(Q)] = 1$. On a alors $[[X,\Phi(Q)],Q] = 1$ et $[[\Phi(Q),Q],X] \subset [\Phi(Q),X] = 1$. D'après le lemme des 3 sous-groupes [Huppert, chapitre III, 1-10], on en déduit que $[[Q,X],\Phi(Q)] = 1$. Mais on a vu ci-dessus que $[Q,X] = Q$. Donc $[Q,\Phi(Q)] = 1$, c'est-à-dire $\Phi(Q) \subset Z(Q)$.

Lemme 3 (Baer).- *Soit* Q *un groupe fini d'ordre impair tel que* Q/Z(Q) *soit abélien. Il existe un groupe* Q^+ *ayant même ensemble sous-jacent que* Q, *et tel que :*

a) Q^+ *est un groupe abélien.*

b) *Si* $x \in Q$, *l'ordre de* x *dans* Q *est égal à l'ordre de* x *dans* Q^+.

c) *Tout automorphisme de* Q *est un automorphisme de* Q^+.

Remarquons d'abord que l'application $x \longmapsto x^2$ de Q dans Q est surjective, donc bijective, car Q est d'ordre fini impair. On notera $x \mapsto x^{1/2}$ l'application réciproque.

Pour $a,b \in Q$, posons $a + b = ab[b,a]^{1/2}$, et soit Q^+ l'ensemble sous-jacent à Q muni de la loi +. Montrons que Q^+ est un groupe abélien. On a :

$$a + b = ab[b,a]^{1/2} = ba[a,b][b,a]^{1/2} = ba[a,b][a,b]^{-1/2} = ba[a,b]^{1/2} = b + a$$

Puis, en posant $0 = 1$ et $-a = a^{-1}$, $a + 0 = a.1[1,a]^{1/2} = a$, $a + (-a) = aa^{-1}[a^{-1},a]^{1/2} = 1 = 0$. Il reste à vérifier l'associativité de +. On sait que $x \longmapsto [a,x]$ est un homorphisme $Q \to Z(Q)$ car $[Q,Q] \subset Z(Q)$ [Huppert, chapitre III, lemme 1-2]. On a donc :

$$(a + b) + c = ab[b,a]^{1/2}c[c,ab[b,a]^{1/2}]^{1/2} = abc[b,a]^{1/2}[c,a]^{1/2}[c,b]^{1/2}$$

$$a + (b + c) = abc[c,b]^{1/2}[bc[c,b]^{1/2},a]^{1/2} = abc[c,b]^{1/2}[b,a]^{1/2}[c,a]^{1/2}$$

et la loi + est bien associative. Donc Q^+ est un groupe abélien.

Pour l'assertion b), on voit par récurrence sur $n \in \mathbb{N}$ que $na = a^n$ pour $a \in Q$, et l'assertion c) est évidente d'après la définition de la loi +.

Lemme 4. *Soit* p *un nombre premier impair. Soient* X *un* p'*-groupe et* P *un* p*-groupe opérant sur* X. *On suppose que* $U = X \rtimes P$ *opère sur un* p*-groupe* Q. *Si* X *centralise* $\Omega_1 C_Q(P)$, *alors* X *centralise* Q.

(Remarque : si P = 1, on retrouve ainsi un théorème de Blackburn).

Supposons que X ne centralise pas Q. En raisonnant par récurrence sur $|Q|$, on peut supposer que tout sous-groupe propre de Q normalisé par U est centralisé par X. Alors d'après le lemme 2, $Q/Z(Q)$ est abélien. Comme p est impair, on peut associer à Q un groupe abélien Q^+ vérifiant les assertions du lemme 3, et U opère sur Q^+. D'après le lemme 1 b), on a $Q^+ = [Q^+,X] \times C_{Q^+}(X)$. $C_{Q^+}(X)$ et $C_Q(X)$ ont même ensemble sous-jacent, donc $C_{Q^+}(X) \neq Q^+$, d'où $[Q^+,X] \neq 0$. Comme P opère sur le p-groupe non trivial $[Q^+,X]$, d'après une propriété élémentaire des p-groupes, il existe un élément a d'ordre p de $[Q^+,X]$ qui est centralisé par P. Comme $Q^+ = [Q^+,X] \times C_{Q^+}(X)$, $a \notin C_{Q^+}(X)$, et d'après le lemme 3 b), a est d'ordre p dans Q. Donc X ne centralise pas $\Omega_1 C_Q(P)$.

Démonstration du théorème.- Posons $\bar{M} = M/O_{p'}(M)$ et soit $a \mapsto \bar{a}$ l'homomorphisme canonique : $M \to \bar{M}$. Montrons que l'hypothèse du lemme 4 est vérifiée pour $U = XP$ opérant sur $Q = O_p(\bar{M})$. Soit $\bar{a}$ un élément d'ordre p de Q qui est centralisé par P. Comme $|P|$ et $|O_{p'}(M)|$ sont premiers entre eux, on a $C_{\bar{M}}(P) = \overline{C_M(P)}$ et on peut prendre un représentant a de $\bar{a}$ tel que $a \in C_M(P)$. Puis, en remplaçant a par sa p-composante, on peut supposer de plus que a est d'ordre p. Alors d'après l'hypothèse du théorème, on a $a \in P$ et $\bar{a} \in \bar{P} \cap O_p(\bar{M})$. Mais $[\bar{P} \cap O_p(\bar{M}), \bar{X}] \subset \bar{X} \cap O_p(\bar{M}) = 1$ car P normalise X et $O_p(\bar{M}) \lhd \bar{M}$. Donc X centralise $\bar{a}$. D'après le lemme 4, X centralise donc $O_p(\bar{M})$. D'après la p-contrainte de M, on a $\bar{X} \subset O_p(\bar{M})$, donc, $\bar{X}$ étant un p'-groupe, $\bar{X} = 1$, c'est-à-dire $X \subset O_{p'}(M)$.

APPENDICE V

UN LEMME SUR CERTAINS GROUPES D'AUTOMORPHISMES D'UN GROUPE ABÉLIEN ÉLÉMENTAIRE

Soit U *un groupe opérant fidèlement sur un groupe abélien élémentaire* Q *d'ordre* d^n (d *premier*). *Soit* T *un sous-groupe normal cyclique de* U *qui opère irréductiblement sur* Q.

a) *Le sous-anneau* $F = \mathbb{F}_d[T]$ *de* End(Q) *est un corps de cardinal* d^n *et* Q *est un* F*-espace vectoriel de dimension 1.*

b) U *est un groupe d'applications semi-linéaires de cet espace vectoriel dans lui-même.*

c) *Si* $s \in Q^{\#}$, $C_U(s)$ *est isomorphe à un groupe d'automorphismes du corps* F.

d) *Soit* P *un sous-groupe de* U. *On suppose que* $P \neq 1$ *et que pour tout sous-groupe* $P_1 \neq 1$ *de* P, *on a* $|C_Q(P_1)| = d$. *Alors* $|P| = p$ *est premier,* $|Q| = d^p$ *et pour* $s \in C_Q(P)^{\#}$, *on a* $C_U(s) = P$.

Notons additivement la loi de composition de Q et supposons que U opère à gauche sur Q.

a) D'après le lemme de Schur, $F_1 = \mathrm{End}_T(Q)$ est un corps fini et T étant commutatif, on a $F = \mathbb{F}_d[T] \subset F_1$. Donc F étant un sous-anneau d'un corps fini est un corps. Or Q est un F-module simple, donc un F-espace vectoriel de dimension 1, et $|F| = |Q|$.

b) et c). Soit $u \in U$. Alors u est un automorphisme de Q pour sa structure additive. Soit $s \in Q^{\#}$ et pour $\lambda \in F$, soit $\sigma(\lambda)$ l'élément de F tel que $u(\lambda s) = \sigma(\lambda)u(s)$. On a $\sigma(\lambda + \mu) = (\lambda) + \sigma(\mu)$ pour $\lambda, \mu \in F$. Puisque U opère sur $T \ltimes Q$, on a pour $\lambda \in T$ et $\mu \in F$, $u(\lambda\, \mu\, s) = u\, \lambda\, u^{-1}.u(\mu\, s) = u\, \lambda\, u^{-1}\sigma(\mu)u(s)$. En particulier, pour $\mu = 1$, $u(\lambda\, s) = u\, \lambda\, u^{-1}.u(s)$. Donc $\sigma(\lambda\, \mu) = \sigma(\lambda)\sigma(\mu)$. σ étant additif, on a $\sigma(\lambda\, \mu) = \sigma(\lambda)\sigma(\mu)$ pour tout λ et tout $\mu \in F$. Donc σ est un auto-

morphisme de corps. Tout $x \in Q$ étant de la forme $\mu s (\mu \in F)$, on a $u(\lambda x) = \sigma(\lambda) u(x)$ pour tout $\lambda \in F$ et tout $x \in Q$, donc u est semi-linéaire. L'application qui à $u \in C_U(s)$ associe l'automorphisme σ tel que $u(\lambda s) = \sigma(\lambda)s$ est un isomorphisme de groupes, d'où c).

