Astérisque

MICHEL ENGUEHARD

Caractérisation des groupes de Ree

Astérisque, tome 142-143 (1986), p. 49-139

<http://www.numdam.org/item?id=AST_1986__142-143__49_0>

Société Mathématique de France
Astérisque 142-143 (1986)

CARACTÉRISATION DES GROUPES DE REE

En 1960, Rimhak Ree [21] a démontré l'existence d'une série infinie de groupes simples finis, parfois appelés "groupes de Chevalley tordus de type G_2"; si K est un corps fini, de caractéristique 3, cardinal q, et dont le groupe des automorphismes est d'ordre impair, le groupe de Chevalley de type G_2 sur K admet un automorphisme involutif particulier, dont le groupe des points fixes, noté ${}^2G_2(q)$ est celui qui nous intéresse. Plus généralement, le groupe ${}^2G_2(F)$ peut être défini pour tout corps F de caractéristique 3 et admettant un endomorphisme dont le carré est le Frobenius. J. Tits a donné de ${}^2G_2(F)$ une belle construction géométrique [29].

Les groupes ${}^2G_2(q)$ ont les propriétés suivantes

(a) ${}^2G_2(q)$ est d'ordre $q^3(q^3 + 1)(q - 1)$ et est simple si $q > 3$;

(b) si t est une involution de ${}^2G_2(q)$, le centralisateur de t dans

$^2G_2(q)$ est isomorphe au produit direct de $\langle t \rangle$ par le groupe unimodulaire $PSL_2(q)$; les 2-groupes de Sylow de $^2G_2(q)$ sont abéliens élémentaires d'ordre 8;

(c) l'opération de $^2G_2(q)$ sur l'ensemble de ses 3-groupes de Sylow est deux fois transitive de degré $(q^3 + 1)$.

Les groupes tordus de type G_2, ou groupes de Ree, jouent un rôle important dans la classification des groupes simples finis, au même titre que les groupes PSL_2 ou les groupes de Suzuki, à la fois comme groupes deux fois transitifs et comme groupes dont les 2-groupes de Sylow ont une structure simple. Dans sa classification des groupes dont les 2-groupes de Sylow sont abéliens, J. H. Walter [31], [32] démontre essentiellement le théorème suivant

" Soit G un groupe simple dont les 2-groupes de Sylow sont abéliens et ne peu-
" vent être engendrés par moins de trois éléments. Soit t une involution de G.
" Alors l'une des assertions (i), (ii) est vraie
" (i) Le centralisateur de t dans G admet un seul 2-groupe de Sylow.
" (ii) Il existe une puissance q d'un nombre premier telle que le centralisa-
" teur de t dans G soit isomorphe à $\langle t \rangle \times PSL_2(q)$.

On voit qu'on est amené à caractériser des groupes simples par la structure du centralisateur d'une involution, programme déjà proposé par R. Brauer au Congrès d'Amsterdam [3].

L'assertion (i) conduit aux groupes PSL_2 en caractéristique 2, caractérisés par Suzuki [24].

L'assertion (ii) conduit aux groupes $^2G_2(q)$, avec quelques singularités pour $q \leqslant 5$; introduisons les conditions suivantes portant sur un groupe fini G

(R1) G n'a pas de sous-groupe d'indice 2 .

(R2) Les 2-groupes de Sylow de G sont abéliens.

(R3) Il existe un entier primaire q et une invoution t de G tels que $C_G(t)$ soit isomorphe au produit direct $\langle t \rangle \times PSL_2(q)$.

Walter [32], Brauer, Suzuki [24] et Janko [19]ont élucidé le cas q = 3 :

" Soit G un groupe non résoluble tel que (R1), (R2) et (R3); si q = 3, G
" est isomorphe à $P\Gamma L_2(8)$.

Janko [18]a obtenu pour q = 5 le "premier groupe de Janko", premier groupe simple sporadique découvert depuis Mathieu

" Soit G un groupe fini tel que (R1), (R2) et (R3). Si q = 5, G est
" simple d'ordre 175 560 et unique à isomorphisme près.

Pour q > 5, la caractérisation des groupes tels que (R1), (R2) et (R3) ou "groupes du type de Ree" est restée en suspens pendant près de 20 ans. Notre but ici est de décrire comment les travaux de H. N. Ward [33] Z. Janko et J. G. Thompson [28], J. G. Thompson [20] et Bombieri [1] permettent d'énoncer le théorème

" Soit G un groupe fini tel que (R1), (R2) et (R3). Si q est supérieur à 5,
" q est une puissance impaire de 3 et G est isomorphe à ${}^2G_2(q)$.

Les pages qui suivent rendent compte, avec quelques détails supplémentaires, d'exposés faits en novembre et décembre 1981. Tout en restant très explicites, nous nous sommes efforcés d'écourter les démonstrations originales, et y sommes parvenus dans quelque mesure.

Le chapitre 1 est consacré au rappel de quelques énoncés plus ou moins classiques et d'ailleurs peu nombreux. On notera surtout les caractérisations des groupes PSL_2 par Gorenstein et Walter [15] (proposition 1.7) et par M. Suzuki [24] (proposition 1.6). Les propositions suivantes concernent les propriétés des p-blocs de caractères d'un groupe fini et leur décomposition en blocs. Parmi celles-ci, il faut signaler la proposition 1.23, qui utilise le lien entre certaines constantes de structure d'un groupe G et celles d'un sous-groupe contenant $C_G^*(u)$, où u est un r-élément réel de G (1); la proposition 1.23 sera utilisée plusieurs fois aux chapitres 2 et 3.

(1) nous disons qu'un élément x de G est réel si seulement si x est conjugué de son inverse dans G; $C_G^*(x)$ désigne l'ensemble des éléments de G qui centralisent x ou le conjuguent en son inverse. Les autres notations sont standard.

Les trois chapitres suivants reprennent [20] et [33]; cependant nous n'avons pas donné le calcul de la table complète des caractères irréductibles du groupe G satisfaisant à (R1), (R2) et (R3); on la trouvera dans [33]. Des considérations élémentaires et l'utilisation du transfert permettent de montrer rapidement que q est impair, G est simple, et de décrire la structure 2-locale de G. Malgré l'emploi de la proposition 1.7, on ne parvient pas à élucider immédiatement la structure locale de G pour les premiers divisant $(q^2 - 1)/8$ (cf les assertions (5) et (7) du chapitre 2). La théorie des 2-blocs et la proposition 1.23 sont sollicitées une première fois pour montrer que la caractéristique est 3 (au chapitre 1, (8) et (9)).

La connaissance de la structure r-locale d'un groupe fini G, pour un premier r, permet en général de calculer un sous-module de l'anneau de Grothendieck $R(G)$ de G. Ainsi la connaissance des centralisateurs des r-sous-groupes (avec les morphismes induits par la conjugaison dans G) permet de calculer le module des caractères généralisés de G qui sont constants sur les éléments r-réguliers, et ceci bloc par bloc (Ll. Puig, communication orale). Dans les hypothèses (Ri), les circonstances favorables sont, pour r = 2, d'une part le faible défaut, d'autre part l'existence d'isométries résultant du contrôle par $C_G(t)$ lui-même de la fusion dans les $\{2,3\}'$-sous-groupes de $C_G(t)$ (notations de (R3)) (cf. aux chapitres 3, (3) et 2, (5)). Ces sous-groupes, cycliques, se partagent en deux familles, ceux dont l'ordre divise $(q - 1)/2$ et ceux dont l'ordre divise $(q + 1)/4$. Dans chaque famille ils sont à intersection triviale dans G, comme ils le sont dans $C_G(t)$. On parvient ainsi à calculer les matrices de décomposition généralisées relatives aux 2-blocs de défaut non nul, et les valeurs des caractères de ces blocs sur les éléments dont l'ordre divise $(q^2 - 1)$. La proposition 1.23, utilisée à deux reprises, permet en particulier de calculer l'ordre de G.