d) Soit P_1 un sous-groupe $\neq 1$ de P. D'après c) P_1 opère sur le corps F et $C_F(P_1) \tilde{=} \mathbb{F}_d$. Or Aut(F) est cyclique d'ordre n et si $|P_1| = p$, le corps des points fixes de P_1 est $\tilde{=} \mathbb{F}_{d^{n/p}}$. Donc $n = p$. Tout sous-groupe $\neq 1$ de P étant d'ordre n, P est d'ordre premier p et $n = p$. On a donc $P \tilde{=} \mathrm{Aut}(F)$ et d'après c) si $s \in C_Q(P)^{\#}$, $C_U(s) = P$.

APPENDICE VI

UNE GÉNÉRALISATION D'UN THÉORÈME DE BURNSIDE

Nous allons démontrer la généralisation suivante du théorème de Burnside sur les groupes de permutation de degré premier [Huppert, chapitre V, § 21] :

Théorème.- Soit W *un groupe opérant sur un ensemble* I. *Soit* K *un sous-groupe de* W *qui opère régulièrement sur* I. *On suppose que pour tout* $k \in K^{\#}$, *on a* $C_W(k) = K$. *Alors ou bien* $W = C_W(I)N_W(K)$, *ou bien* W *opère de manière doublement transitive sur* I.

On suppose que $|I| > 1$. Soit π le caractère de l'opération de W sur I : $\pi(x)$ est le nombre de points fixes de x dans I. On a $[\pi, 1_W] = 1$. Soit $\pi = 1_W + \sum_{i=1}^{t} \psi_i$ la décomposition de π en somme de caractères irréductibles. Si $t = 1$, W opère de manière doublement transitive sur I [Isaacs (5-17)]. On supposera donc :

1) $t \geq 2$

2) Supposons $N_W(K) = K$. Alors W est un groupe de Frobenius de complément K. Soit M le noyau de Frobenius de W. Si $a \in I$, on a $|W| = |K||W_a|$, donc $W_a = M$. Il en résulte que $M = C_W(I)$ et $W = C_W(I)K$.

On suppose dans la suite que $E = N_W(K) \neq K$. On peut alors appliquer la théorie des caractères exceptionnels [Isaacs, (7-16) à (7-20)]. On suppose connus les résultats suivants :

a) Ou bien les éléments de $K^{\#}$ sont tous conjugués dans E, ou bien il existe une bijection $f : \mathcal{S} \to \mathcal{E}$ où $\mathcal{S} = \{\chi \in \mathrm{Irr}(E)/K \not\subset \mathrm{Ker}\ \chi\}$ et $\mathcal{E} \subset \mathrm{Irr}(W)$ (ensemble des caractères exceptionnels) et $\varepsilon = \pm 1$ tels que $\mathrm{Ind}_E^W(\chi_1 - \chi_2) = \varepsilon(f(\chi_1) - f(\chi_2))$ pour $\chi_1, \chi_2 \in \mathcal{S}$. Dans ce deuxième cas :

b) Si $\psi \in \mathrm{Irr}(W)$ et $\psi \notin \mathcal{E}$, alors ψ est constant sue $K^{\#}$, et :

c) Si $x \in W$ n'est pas conjugué à un élément de $K^{\#}$, alors $\psi(x)$ est indépendant de ψ pour $\psi \in \mathcal{E}$.

3) On est dans le deuxième cas de a) et les ψ_i sont des caractères exceptionnels.

D'après l'hypothèse, $\mathrm{Res}_K^W \pi$ est le caractère régulier de K : $\mathrm{Res}_K^W \pi = 1_K + \sum_{i=1}^{t} \mathrm{Res}_K^W \psi_i = \sum_{\chi \in \mathrm{Irr}(K)} \chi$. Puisque $t \geq 2$, on a $\mathrm{Res}_K^W \psi_i = \sum_{\chi \in \mathcal{C}_i} \chi$, avec $\emptyset \neq \mathcal{C}_i \subsetneq \mathrm{Irr}(K) - \{1_K\}$.

Si $\psi \in \mathrm{Irr}(W)$ est constant sur $K^{\#}$, alors $\mathrm{Res}_K^W \psi$ contient tous les caractères de $\mathrm{Irr}(K) - \{1_K\}$ avec la même multiplicité. En effet, si $\psi(x) = a$ pour $x \in K^{\#}$ et $\chi \in \mathrm{Irr}(K) - \{1_K\}$, on a $[\chi, \mathrm{Res}_K^W \psi] = \frac{1}{|K|}[\psi(1) + (|K| - 1)\, \bar{a} \sum_{x \in K^{\#}} \chi(x)]$ et $\sum_{x \in K^{\#}} \chi(x) = |K|([\chi, 1_K] - 1) = -|K|$ est indépendant de χ.

D'après la forme de $\mathrm{Res}_K^W \psi_i$, il en résulte que ψ_i n'est pas constant sur $K^{\#}$. Donc les éléments de $K^{\#}$ ne sont pas tous conjugués et d'après b) ψ_i est exceptionnel.

4) Soit $y \in W$, y non conjugué à un élément de $K^{\#}$. Alors $\psi_1(y) = \ldots = \psi_t(y)$ et $\psi_1(y)$ est un entier tel que $0 \leq \psi_1(y) \leq \psi_1(1)$.

On $\psi_1(y) = \ldots = \psi_t(y)$ d'après c) et 3). Il en résulte que $\pi(y) = 1 + t\psi_1(y)$. Donc $\psi_1(y) \in \mathbb{Q}$ et comme $\psi_1(y)$ est un entier algébrique, $\psi_1(y) \in \mathbb{Z}$. Comme $\pi(y) \geq 0$ et $t \geq 2$, on a $\psi_1(y) \geq -1/t$ d'où $\psi_1(y) \geq 0$.

5) Soient $s = \psi_1(1)$ et pour $0 \leq i \leq s$, n_i le nombre des $y \in W$ tels que y ne soit pas conjugué à un élément de $K^{\#}$ et $\psi_1(y) = i$. On a :

$$(5.1) \quad \sum_{i=1}^{s} i n_i = |W : E| s \quad \text{et} \quad (5.2) \quad \sum_{i=1}^{s} i^2 n_i = |W : E| s^2.$$

On écrit que $[\psi_1, 1_W] = 0$ et que $[\psi_1, \psi_2] = 0$:

$$0 = |W|[\psi_1, 1_W] = \sum_{y \in W} \psi_1(y) = \sum_{i=1}^{s} i n_i + |W : E| \sum_{y \in K^{\#}} \psi_1(y). \qquad \text{Mais on a :}$$

$$0 = |K|[\mathrm{Res}_K^W \psi_1, 1_K] = \sum_{y \in K^{\#}} \psi_1(y) + \psi_1(1), \text{ donc } \sum_{y \in K^{\#}} \psi_1(y) = -s$$

et on obtient $0 = \sum_{i=1}^{s} i n_i - s|W : E|$.

$0 = |W|[\psi_1,\psi_2] = \sum_{i=1}^{s} i^2 n_i + |W:E| \sum_{y\in K^\#} \psi_1(y)\overline{\psi_2(y)}$. Mais on a :

$0 = |K|[\mathrm{Res}_K^W \psi_1, \mathrm{Res}_K^W \psi_2] = \sum_{y\in K^\#} \psi_1(y)\overline{\psi_2(y)} + \psi_1(1)^2$, donc

$\sum_{y\in K^\#} \psi_1(y)\overline{\psi_2(y)} = -s^2$ et on obtient :

$0 = \sum_{i=1}^{s} i^2 n_i - s^2 |W:E|$.