La détermination de la structure 3-locale de G (chapitre 4) exige une avancée plus pénible vers la table des caractères de G, par l'emploi des formules d'orthogonalité, etc... Un 3-groupe de Sylow U de G est d'ordre q^3, de classe 3, et admet, dans son normalisateur dans G, un groupe cyclique d'automorphismes H,

d'ordre $(q - 1)$. Seul le 2-Sylow de H a des points fixes sur $(U - \{1\})$. En outre, si x est un élément de $([U,U] - Z(U))$, $C_U(x) = [U,U]$. Ces propriétés permettent de déterminer $B = N_G(U)$ modulo le choix d'un certain automorphisme σ de $\mathbb{F}_q$ (cf chapitre 4, (4) et l'article qui précède). Dans le cas des groupes ${}^2G_2(q)$, on a $\sigma^2 = 3$. Avant de déterminer σ, on classifie sans difficulté au chapitre 5 les sous-groupes de G dont l'ordre est premier à $q^2 - q$.

Le groupe G étant extension transitive d'un certain groupe $B(\sigma)$, opérant sur $B(\sigma)/H$ (cf. chapitre 4, (2)), il suffit maintenant de démontrer que

(a) le carré de σ est l'automorphisme de Frobenius;

(b) si (a) est vrai, l'extension est unique.

L'assertion (a) est démontrée grâce à une propriété de σ (la "condition de Thompson", [28] II), propriété qui résulte de l'existence de l'extension. Une extension de $B(\sigma)$ opérant comme indiqué plus haut sur $B(\sigma)/H$, est en effet définie par deux applications

$$\omega : (U - \{1\}) \longrightarrow (U - \{1\})$$

$$\rho : (U - \{1\}) \longrightarrow H$$

satisfaisant à certaines conditions dont la plus complexe exprime l'associativité du produit. Plus précisément, ω et ρ sont définies, après choix d'un élément s (ici d'ordre 2) qui normalise H mais n'est pas dans H, par

$$\text{si } u \in (U - \{1\}) \quad \text{sus} \in \omega(u)s U \rho(u) .$$

(le fait que G soit 2 fois transitif sur G/B, U étant régulier sur $(G/B - \{B\})$ implique l'existence d'une décomposition à la Bruhat). Encore faut-il, pour écrire que le produit est associatif, connaître ω en quelque endroit.
On démontre (chapitre 6, (1)) que ${}^2G_2(3)$, c'est-à-dire $P\Gamma L_2(8)$, est plongé dans G, l'injection étant précisée à un paramètre $d \in \mathbb{F}_q$ près. Celà permet de calculer ω sur [U,U], en fonction de d et σ et la condition de Thompson s'en déduit (formules 21 et 22, chapitre 6).

C'est Bombieri [1] qui a montré que cette condition impliquait (a), sauf peut-être pour un nombre fini de cas, lesquels ont été traités par calcul sur ordinateur. Ayant remarqué que sa démonstration valait pour un

corps infini, nous démontrons (a) sans l'hypothèse "K fini" (cf le théorème chap. 7). La démonstration de Bombieri consiste essentiellement à

1) déduire de la condition de Thompson l'existence d'un polynôme $H \in \mathbf{F}_3[Z_i]$ $(0 \leqslant i \leqslant 4)$ tel que

$$(*) \quad H(z^{\sigma^i}) = 0 \quad \text{pour tout } z \in K ,$$

2) à en conclure, grâce à un lemme élémentaire, à l'existence d'une relation de la forme

$$(**) \quad \sigma^{\ell} = 3^{\pm\lambda} \quad \text{où} \quad 0 \leqslant \ell \leqslant 4 \quad \text{et} \lambda \in \mathbf{N} , \lambda \text{ étant}$$

majoré par une fonction des degrés partiels de H.

Notre lemme 6 (chapitre 7,(2)(a)) ([1]) et son corollaire remplacent le lemme 3 de [1]. Comme en outre le corps des points fixes de σ est par hypothèse le corps premier $\mathbf{F}_3$, il est clair qu'il suffit de se ramener à $\ell = 0$ ou $\ell = 1$ ou $\sigma^2 = 3$ dans (*) et (**). Pour diminuer ℓ, on revient en arrière dans la procédure d'élimination qui conduit de la condition de Thompson à (*) : en utilisant (**), on peut restreindre les valeurs de i dans (*), donc aussi ℓ dans (**) (cf ch. 7, (2)(b)).

On ne peut éviter de poser la question : à quelles conditions l'existence d'une extension transitive de $B(\sigma)$ (défini comme au chapitre 4, (4), mais sur un corps K d'ordre infini de caractéristique 3) impose-t-elle $\sigma^2 = 3$. Nous n'avons pas de résultats significatifs dans cette direction. Dans le cas fini, le plongement de ${}^2G_2(3)$ dans G est exhibé à l'aide d'un élément d'ordre 7 qui opère comme on l'imagine sur un 2-groupe abélien élémentaire d'ordre 8 et est lui-même inversé par une involution... Au paragraphe (2) du chapitre 6, que K soit fini n'importe pas.

([1]) Ce lemme a été généralisé par J.-Y Hée (communication orale); cf aussi la proposition 2.1, dans J. Tits, Homomorphismes "abstraits de groupes algébriques simples, Ann. of Math., 97 (1973), p.508.

Pour démontrer l'assertion (b) plus haut, on revient aux corps finis, en reprenant [28]III sans grand changement. La connaissance de σ permet de montrer que d est nul, par un calcul en partie laissé au lecteur. Pour conclure à l'unicité de ω est utilisée la géométrie formée par les ensembles de points fixes d'involutions de G (dans son opération sur G/B). On démontre que cette géométrie est déterminée par les relations en ω déjà obtenues au chapitre 6 et la connaissance de σ, et qu'en conséquence l'application ω est elle-même déterminée. La tâche est relativement facile parce-que d'une part $C_G(t)$ a seulement trois orbites dans son opération sur G/B, et d'autre part B a seulement trois orbites dans son opération par conjugaison sur l'ensemble des involutions de G.

1. PRÉALABLES

Proposition 1.1. (Zassenhaus, Brauer, Wielandt [34]) *Soit X un groupe fini sur lequel opère un groupe de Klein $Q = \{1, t_1, t_2, t_3\}$. Soient*

$$X_j = C_X(t_j) , \quad j = 1, 2, 3.$$

(1) Si $X_1 = \{1\}$, X est abélien et $t_1(x) = x^{-1}$ pour tout $x \in X$.

(2) Si X est d'ordre impair, on a

$$X = X_1X_2X_3 \quad \text{et} \quad |X||C_X(Q)|^2 = |X_1||X_2||X_3| .$$

Si en outre $C_X(Q) = \{1\}$, les groupes X_1, X_2 et X_3 sont abéliens.

Proposition 1.2. (Janko, Thompson [20] p.287) *Soient D un groupe diédral d'ordre $2n$, où n est impair, C le sous-groupe d'indice 2 de D et t une involution de D. Si D opère sur un groupe X d'ordre premier à 2 de telle sorte que C opère sans point fixe sur X, on a*

$$|C_X(t)|^2 = |X| .$$

Démonstration.

Pour tout nombre premier p, D normalise un p-groupe de Sylow de X, soit P, et $C_P(t)$ est alors un p-groupe de Sylow de $C_X(t)$. On peut donc supposer que X est un p-groupe.

Pour tout sous-groupe normal Y de X stable par D on a

$$C_{X/Y}(t) = C_X(t)Y/Y$$

soit
$$|C_X(t)| = |C_Y(t)||C_{X/Y}(t)|$$

et C opère sans point fixe sur Y et sur Y/X.

En considérant une D-suite de composition de X, on voit qu'il suffit de démontrer la proposition sous l'hypothèse "X est un p-groupe abélien élémentaire".

Or toute représentation fidèle de D en caractéristique p est induite d'une représentation de C; l'espace des points fixes de t est donc de dimension moitié de la dimension de l'espace de la représentation, ce qui démontre

$$|C_X(t)|^2 = |X|.$$

Proposition 1.3. (Burnside) *Soient X un groupe fini, P un groupe de Sylow de X, et A et B deux sous-ensembles normaux de P. Si A et B sont conjugués dans X, A et B sont conjugués dans $N_X(P)$.*

Proposition 1.4. (transfert) *Soient X un groupe fini, P p-groupe de Sylow de X. On suppose que P est abélien et que X n'a pas d'image d'ordre p. On a*

$$P \cap Z(N_X(P)) = \{1\}.$$

Proposition 1.5. (Huppert [16] IV.8.6) *Soient X un groupe fini et P un p-groupe de Sylow de X. On suppose que P est métacyclique non abélien, d'ordre impair. Alors X admet une image d'ordre p.*

Proposition 1.6. (Suzuki [24]) *Soit G un groupe d'ordre pair tel que le centralisateur dans G de toute involution de G soit abélien.*

Ou bien (i) les 2-groupes de Sylow de G sont cycliques,

ou bien (ii) un 2-groupe de Sylow de G est normal dans G,

ou bien (iii) G est isomorphe au produit direct d'un groupe abélien d'ordre impair par $PSL_2(2^n)$.