6) $W = (\mathrm{Ker}\ \pi)E$

En multipliant (5.1) par s et en soustrayant (5.2), on obtient $\sum_{i=1}^{s} i(s-i)n_i = 0$. Pour $1 \le i \le s-1$, on a $i(s-i) > 0$ d'où $n_i = 0$. D'après (5.1), il en résulte alors que $sn_s = |W:E|s$ donc $n_s = |W:E|$. Mais n_s est le nombre des éléments y de W tels que $\psi_1(y) = \psi_1(1)$, c'est-à-dire $\pi(y) = \pi(1)$. Donc $|\mathrm{Ker}\ \pi| = |W:E|$.

D'autre part, $(\mathrm{Ker}\ \pi) \cap E = 1$ car si $x \in (\mathrm{Ker}\ \pi) \cap E$, on a $[x,K] \subset K \cap (\mathrm{Ker}\ \pi) = 1$, donc $x \in C_W(K) \subset K$, donc $x \in K \cap (\mathrm{Ker}\ \pi) = 1$. Par conséquent, on a $W = (\mathrm{Ker}\ \pi)E$.

APPENDICE VII

Le théorème suivant généralise le lemme 2 du chapitre I, § 6.

Théorème.- Soit $Q \rtimes P$ *un groupe opérant sur un groupe* K. *On suppose que :*

a) $|P| = p$ *est premier,* $p \nmid |Q|$ *et* $|C_Q(P)|$ *est impair.*

b) $|K|$ *est premier à* $|Q \rtimes P|$.

Alors K *est engendré par la réunion des sous-groupes* $C_K([P,Q])$ *et* $C_K(P^x)$ *pour* $x \in Q$.

La démonstration est divisée en deux parties.

1ère partie : réduction à un cas particulier.

On suppose que $K \rtimes (Q \rtimes P)$ est un contre-exemple au théorème tel que $|K \rtimes (Q \rtimes P)|$ soit minimal.

1) K est un r-groupe abélien élémentaire $\neq 1$ pour un nombre premier r, QP opère fidèlement et de manière irréductible sur K, et on a $C_K(P) = C_K([P,Q]) = 1$

Puisque $|K|$ est premier à $|Q \rtimes P|$, on sait que pour tout r premier, il existe un r-Sylow K_r de K normalisé par $Q \rtimes P$. (La démonstration de ceci utilise l'argument de Frattini et le théorème de Schur-Zassenhaus. Le théorème de Feit-Thompson est utilisé ici si on ne suppose pas que K ou Q est résoluble). Puisque K est engendré par les K_r, l'hypothèse de récurrence montre que le théorème est vrai pour $K \rtimes (Q \rtimes P)$ si K n'est pas un r-groupe. Donc K est un r-groupe. Soit $Z = \langle C_K([P,Q]), C_K(P^x) \mid x \in Q \rangle$. Alors $\Phi(K) \subset Z$ d'après l'hypothèse de récurrence. Donc $Z \lhd K$. Puisque $Q \rtimes P$ normalise Z, $Q \rtimes P$ opère sur K/Z.

Supposons $Z \neq 1$. L'hypothèse de récurrence montre que $K/Z = \langle C_{K/Z}([P,Q]), C_{K/Z}(P^x) \mid x \in Q \rangle$. Mais puisque $|K|$ est premier à $|Q \rtimes P|$,

$C_{K/Z}([P,Q]) = C_K([P,Q])Z/Z = 1$ et $C_{K/Z}(P^x) = 1$. Donc $K = Z$ et le théorème est vrai pour $K \rtimes (Q \rtimes P)$.

Donc $Z = 1$ et $\Phi(K) = 1$. Supposons $C_Q(K) \neq 1$. Alors en appliquant l'hypothèse de récurrence à $K \rtimes ((Q/C_Q(K)) \rtimes P)$, on voit que $[P,Q]$ centralise K, et le théorème est vrai pour $K \rtimes (Q \rtimes P)$. Donv $C_Q(K) = 1$. D'après l'hypothèse de récurrence, il est clair que QP opère irréductiblement sur K.

2) Q est un q-groupe (q nombre premier $\neq p,r$), $[Q,P] = Q$ et $\Phi(Q) \subset Z(Q)$.

Pour tout diviseur premier q_i de $|Q|$, il existe un q_i-Sylow Q_i de Q normalisé par P. Si Q n'est pas un q-groupe, l'hypothèse de récurrence montre que P centralise chacun des Q_i, donc centralise Q, ce qui est absurde. Donc Q est un q-groupe. D'après l'hypothèse de récurrence, P centralise tout sous-groupe propre de Q qu'il normalise. D'après l'appendice IV, lemme 1 a) et lemme 2, on a alors $[Q,P] = Q$ et $\Phi(Q) \subset Z(Q)$.

3) Si Q est abélien, alors QP est un groupe de Frobenius de noyau Q.

D'après l'appendice IV, lemme 1 b), on a alors $[Q,P] = Q = [Q,P] \times C_Q(P)$, donc $C_Q(P) = 1$.

4) Supposons Q non abélien. Alors Q est extra-spécial (c'est-à-dire $[Q,Q] = \Phi(Q) = Z(Q)$ est d'ordre q), P opère sans point fixe sur $Q/Z(Q)$ et centralise $Z(Q)$.

On a $[Q,Q] \subset \Phi(Q) \subset Z(Q)$. D'après l'appendice IV, lemme 1 b), on a, en posant $\bar{Q} = Q/[Q,Q]$, $\bar{Q} = [\bar{Q},P] \times C_{\bar{Q}}(P)$. Mais on a $[Q,P] = Q$, donc $[\bar{Q},P] = \bar{Q}$, donc $C_{\bar{Q}}(P) = 1$. On a $Z(Q) \subsetneq Q$ donc par hypothèse de récurrence, P centralise $Z(Q)$. Il en résulte que $Z(Q) \subset [Q,Q]$, d'où $[Q,Q] = \Phi(Q) = Z(Q)$.

Puisque QP opère fidèlement et irréductiblement sur K, $Z(Q) = Z(QP)$ est cyclique. Soient $a,b \in Q$. Puisque Q est de classe 2, on a $[a,b]^q = [a,b^q]$. Mais $b^q \in \Phi(Q) \subset Z(Q)$, donc $[a,b]^q = 1$. Puisque $[Q,Q]$ est abélien et engendré par les $[a,b]$ ($a,b \in Q$), $[Q,Q] = Z(Q)$ est d'exposant q, et puisque $Z(Q)$ est cyclique, il est d'ordre q.

5) QP a un caractère irréductible sur $\mathbb{C}$ dont le noyau ne contient pas $Z(Q)$ et dont la restriction à P ne contient pas le caractère unité.

Soit $\overline{\mathbb{F}}_r$ la clôture algébrique de $\mathbb{F}_r$. Le groupe QP opère sur le $\overline{\mathbb{F}}_r$-espace vectoriel $V = \overline{\mathbb{F}}_r \otimes K$. Soit $x \in P^{\#}$. Puisque $C_K(P) = 1$, l'endomorphisme de K défini par x n'a pas de valeur propre égale à 1. Donc l'endomorphisme de

V défini par x n'a pas de valeur propre égale à 1, car ces deux endomorphismes ont le même polynôme caractéristique. Donc P opère sans point fixe sur V.

Or V est produit direct de $\overline{\mathbb{F}}_r[QP]$-modules simples V_i, et comme QP opère fidèlement sur V, il existe i tel que Z(Q) opère non trivialement sur V_i. Il existe donc un caractère irréductible de QP sur $\overline{\mathbb{F}}_r$ dont le noyau ne contient pas Z(Q) et dont la restriction à P ne contient pas le caractère unité. D'après [Huppert, chapitre V, théorème 12.9], il existe un caractère irréductible de QP sur $\mathbb{C}$ qui a les mêmes propriétés.

2ème partie : caractères de QP.

On va montrer que pour les groupes QP obtenus dans la première partie, la restriction à P d'un caractère irréductible de QP dont le noyau ne contient pas Z(Q) contient le caractère unité.

1) Supposons d'abord que Q soit abélien.

Alors QP est un groupe de Frobenius de noyau Q. On sait que les caractères irréductibles de QP qui n'ont pas Q dans leur noyau sont de la forme $\mathrm{Ind}_Q^{QP}(\lambda)$ où λ est un caractère linéaire $\neq 1$ de Q. La restriction à P d'un tel caractère est le caractère régulier de P (qui vaut p en 1 et 0 sur $P^{\#}$) donc contient le caractère unité de P.