Proposition 1.7. (Gorenstein et Walter [15]) *Soit G un groupe fini dont les 2-groupes de Sylow sont diédraux. On suppose que le centralisateur dans G d'une involution du centre d'un 2-groupe de Sylow admet un 2-complément abélien. Alors G admet un sous-groupe normal d'ordre impair H tel que G/H soit isomorphe à l'un des groupes suivants*

un 2-groupe de Sylow de G, $PSL_2(q)$, $PGL_2(q)$ ($p \equiv 3, 5 \pmod 8$), A_7.

(on n'utilisera cette proposition que dans le cas très particulier où un 2-groupe de Sylow de G est d'ordre 4 égal à son centralisateur, ce qui élimine les groupes $PGL_2(q)$ et A_7)

Proposition 1.8. *Soient p un nombre premier au moins égal à 5 et X un sous-groupe d'ordre impair de $GL_3(p)$. Un p-groupe de Sylow de X est normal dans X.*

En effet X est résoluble d'après le théorème de Feit et Thompson [12]. Selon le théorème de Hall et Higman [17], si p divise l'ordre de X, X admet un p-sous-groupe normal non trivial; donc X a un p-groupe de Sylow normal.

La fin de ce paragraphe est consacré à la théorie de Brauer [2] à [8] . Il a paru plus commode, quitte à quelques longueurs, de rappeler la plupart des résultats. Sauf référence expresse ils sont démontrés dans les livres de Dornhoff [11] et de Goldschmidt [14]. On en profite pour fixer quelques notations.

Une fois pour toutes G est un groupe fini.

On fixe un nombre premier p, un corps K de caractéristique nulle, suffisamment gros, complet pour une valuation discrète associée à p, et on désigne par A l'anneau de valuation de K, par k le corps résiduel, qui est donc de caractéristique p.

On note Irr(G) l'ensemble des caractères absolument irréductibles de G (en caractéristique nulle) et on suppose que tout élément de Irr(G) est à valeurs dans A. On note $R(G)$ le $\mathbb{Z}$-module engendré par les éléments de Irr(G).

A toute représentation de G sur k Brauer associe un"caractère modulaire" que nous considérerons comme une fonction centrale sur G, à valeurs dans A, et nulle sur les classes non p-régulières. Soit $R_p(G)$ le $\mathbb{Z}$-module engendré par l'ensemble $\mathrm{Irr}_p(G)$ des caractères modulaires irréductibles de G.

A la réduction des représentations de G sur A en des représentations sur k correspond l'application

$$d : R(G) \longrightarrow R_p(G)$$

où $d(\chi)$ coïncide avec χ sur les classes p-régulières.

Une fonction sur G et à valeurs dans X (X = K, A, k ...) définit naturellement une forme X-linéaire sur l'anneau de groupe XG. En particulier une fonction centrale sur G définit une forme sur le centre ZXG de XG .

Si $\chi \in \mathrm{Irr}(G)$, la restriction de $\chi/\chi(1)$ à ZAG est à valeurs dans A; elle définit par réduction un caractère de $Zk G$, noté ω_χ.

Un p-bloc (ou bloc, si p est fixé) de G est un idempotent primitif de ZAG. Comme tout élément de AG, un bloc b permute les fonctions définies sur AG, par

$$(b.\xi)(u) = \xi(bu) \quad (u \in AG).$$

Il stabilise en particulier le module des formes A-linéaires sur ZAG, et, par réduction, celui des formes k-linéaires définies sur $Zk G$. On obtient ainsi des décompositions en sommes directes

$$R(G) = \sum_b b.R(G) \qquad \text{et} \qquad R_p(G) = \sum_b b.R_p(G)$$

(b parcourant l'ensemble des blocs de G)

et l'application de décomposition commute à l'action des blocs, d'où

$$d_b : b.R(G) \longrightarrow b.R_p(G) .$$

Plus précisément on a aussi

Proposition 1.9. *Soit* $\chi \in (Irr(G) \cup Irr_p(G))$, *et soit b un bloc de G. On a*

$$b.\chi = \chi \quad \textit{ou} \quad b.\chi = 0 .$$

Si, dans les notations de 1.9, on a $b.\chi = \chi$, on dira que "χ est dans b" ou même que "b contient χ".