On suppose dans la suite que Q est non-abélien, donc extra-spécial.

2) Caractères de Q.

Puisque Q est un q-groupe extra-spécial, l'application commutateur : $(x,y) \longmapsto [x,y]$ induit une forme bilinéaire alternée non dégénérée : $Q/Z(Q) \times Q/Z(Q) \to Z(Q)$. Il en résulte qu'il existe un entier $m \geq 1$ tel que $|Q| = q^{2m+1}$ et que pour $x \in Q - Z(Q)$, on a $|C_Q(x)| = q^{2m}$.

Soit ψ un caractère irréductible de Q tel que $Z(Q) \not\subset \mathrm{Ker}\,\psi$. D'après les deuxièmes relations d'orthogonalité, ψ s'annule sur $Q - Z(Q)$, puisque pour $x \in Q - Z(Q)$, on a :

$$\sum_{\phi \in \mathrm{Irr}(Q),\, Z(Q) \subset \mathrm{Ker}\,\phi} |\phi(x)|^2 = |Q/Z(Q)| = q^{2m} = |C_Q(x)|.$$

On a donc $1 = [\psi,\psi] = \frac{1}{|Q|}\,\psi(1)^2|Z(Q)|$ d'où $\psi(1)^2 = |Q|/|Z(Q)| = q^{2m}$, et $\psi(1) = q^m$. D'autre part, $\mathrm{Res}^Q_{Z(Q)}(\psi) = \psi(1)\lambda$ pour un caractère linéaire λ de $Z(Q)$, et $\lambda \neq 1$ car $Z(Q) \notin \mathrm{Ker}\,\psi$. En résumé :

$$\begin{cases} \psi(x) = q^m\lambda(x) & \text{pour } x \in Z(Q), \text{ où } \lambda \in \mathrm{Irr}(Z(Q)) - \{1_{Z(Q)}\}. \\ \psi(x) = 0 & \text{pour } x \in Q - Z(Q)\ . \end{cases}$$

Soit χ un caractère irréductible de QP tel que $Z(Q) \notin \mathrm{Ker}\,\chi$.

3) $\mathrm{Res}^{QP}_Q\chi = e\psi$, <u>où</u> e <u>est un entier</u> ≥ 1 <u>et</u> ψ <u>un caractère irréductible de</u> Q <u>tel que</u> $Z(Q) \notin \mathrm{Ker}\,\psi$.

D'après le théorème de Clifford, $\mathrm{Res}^{QP}_Q\chi = e\sum\psi_i$ où les ψ_i sont des caractères irréductibles de Q conjugués par P. Si ψ_1 est de degré 1, on a $Z(Q) \subset \mathrm{Ker}\,\psi_i$ pour tout i, d'où $Z(Q) \subset \mathrm{Ker}\,\chi$, contrairement à l'hypothèse. Donc $Z(Q) \notin \mathrm{Ker}\,\psi_1$. D'après 2) et le fait que P centralise $Z(Q)$, on voit que ψ_1 est invariant par P. Donc $\mathrm{Res}^{QP}_Q\chi = e\psi$, avec $\psi = \psi_1$.

4) $\sum_{x\in P^\#}|\chi(x)|^2 = p - e^2$.

On écrit que $[\chi,\chi]_{QP} = 1$, c'est-à-dire $p|Q| = \sum_{y\in QP}|\chi(y)|^2$. Pour $y \in Z(Q)$, on a $|\chi(y)| = \chi(1) = e\psi(1)$. Pour $y \in Q - Z(Q)$ on a $\chi(y) = 0$ d'après 2) et 3). Si $y \in QP - Q$, puisque $QP/Z(Q)$ est un groupe de Frobenius de noyau $Q/Z(Q)$ et $Z(Q) = Z(QP)$, y se met de manière unique sous la forme $y = zx^t$, où $z \in Z(Q)$, $x \in P^\#$ et $t \in Q/Z(Q)$. Pour un tel y, on a $|\chi(y)| = |\chi(x^t)| = |\chi(x)|$ car χ est irréductible et $z \in Z(QP)$. On a donc :

$$p|Q| = \sum_{y\in QP}|\chi(y)|^2 = |Z(Q)|e^2\psi(1)^2 + |Z(Q)||Q/Z(Q)|\sum_{x\in P^\#}|\chi(x)|^2\ .$$

Comme $|Z(Q)|\psi(1)^2 = |Q|$ d'après 2), il vient donc $p = e^2 + \sum_{x\in P^\#}|\chi(x)|^2$.

5) <u>Soient</u> α_i $(i = 1,\ldots,p)$ <u>les caractères irréductibles de</u> P <u>et</u> $n_i = [\mathrm{Res}_P\chi,\alpha_i]$. <u>Il existe un indice</u> i_o <u>et un entier</u> n <u>tels que</u> $n_i = n$ <u>pour</u> $i \neq i_o$ <u>et</u> $n_{i_o} = n \pm 1$. <u>De plus</u> $e = 1$.

On a $\sum_{i=1}^p n_i^2 = [\mathrm{Res}_P\chi,\mathrm{Res}_P\chi]$ d'où d'après 4), $\sum_{i=1}^p n_i^2 = \frac{1}{p}(\chi(1)^2 + p - e^2) = \frac{1}{p}[(\Sigma n_i)^2 + p - e^2]$. Cette égalité s'écrit aussi $(p-1)\sum_i n_i^2 = 2\sum_{\{i,j\},i\neq j} n_in_j + (p - e^2)$

ou : $\sum_{\{i,j\},i\neq j} (n_i - n_j)^2 = p - e^2$. Mais il est facile de vérifier, par récurrence sur p, le lemme suivant :

Soit p un nombre entier ≥ 1 et $n_1,\ldots,n_p$ des nombres entiers. a) Si les n_i ne sont pas tous égaux, on a $\sum_{\{i,j\}} (n_i - n_j)^2 \geq p - 1$. b) Si $\sum_{\{i,j\}} (n_i - n_j)^2 = p - 1$, alors il existe un indice i_o et un entier n tels que $n_i = n$ pour $i \neq i_o$ et $n_{i_o} = n \pm 1$.

Puisque l'égalité $p = e^2$ est impossible, les n_i définis dans 5) ne peuvent pas être tous égaux. Donc $\sum_{\{i,j\}} (n_i - n_j)^2 = p - e^2 \geq p - 1$, d'où $e = 1$. On a alors $\sum_{\{i,j\}} (n_i - n_j)^2 = p - 1$, ce qui prouve 5) d'après b).

6) $\mathrm{Res}_P\chi$ contient le caractère unité de P.

Il suffit de montrer que, avec les notations de 5), $n_i \neq 0$ pour tout i. On a $\chi(1) = \psi(1) = q^m$ donc, en posant $\delta = n_{i_o} - n = \pm 1$, $pn + \delta = \sum_i n_i = q^m$. On a donc $n = (q^m - \delta)/p \neq 0$.

D'autre part, $n_{i_o} = \frac{q^m - \delta}{p} + \delta$. Si $n_{i_o} = 0$, alors $q^m = -\delta(p - 1)$. Puisque $m > 0$, cette égalité n'est possible que si $\delta = -1$, $p > 2$ et q est alors pair. Mais cela contredit l'hypothèse selon laquelle $|C_Q(P)|$ est impair.

Remarque : L'hypothèse "$|C_Q(P)|$ est impair" peut être remplacée par : "p n'est pas un nombre premier de la forme $2^m + 1$".

APPENDICE VIII

GROUPES D'AUTOMORPHISMES DE CERTAINS 2-GROUPES DE SUZUKI

Lemme 1. a) *Soient* P *un 2-groupe,* W *un sous-groupe de* Z(P) *tel que* W *et* V = P/W *soient abéliens élémentaires. L'application* $x \longmapsto x^2$ *induit une application quadratique de* V *dans* W, V *et* W *étant considérés comme* $\mathbb{F}_2$*-espaces vectoriels.*

b) *Soient* V, W *des espaces vectoriels de dimension finie sur* $\mathbb{F}_2$. *Pour toute application quadratique* q : V → W, *il existe une extension centrale* $W \xrightarrow{\iota} P \xrightarrow{\pi} V$ *telle que l'application* P/ι(W) *dans* ι(W) *définie dans* a) *s'identifie à* q.

c) *Soient* V, W,V',W' *des espaces vectoriels de dimension finie sur* $\mathbb{F}_2$, $W \to P \xrightarrow{\pi} V$ *et* $W' \to P' \xrightarrow{\pi'} V'$ *des extensions centrales,* q : V → W *et* q' : V' → W' *les applications quadratiques associées. Soient* f : V → V' *et* g : W → W' *des isomorphismes. Pour qu'il existe un isomorphisme* : P → P' *qui induise* f *sur* V *et* g *sur* W, *il faut et il suffit que* g ∘ q = q' ∘ f.

d) *Si* V, W *sont des espaces vectoriels de dimension finie sur* $\mathbb{F}_2$ *et* W → P → V *est une extension centrale, l'ensemble des automorphismes de* P *qui induisent l'identité sur* V *et sur* W *est un groupe isomorphe au groupe additif* Hom(V,W).

Si V, W sont des espaces vectoriels sur $\mathbb{F}_2$, rappelons qu'une application q : V → W est quadratique si l'application $(x,y) \longmapsto q(x+y) - q(x) - q(y)$ est bilinéaire.

a) Il est clair que $x \longmapsto x^2$ induit une application q : V → W et que l'application commutateur induit une application $(x,y) \longmapsto [x,y]$ de V × V dans W. Celle-ci est bilinéaire d'après Huppert, chapitre III, (1-2). Si $\bar{x}$, $\bar{y}$ sont les

images dans V de $x,y \in P$, on a :

$$q(\bar{x}+\bar{y}) = (xy)^2 = x^2y^2[y,x] = q(\bar{x}) + q(\bar{y}) + [x,y].$$

Donc q est une application quadratique.

b) Soit $(e_1,\ldots,e_n)$ une base de V sur $\mathbb{F}_2$. Soit $b : V \times V \to W$ l'application bilinéaire telle que :

$$b(e_i,e_i) = q(e_i), \quad b(e_i,e_j) = q(e_i+e_j) + q(e_i) + q(e_j) \quad \text{si} \quad i<j,$$

$$b(e_i,e_j) = 0 \quad \text{si} \quad i>j.$$

On a alors $b(v,v) = q(v)$ pour tout $v \in V$ et il suffit de prendre pour P l'ensemble $V \times W$ muni de la loi de composition :

$$(v_1,w_1)(v_2,w_2) = (v_1+v_2, b(v_1,v_2) + w_1 + w_2)$$

et de poser $\iota(w) = (0,w)$, $\pi(v,w) = v$ pour $v \in V$, $w \in W$.

c) La nécessité est immédiate. Supposons que $g \circ q = q' \circ f$. Soient $(e_1,\ldots,e_n)$ une base de V et $x_1,\ldots,x_n \in P$ tels que $\pi(x_i) = e_i$, $y_1,\ldots,y_n \in P'$ tels que $\pi'(y_i) = f(e_i)$. Identifions W, W' à leurs images dans P, P' respectivement. Par hypothèse $g(x_i^2) = y_i^2$ et $g([x_i,x_j]) = [y_i,y_j]$ car $[x_i,x_j] = (x_i\,x_j)^2 x_i^2 x_j^2$. Tout élément x de P s'écrit de manière unique sous la forme $x = x_1^{a_1} \ldots x_n^{a_n} w$ $(0 \le a_i \le 1,\ w \in W)$. En posant alors $h(x) = y_1^{a_1} \ldots y_n^{a_n} g(w)$, h est un isomorphisme : $P \to P'$ qui induit f sur V et g sur W.

d) D'après c) toute extension centrale de W par V est équivalente à une des extensions construites dans b). On vérifie que l'ensemble des automorphismes du groupe P construit dans b), qui induisent l'identité sur V et sur W, est l'ensemble des applications $(v,w) \longmapsto (v,h(v)+w)$ où h est un homomorphisme: $V \to W$.

Lemme 2.- Soit K un corps fini de caractéristique 2.

a) L'ensemble des applications $\mathbb{F}_2$-linéaires : $K \to K$ est un K-espace vectoriel ayant pour base l'ensemble des automorphismes de corps de K.

b) L'ensemble des applications $\mathbb{F}_2$-bilinéaires : $K \times K \to K$ est un K-espace vectoriel ayant pour base la famille des applications $(x,y) \longmapsto \sigma(x)\tau(y)$,

(σ,τ) *parcourant les couples d'automorphismes de* K.

c) *L'ensemble des applications* $\mathbb{F}_2$*-quadratiques* : $K \to K$ *est un* K*-espace vectoriel ayant pour base la famille des applications* $x \mapsto \sigma(x)\tau(x)$, $\{\sigma,\tau\}$ *parcourant les parties de cardinal 1 ou 2 de* Aut(K).

d) *L'ensemble des applications* $\mathbb{F}_2$*-quadratiques* : $K \times K \to K$ *est un* K*-espace vectoriel ayant pour base l'ensemble des applications* :

$$(x,y) \longmapsto \sigma(x)\tau(y) \qquad ((\sigma,\tau) \in \mathrm{Aut}(K) \times \mathrm{Aut}(K)),$$

$$(x,y) \longmapsto \sigma(x)\tau(x) \quad \text{et} \quad (x,y) \longmapsto \sigma(y)\tau(y) \quad (\{\sigma,\tau\} \subset \mathrm{Aut}(K)).$$

a) On sait que les automorphismes de corps de K sont linéairement indépendants sur K. Si $|K| = 2^n$, on a $|\mathrm{Hom}_{\mathbb{F}_2}(K,K)| = |K|^n$ et $|\mathrm{Aut}(K)| = n$, d'où le résultat.

b) Supposons $\Sigma\lambda_{\sigma\tau}\ \sigma(x)\tau(y) = 0$ quels que soient $x,y \in K$, la sommation étant étendue aux $(\sigma,\tau) \in \mathrm{Aut}(K) \times \mathrm{Aut}(K)$, et $\lambda_{\sigma\tau} \in K$. En appliquant deux fois a), on voit alors que $\lambda_{\sigma\tau} = 0$ pour tout σ et tout τ. Donc les applications $(x,y) \longmapsto \sigma(x)\tau(y)$ sont linéairement indépendantes sur K. Comme l'espace des applications $\mathbb{F}_2$-bilinéaires : $K \times K \to K$ est de dimension n^2 sur K, on a le résultat.

c) Soit $q(x) = \Sigma\lambda_{\sigma\tau}\ \sigma(x)\tau(x)$, somme étendue aux $\{\sigma,\tau\} \subset \mathrm{Aut}(K)$, et $\lambda_{\sigma\tau} \in K$. Supposons $q(x) = 0$ pour tout $x \in K$. Alors $q(x+y) + q(x) + q(y) =$ $= \Sigma_{\{\sigma,\tau\}}\lambda_{\sigma\tau}(\sigma(x)\tau(y) + \sigma(y)\tau(x)) = 0$. D'après b) il en résulte que $\lambda_{\sigma\tau} = 0$ pour $\sigma \neq \tau$. On a alors $q(x) = \Sigma_\sigma\lambda_{\sigma\sigma}\sigma(x)^2 = \Sigma_\sigma\lambda_{\sigma\sigma}\sigma(x^2) = 0$ pour tout x, et d'après a) $\lambda_{\sigma\sigma} = 0$. Les applications $x \longmapsto \sigma(x)\tau(x)$ sont donc linéairement indépendantes sur K. D'autre part, si q est une application quadratique : $K \to K$, il existe une application $\mathbb{F}_2$-bilinéaire $f : K \times K \to K$ telle que $q(x) = f(x,x)$ (voir lemme 1,b)). D'après b), q est donc combinaison K-linéaire des applications $x \longmapsto \sigma(x)\tau(x)$.

d) Toute application quadratique $q : K \times K \to K$ se met sous la forme $q(x,y) = q_1(x) + q_2(y) + f(x,y)$ où q_1 et q_2 sont des applications quadratiques $K \to K$ et où f est $\mathbb{F}_2$-bilinéaire. Il est clair que q détermine q_1, q_2, f de manière unique et que si q_1, q_2, f sont donnés, l'application q définie par la formule ci-dessus est quadratique. Donc d) résulte de b) et c).