La matrice de décomposition de b, matrice de d_b relativement aux bases $b.\mathrm{Irr}(G)$ et $b.\mathrm{Irr}_p(G)$ de $b.R(G)$ et $b.R_p(G)$, sera noté D_b; la matrice de Cartan sera notée C_b (on a $C_b = D_b.{}^t(D_b)$). Rappelons

Proposition 1.10. *(a) Les coefficients de* D_b *sont des entiers naturels.*

(b) D_b *est indécomposable en blocs.*

(c) C_p *est non singulière.*

A tout bloc b de G est associée une classes de p-sous-groupes de G, dits groupes de défaut de b. Posons

$$|G|_p = p^\alpha \quad \text{et, si D est groupe de défaut de b,} \quad |D| = p^{\alpha(b)}.$$

L'entier $\alpha(b)$ est le défaut de b.

Proposition 1.11. *Deux éléments* χ *et* ξ *de* $Irr(G)$ *sont dans le même bloc si et seulement si*

$$\omega_\chi = \omega_\xi .$$

Pour celà il suffit que ω_χ *et* ω_ξ *coïncident sur les classes p-régulières.*

Proposition 1.12. *Le bloc b de G est de défaut* β *si et seulement si*

(1) si $\chi \in b.Irr(G)$, $p^{\alpha-\beta}$ *divise* $\chi(1)$,

et (2) il existe $\chi \in b.Irr(G)$ *tel que* $\chi(1)/p^{\alpha-\beta}$ *soit premier à p.*

Proposition 1.13. ([8]) *Si* $\beta \in \{0,1,2\}$, *un élément* χ *de* $Irr(G)$ *est dans un bloc de défaut* β *si et seulement si* $\chi(1)/p^{\alpha-\beta}$ *est un entier premier à p.* [1]

Proposition 1.14. ([8]) *Soit b un bloc de G de défaut* β.

(a) Si β *n'est pas nul,* $|b.Irr(G)| > |b.Irr_p(G)|$.

(b) Si $\beta \leqslant 2$, $|b.Irr(G)| \leqslant p^\beta$.

Proposition 1.15. *Le nombre de blocs de défaut maximum est égal au nombre de classes p-régulières qui rencontrent le centralisateur d'un p-groupe de Sylow de G.*

Soit L un sous-groupe de G. Brauer a défini une application, dite correspondance de Brauer, et que nous noterons Br_L^G, qui transforme certains blocs de L en des blocs de G.

Proposition 1.16. *Soient D un p-sous-groupe de G et H et L des sous-groupes de G tels que*

$$DC_G(D) \subset L \subset N_G(D) \quad \text{et} \quad L \subset H.$$

(a) Pour tout bloc b de L, $Br_L^G(b)$ *est un bloc de G et D est contenu dans un groupe de défaut de* $Br_L^G(b)$.

(b) $Br_H^G(Br_L^H(b))$ *est défini et égal à* $Br_L^G(b)$.

([1]) proposition généralisée par P. Fong sous l'hypothèse "le groupe défaut est abélien" in Trans. Amer. Math. Soc. 103 (1962) 484-494.

Proposition 1.17. *Soient D un p-sous-groupe normal de G et L = $DC_G(D)$. Soit E l'ensemble des éléments de Irr(L/D) qui sont dans un bloc de défaut nul et dont le stabilisateur dans G/L est un p'-groupe. Tout bloc de groupe de défaut D de G stabilise une et une seule orbite selon G/L dans E et on définit ainsi une bijection entre l'ensemble des blocs de G de groupe de défaut D et l'ensemble quotient E/(G/L).*

Proposition 1.18. (Brauer's First Main Theorem) *Soient D un p-sous-groupe de G et H un sous-groupe de G contenant $N_G(D)$. La correspondance de Brauer de H à G induit une bijection entre l'ensemble des blocs de H de groupe de défaut D et l'ensemble des blocs de G de groupe de défaut D.*

On appelle bloc principal de G, et on note $b_o(G)$, le bloc de G qui contient 1_G. Le Bloc principal est toujours de défaut maximum α.