Soient $K = \mathbb{F}_{2^n}$ et ϕ un automorphisme de K. Rappelons que (suivant la

notation de l'article "Suzuki 2-groups" de G. Higman) le groupe $A(n,\phi)$ est une extension centrale de K par K, associée suivant le lemme 1 b) à l'application quadratique $x \longmapsto x\phi(x)$ de K dans K. Si $P = A(n,\phi)$, on a donc une suite exacte $K \xrightarrow{1} P \to K$ et on vérifie que si $\phi \neq 1$, $Z(P) = 1(K)$. Donc si $\alpha \in \mathrm{Aut}(P)$, il existe des isomorphismes f_α, g_α de groupes additifs tels que le diagramme

$$\begin{array}{ccccc} K & \longrightarrow & P & \longrightarrow & K \\ \downarrow{\scriptstyle g_\alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle f_\alpha} \\ K & \longrightarrow & P & \longrightarrow & K \end{array}$$

soit commutatif.

Proposition 1.- Soit $K = \mathbb{F}_{2^n}$ *et* ϕ *un automorphisme de* K *tel que* $\phi^4 \neq 1$. *L'application* $\alpha \mapsto f_\alpha$ *est un homomorphisme surjectif de* $\mathrm{Aut}(A(n,\phi))$ *sur le groupe des applications* $x \mapsto \lambda\sigma(x)$ *de* K *dans* K ($\lambda \in K^*, \sigma \in \mathrm{Aut}(K)$). *Le noyau de* $\alpha \mapsto f_\alpha$ *est un 2-groupe abélien élémentaire.*

Posons $\phi(x) = x^{2^s}$ et $q(x) = x\phi(x)$ pour $x \in K$. Soient f, g des isomorphismes additifs de K sur K provenant d'un automorphisme de $A(n,\phi)$, et qui vérifient donc $g \circ q = q \circ f$ (lemme 1 c)). D'après le lemme 2 a), on peut poser

$$f(x) = \sum_{i=0}^{n-1} \lambda_i x^{2^i} \quad , \quad g(x) = \sum_{i=0}^{n-1} \mu_i x^{2^i} \qquad (\lambda_i, \mu_i \in K).$$

On a alors :

$$(1) \qquad g(q(x)) = \sum_{i=0}^{n-1} \mu_i x^{2^i + 2^{i+s}}$$

$$(2) \qquad q(f(x)) = \Big(\sum_{i=0}^{n-1} \lambda_i x^{2^i}\Big)\Big(\sum_{i=0}^{n-1} \lambda_i^{2^s} x^{2^{i+s}}\Big)$$

Si i et j sont des entiers modulo n, les coefficients de $x^{2^i+2^j}$ dans (1) et (2) sont égaux d'après le lemme 2 c). En particulier, puisque $s \neq 0$, le coefficient de $x^{2^i+2^i}$ dans (1) est nul, donc :

$$(3) \qquad \lambda_i \lambda_{i-s}^{2^s} = 0 \quad \text{pour tout i.}$$

Si $i \neq j$ et $i - j \neq \pm s \pmod n$, le coefficient de $x^{2^i+2^j}$ dans (1) est nul, donc

(4) $\lambda_i \lambda_{j-s}^{2^s} + \lambda_j \lambda_{i-s}^{2^s} = 0$ si $i - j \not\equiv 0, \pm s \pmod{n}$.

Puisque $f \neq 0$, il existe i tel que $\lambda_i \neq 0$. D'après (3), on a alors $\lambda_{i-s} = 0$ et d'après (4) $\lambda_{j-s} = 0$ pour j tel que $i - j \not\equiv 0, \pm s \pmod{n}$.

Supposons qu'il existe $j \not\equiv i \pmod{n}$ tel que $\lambda_j \neq 0$. Alors $j \not\equiv i$, $j \not\equiv i - s$ et $i - (j + s) \equiv 0$ ou $\pm s \pmod{n}$. Donc $j \equiv i - 2s \pmod{n}$ et $\lambda_j \neq 0$ implique que $j \equiv i$ ou $j \equiv i - 2s \pmod{n}$. En faisant le même raisonnement avec $i - 2s$ à la place de i, on voit que $i \equiv (i - 2s) - 2s \pmod{n}$, donc $4s \equiv 0 \pmod{n}$ et $\phi^4 = 1$, contrairement à l'hypothèse.

Il existe donc $\lambda \in K^*$ et i tels que $f(x) = \lambda x^{2^i}$. En comparant les coefficients de $x^{2^j + 2^{j+s}}$ dans (1) et (2), on voit alors que $\mu_i = \lambda^{1+2^s}$ et $\mu_j = 0$ pour $j \not\equiv i \pmod{n}$. Les couples (f,g) induits par des automorphismes de $A(n,\phi)$ sont donc de la forme :

$$f(x) = \lambda x^{2^i} \quad , \quad g(x) = \lambda \phi(\lambda) x^{2^i} \quad , \quad \lambda \in K^* , \quad 0 \leq i \leq n - 1 .$$

Réciproquement, si f, g sont définis par ces formules, ce sont des isomorphismes additifs : $K \to K$ tels que $g \circ q = q \circ f$, donc proviennent d'un automorphisme de $A(n,\phi)$ (lemme 1 c)). Cela démontre la première partie de la proposition, et la deuxième partie résulte du lemme 1 d).

Remarque : Si ϕ est d'ordre 4, on trouve des automorphismes de $A(n,\phi)$ correspondant à des couples (f,g) tels que $f(x) = \lambda_1 x + \lambda_2 \phi^2(x)$, avec $\lambda_1, \lambda_2 \in K^*$. Ceci avait été omis dans l'article de G. Higman et m'a été indiqué par Bouc et Enguehard.

Soient $K = \mathbb{F}_{2^n}$ et $\varepsilon \in K$ tel que pour $a,b \in K$, $a^2 + \varepsilon ab + b^2 = 0$ implique $a = b = 0$. Le groupe $B(n,1,\varepsilon)$ est une extension centrale de K par $K \times K$ associée suivant le lemme 1 b) à l'application quadratique $(a,b) \longmapsto a^2 + \varepsilon ab + b^2$.

Proposition 2.- Soient $K = \mathbb{F}_{2^n}$, $L = K \times K$ *et* $q : L \to K$ *l'application quadratique associée au groupe* $B(n,1,\varepsilon)$. *Il existe une structure de corps sur* L, *compatible avec sa structure de* K*-espace vectoriel, telle que* $q(x) = x\bar{x}$ *pour* $x \in L$, $x \longmapsto \bar{x}$ *étant l'automorphisme d'ordre 2 de cette structure de corps.*

Puisque $q(a,b) = a^2 + \varepsilon ab + b^2 \neq 0$ pour $(a,b) \neq (0,0)$, le polynôme $X^2 + \varepsilon X + 1$ est irréductible sur K. Soit $\alpha \in \mathbb{F}_{2^{2n}}$ tel que $\alpha^2 + \varepsilon\alpha + 1 = 0$ et identifions $(a,b) \in L$ à $a + b\alpha$. Comme $\alpha + \bar{\alpha} = \varepsilon$ et $\alpha\,\bar{\alpha} = 1$, on a alors $(a + b\alpha)\overline{(a + b\alpha)} = q(a + b\alpha)$ pour $a,b \in K$.

D'après cette proposition, la structure de $B(n,1,\varepsilon)$ est indépendante de ε si ε satisfait la condition donnée ci-dessus. Posons $B(n,1) = B(n,1,\varepsilon)$. Si $P = B(n,1)$, $K = \mathbb{F}_{2^n}$ et $L = \mathbb{F}_{2^{2n}}$ on a ainsi une extension centrale $K \xrightarrow{\iota} P \to L$. Soit $\alpha \in \mathrm{Aut}(P)$. On vérifie que $\iota(K) = \Omega_1(P)$ donc α induit des isomorphismes f_α, g_α de groupes additifs tels que le diagramme

$$\begin{array}{ccccc} K & \longrightarrow & P & \longrightarrow & L \\ \downarrow{\scriptstyle g_\alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle f_\alpha} \\ K & \longrightarrow & P & \longrightarrow & L \end{array}$$

soit commutatif.

Proposition 3.- *Avec les notations ci-dessus, $\alpha \longmapsto f_\alpha$ est un homomorphisme surjectif de $\mathrm{Aut}(B(n,1))$ sur le groupe des applications $x \longmapsto \lambda\sigma(x)$ de L dans L ($\lambda \in L^*$, $\sigma \in \mathrm{Aut}(L)$). Le noyau de $\alpha \longmapsto f_\alpha$ est un 2-groupe abélien élémentaire.*

Soient $f : L \to L$, $g : K \to K$ des isomorphismes additifs provenant d'un automorphisme de $B(n,1)$. On a $g \circ q = q \circ f$ où $q(x) = x\bar{x}$ pour $x \in L$. D'après le lemme 2 a), on peut poser

$$f(x) = \sum_{i=0}^{2n-1} \lambda_i x^{2^i} \quad (\lambda_i \in L), \qquad g(x) = \sum_{i=0}^{n-1} \mu_i x^{2^i} \quad (\mu_i \in K).$$

On a alors pour $x \in L$:

$$(1) \qquad g(q(x)) = \sum_{i=0}^{n-1} \mu_i x^{2^i + 2^{i+n}}$$

$$(2) \qquad q(f(x)) = \Big(\sum_{i=0}^{2n-1} \lambda_i x^{2^i}\Big)\Big(\sum_{i=0}^{2n-1} \lambda_i^{2^n} x^{2^{i+n}}\Big)$$

Si i et j sont des entiers modulo 2n, les coefficients de $x^{2^i + 2^j}$ dans (1) et (2) sont égaux d'après le lemme 2 c) car $g \circ q$ et $q \circ f$ peuvent être considérés

comme des applications quadratiques : $L \to L$. Comme dans la proposition 1 :

(3) $\lambda_i \lambda_{i-n}^{2^n} = 0$ pour tout i.

(4) $\lambda_i \lambda_{j-n}^{2^n} + \lambda_j \lambda_{i-n}^{2^n} = 0$ si $i - j \not\equiv 0, n \pmod{2n}$.

Puisque $f \neq 0$, il existe i tel que $\lambda_i \neq 0$. D'après (3), on a alors $\lambda_{i-n} = 0$ et d'après (4) $\lambda_{j-n} = 0$ pour j tel que $j \not\equiv i, i-n \pmod{2n}$. Donc $\lambda_j = 0$ pour $j \not\equiv i \pmod{2n}$.

Il existe donc $\lambda \in L^*$ et i tels que $f(x) = \lambda x^{2^i}$. En comparant les coefficients de $x^{2^j+2^{j+n}}$ dans (1) et (2), on voit que :

Si $0 \leq i \leq n-1$, $\mu_i = \lambda \bar{\lambda}$ et $\mu_j = 0$ pour $j \neq i$.

Si $n \leq i \leq 2n-1$, $\mu_{i-n} = \lambda \bar{\lambda}$ et $\mu_j = 0$ pour $j \neq i-n$.

Les couples (f,g) induits par des automorphismes de B(n,1) sont donc de la forme :

$$f(x) = \lambda x^{2^i} \quad , \quad g(x) = \lambda \bar{\lambda} x^{2^i} \quad , \quad \lambda \in L^* \quad , \quad 0 \leq i \leq 2n-1.$$

Réciproquement, si f,g sont définis par ces formules, ce sont des isomorphismes additifs tels que $g \circ q = q \circ f$, donc proviennent d'un automorphisme de B(n,1). Cela démontre la première partie de la proposition, et la deuxième partie résulte du lemme 1 d).

Soient $n = 2s+1$ (s entier ≥ 1), $K = \mathbb{F}_{2^n}$, ϕ l'automorphisme $x \longmapsto x^{2^s}$ de K et $\varepsilon \in K$ tel que pour $x,y \in K$, $x\phi(x) + \varepsilon x^{1/2}\phi(y^2) + y^2 = 0$ implique $x = y = 0$ (en particulier $\varepsilon \neq 0$). Le groupe $C(n,\varepsilon)$ est alors une extension centrale de K par $K \times K$ associée suivant le lemme 1 b) à l'application quadratique $(x,y) \longmapsto q(x,y) = x\phi(x) + \varepsilon x^{1/2}\phi(y^2) + y^2$. Si $P = C(n,\varepsilon)$ on a ainsi une suite exacte $K \xrightarrow{\iota} P \xrightarrow{\pi} K \times K$ et $\iota(K) = \Omega_1(P)$ donc tout automorphisme α de P induit des isomorphismes additifs $f_\alpha : K \times K \to K \times K$ et $g_\alpha : K \to K$. Soit $P_1 = \pi^{-1}(0 \times K)$.

Proposition 4.- *Avec les notations ci-dessus,* $\alpha \mapsto f_\alpha$ *est un homomorphisme du groupe des automorphismes de* P *qui laissent stable* P_1 *dans le groupe des applications* $(x,y) \longmapsto (\lambda_1\sigma(x), \lambda_2\sigma(y))$ *de* $K \times K$ *dans* $K \times K$ $(\lambda_1, \lambda_2 \in K^*, \sigma \in \mathrm{Aut}(K))$. *Le noyau de* $\alpha \mapsto f_\alpha$ *est un 2-groupe abélien élémentaire.*

Soient $f : K \times K \to K \times K$, $g : K \to K$ des isomorphismes additifs provenant d'un automosphisme de P qui laisse stable P_1. On a $f(O \times K) \subset O \times K$ et $g \circ q = q \circ f$. Posons :

$$f(x,O) = (f_1(x), f_3(x)) \quad , \quad f(O,y) = (O, f_2 y)) \quad (x,y \in K).$$

D'après le lemme 2 a), on peut poser :

$$f_j(x) = \sum_{i=o}^{n-1} \lambda_{ij} x^{2^i} \quad (j = 1,2,3,\ \lambda_{ij} \in K) \quad , \quad g(x) = \sum_{i=o}^{n-1} \mu_i x^{2^i} \quad (\mu_i \in K).$$

On a alors pour $x,y \in K$:

$$(1) \quad g(q(x,y)) = \sum_{i=o}^{n-1} \mu_i (x^{1+2^s} + \varepsilon x^{2^{2s}} y^{2^{s+1}} + y^2)^{2^i}$$

$$(2) \quad q(f(x,y)) = (\sum_{i=o}^{n-1} \lambda_{i1} x^{2^i})(\sum_{i=o}^{n-1} \lambda_{i1} x^{2^i})^{2^s}$$

$$+ \varepsilon (\sum_{i=o}^{n-1} \lambda_{i1} x^{2^i})^{2^{2s}} (\sum_{i=o}^{n-1} \lambda_{i3} x^{2^i} + \sum_{i=o}^{n-1} \lambda_{i2} y^{2^i})^{2^{s+1}}$$

$$+ (\sum_{i=o}^{n-1} \lambda_{i3} x^{2^i} + \sum_{i=o}^{n-1} \lambda_{i2} y^{2^i})^2$$

D'après le lemme 2 d), les coefficients de $x^{2^i+2^j}$, de $x^{2^i} y^{2^j}$, de $y^{2^i+2^j}$ sont les mêmes dans (1) et (2). Dans (1), le coefficient de $x^{2^i} y^{2^j}$ est nul pour $i - j \not\equiv s - 1 \pmod n$ et il en est de même dans (2), d'où $\varepsilon \lambda_{i1} \lambda_{j2} = 0$ pour $i \not\equiv j \pmod n$, donc :

$$(3) \quad \lambda_{i1} = 0 \quad \text{ou} \quad \lambda_{j2} = 0 \quad \text{pour} \quad i \not\equiv j \pmod n.$$

Comme f est inversible, $f_1 \neq 0$ et $f_2 \neq 0$ et il existe i, j tels que $\lambda_{i1} \neq 0$ $\lambda_{j2} \neq 0$. D'après (3), $i = j$ et $\lambda_{k1} = \lambda_{k2} = 0$ pour $k \neq i$. Il existe donc $\lambda_1, \lambda_2 \in K^*$ et i tels que $f_1(x) = \lambda_1 x^{2^i}$, $f_2(x) = \lambda_2 x^{2^i}$. En comparant les coefficients de $x^{2^j+2^j}$ dans (1) et (2), on obtient :

$$\lambda_{j3}^2 = 0 \quad \text{pour} \quad j \not\equiv i + 2s \pmod n \quad , \quad \lambda_{i+2s,3}^2 + \varepsilon \lambda_1^{2^{2s}} \lambda_{i+s-1,3}^{2^{s+1}} = 0$$

Puisque $i + s - 1 \not\equiv i + 2s \pmod{n}$, on a donc $\lambda_{j3} = 0$ pour tout j, donc $f_3 = 0$. Puis en comparant les coefficients de $y^{2^j+2^j}$ dans (1) et (2), $\mu_j = 0$ pour $j \neq i$ et $\mu_i = \lambda_2^2$. Les couples (f,g) cherchés sont donc de la forme :

$$f(x,y) = (\lambda_1 x^{2^i}, \lambda_2 y^{2^i}) \quad , \quad g(x) = \lambda_2^2 x^{2^i}$$

Cela prouve la première assertion, et la deuxième résulte du lemme 1 d).

Remarque : En poursuivant le calcul ci-dessus, on voit que $\lambda_2^2 = \lambda_1^{1+2^s}$ et que $\varepsilon^{2^i} = \varepsilon$, ces conditions étant aussi suffisantes pour que $g \circ q = q \circ f$.

APPENDICE IX

LES REPRÉSENTATIONS IRRÉDUCTIBLES DE $GL(3, \mathbb{F}_2)$ SUR $\mathbb{F}_2$

Proposition.- Le groupe $GL(3, \mathbb{F}_2)$ a, à similitude près, 4 représentations irréductibles sur le corps $\mathbb{F}_2$, et elles sont de degré 1, 3, 3 et 8.

On va d'abord décrire des représentations R_1, R_2, R_3, R_4 de $G = GL(3, \mathbb{F}_2)$ sur $\mathbb{F}_2$, qui sont irréductibles et deux à deux non semblables sur $\mathbb{F}_2$.

R_1 est la représentation principale : $G \to \mathbb{F}_2^*$, de degré 1

R_2 est la représentation naturelle $X \longmapsto X : G \to GL(3, \mathbb{F}_2)$, de degré 3.

R_3 est la représentation $X \longmapsto {}^tX^{-1} : G \to GL(3, \mathbb{F}_2)$, de degré 3.

Soit E l'espace des matrices 3×3 à coefficients dans $\mathbb{F}_2$, de trace nulle On définit une opération à gauche de G sur E par $(X,A) \longmapsto X A X^{-1}$ pour $X \in G$ et $A \in E$. On a ainsi une représentation $R_4 : G \to GL(E)$, de degré 8.

Il est clair que les représentations R_1, R_2, R_3 sont irréductibles sur $\mathbb{F}_2$.

1) R_2 et R_3 ne sont pas semblables :

Soit (e_1, e_2, e_3) la base canonique de $\mathbb{F}_2^3$. Dans le calcul qui suit, on suppose que $GL(3, \mathbb{F}_2)$ opère à gauche sur $\mathbb{F}_2^3$, les coordonnées de Xe_j étant données par la j-ème colonne de $X \in GL(3, \mathbb{F}_2)$.

Supposons qu'il existe $A \in GL(3, \mathbb{F}_2)$ tel que $A X A^{-1} = {}^tX^{-1}$ pour tout $X \in GL(3, \mathbb{F}_2)$. Posons

$$X_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \qquad X_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

On a $X_2 = {}^tX_1^{-1}$, $\mathrm{Ker}(X_1 - 1) = \langle e_1 \rangle$, $\mathrm{Ker}(X_2 - 1) = \langle e_3 \rangle$. Puisque $A X A^{-1} = {}^tX^{-1}$ pour $X = X_1$ et pour $X = X_2$, on a donc $A.e_1 = e_3$ et $A.e_3 = e_1$. On a $\mathrm{Im}(X_1 - 1) = \langle e_1, e_2 \rangle$ et $\mathrm{Im}(X_2 - 1) = \langle e_2, e_3 \rangle$, donc $A.e_2 \in \langle e_2, e_3 \rangle$ et $A.e_2 \in \langle e_1, e_2 \rangle$, d'où $A.e_2 = e_2$ et :

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Mais pour cette valeur de A, on constate que $A X_1 A^{-1} \neq X_2$.
Donc R_2 et R_3 ne sont pas semblables sur $\mathbb{F}_2$.

2) R_4 est irréductible :

Les orbites de $G = GL(3, \mathbb{F}_2)$ dans E sont les classes de similitude de matrices 3×3 à coefficients dans $\mathbb{F}_2$, de trace nulle. Celles-ci sont décrites par le théorème suivant (Mac Lane, Birkhoff, Algèbre, chapitre X, § 4, théorème 8) :

Soit K *un corps commutatif. Si* $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_o \in K[X]$, *on pose*

$$M(f) = \begin{bmatrix} 0 & 0 & 0 \ldots 0 & -a_o \\ 1 & 0 & 0 \ldots 0 & -a_1 \\ 0 & 1 & 0 \ldots 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 \ldots 1 & -a_{n-1} \end{bmatrix}$$

Toute matrice carrée à coefficients dans K *est semblable sur* K *à une matrice et une seule de la forme* $M(f_1) \oplus M(f_2) \oplus \ldots \oplus M(f_k)$ *où* $f_1, \ldots, f_k$ *sont des polynômes unitaires non constants de* K[X] *tels que* f_{i+1} *divise* f_i $(i = 1, \ldots, k-1)$.

En appliquant ce théorème, on voit que les matrices suivantes forment un système de représentants des orbites de G dans E :

$$A_o = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} (f_1 = f_2 = f_3 = X), \qquad A_1 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} (f_1 = X^2, f_2 = X),$$

$$A_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} (f_1 = X^2 + X, f_2 = X + 1), \qquad A_3 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} (f_1 = X^3),$$

$$A_4 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} (f_1 = X^3 + 1), \qquad A_5 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} (f_1 = X^3 + X + 1).$$

$$A_6 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} (f_1 = X^3 + X).$$

Soit C_i l'ensemble des matrices semblables à A_i, sur $\mathbb{F}_2$ $(0 \leq i \leq 6)$. Il est facile de déterminer $C_G(A_i)$ pour chacune des matrices A_i, d'où $|C_i| = |G|/|C_G(A_i)|$. On obtient ainsi :

$|C_o| = 1$, $|C_1| = 21$, $|C_2| = 28$, $|C_3| = 42$, $|C_4| = 56$, $|C_5| = 24$ et $|C_6| = 84$

Soit V un sous-espace vectoriel de E, $V \neq 0$, tel que V soit réunion de certaines des orbites C_i. On a $0 = A_o \in V$.

Puisque $|V| \equiv 0 \pmod 2$, $|C_1| \equiv 1 \pmod 2$ et $|C_i| \equiv 0 \pmod 2$ pour $i \neq 0, 1$, on a $C_1 \subset V$.

Puisque $|V| \equiv 0 \pmod 4$, $|C_1| \equiv 1 \pmod 4$, $|C_3| \equiv 2 \pmod 4$ et $|C_i| \equiv 0 \pmod 4$ pour $i \neq 0, 1, 3$, on a $C_3 \subset V$.

On a $A_6 - A_3 \in C_1$ donc $A_6 \in V$ et $C_6 \subset V$. Puisque $|V| \geq |C_o \cup C_1 \cup C_3 \cup C_6| = 148$ et $|V|$ divise $|E| = 2^8$, on a $V = E$. Cela prouve que R_4 est irréductible.

On a ainsi vu que R_1, R_2, R_3, R_4 sont des $\mathbb{F}_2$-représentations de G irréductibles et deux à deux non semblables. On utilise alors les deux théorèmes suivants :

3) *Soit* L *un corps algébriquement clos de caractéristique* p *et* G *un groupe fini. Le nombre de* L*-représentations irréductibles de* G*, à similitude près, est égal au nombre de classes de conjugaison de* p'*-éléments de* G.

Voir Isaacs, chapitre 15 (15-11).

4) *Soient* K *un corps,* L *une extension de* K *et* G *un groupe fini. Le nombre des* K*-représentations irréductibles de* G*, à similitude près, est inférieur ou égal au nombre des* L*-représentations irréductibles de* G*, à similitude près.*

Cela résulte de Isaacs, chapitre 9, (9-7).

On peut déterminer les classes de conjugaison de G en utilisant le théorème cité dans 2). On trouve ainsi que G a 4 classes de 2'-éléments ($\{1\}$, une classe d'éléments d'ordre 3, deux classes d'éléments d'ordre 7).

Soient $K = \mathbb{F}_2$ et L une clôture algébrique de $\mathbb{F}_2$. D'après 3), G a 4 L-représentations irréductibles, à similitude près. D'après 4), le nombre des K-représentations irréductibles de G, à similitude près, est alors ≤ 4. Comme on a trouvé 4 K-représentations irréductibles de G deux à deux non semblables, toute K-représentation irréductible de G est semblable à l'une de celles-ci.

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