Proposition 1.19. *Soient D, H et G comme en 1.16. On a*

$$Br_H^G(b) = b_o(G)$$

si et seulement si $b = b_o(H)$.

Pour énoncer le deuxième théorème fondamental de Brauer, nous posons, (cf [10])

si u est un p-élément de G, et B un bloc de G,

$$Br^{u,G}(B) = \sum_b b \qquad (b \text{ bloc de } C_G(u) \text{ tel que } Br^G_{C_G(u)}(b) = B)$$

En outre, si χ est une fonction centrale sur G, on définit $d^{u,G}(\chi)$, fonction centrale sur $C_G(u)$, par

$$(d^{u,G}(\chi))(s) = \chi(us) \quad \text{si s est p-régulier et } s \in C_G(u)$$

$$= 0 \qquad \text{sinon.}$$

Enfin notons $\mathbb{Z}_u$ l'anneau obtenu en adjoignant à $\mathbb{Z}$ les racines de l'unité d'ordre l'ordre de u.

Proposition 1.20. (Brauer's Second Main Theorem) *Soient u un p-élément et b un bloc de G. On a*

$$d^{u,G}(b.R(G)) \subset \mathbb{Z}_u \otimes (Br^{u,G}(b).R_p(C_G(u)) .$$

La restriction de $d^{u,G}$ à $b.R(G)$ est définie, relativement aux bases $b.Irr(G)$ et $Br^{u,G}.Irr_p(C_G(u))$, par une matrice à coefficients dans $\mathbb{Z}_u$, qui sera notée $D_b^{u,G}$ ou D_b^u .

Proposition 1.21. *Soient u et v deux p-éléments de G et b un bloc de G.*

(a) Si u et v ne sont pas conjugués dans G, on a

$$D_b^{u,G}.{}^{\tau}(D_b^{v,G}) = 0 .$$

(b) Pour des ordres convenables et cohérents sur les bases de $b.R(G)$ et de $Br^{u,G}(b).R_p(C_G(u))$ et sur les blocs de $C_G(u)$ dont $Br^{u,G}(b)$ est la somme on a

$$D_b^{u,G}.{}^{\tau}(D_b^{u,G}) = diag_e(C_e) \qquad (Br^G_{C_G(u)}(e) = b)$$

Si $\mathcal{D}$ est un sous-ensemble de G, on pose

$$R(G|\mathcal{D}) = \{\chi \in R(G)/\ \chi \text{ est nulle sur } G-\mathcal{D}\}.$$

Proposition 1.22. ([15]Proposition 25, [30]). *Soit $\mathcal{D}$ un sous-ensemble à intersections triviales de G, de normalisateur H. On suppose que $\mathcal{D}$ est réunion de p-sections de H. Si b est un bloc de H tel que $b.R(H|\mathcal{D})$ soit non nul, $Br^G_H(b)$ est défini et on a*

$$Ind^G_H(b.R(H|\mathcal{D})) \subset Br^G_H(b).R(G) .$$

Démonstration: Il résulte de 1.20 que l'opération selon b commute à la multiplication par la fonction caractéristique d'une p-section ([10]). On a donc

$$b.R(H|\mathcal{D}) = b.R(H) \cap R(H|\mathcal{D}) .$$

Il résulte donc de la proposition 1.20 que si $b.R(H|\mathcal{D})$ n'est pas nul, il existe un p-élément u de $\mathcal{D}$ tel que $d^{u,H}(b.R(H))$ ne soit pas nul, donc il existe un bloc b_u de $C_G(u) = C_H(u)$ tel que $b = Br^G_{C_G(u)}(b_u)$.

Selon 1.16, $Br^{G}_{C_G(u)}(b_u)$ est défini et égal à $Br^{G}_{H}(b)$.

Soit B un bloc de G autre que $Br^{G}_{H}(b)$. Il nous faut démontrer que si $\theta \in b.R(H|\mathcal{D})$, alors $B.(Ind^{G}_{H}(\theta)) = 0$.

Il suffit pour celà que pour tout p-élément v de G on ait

$$d^{v,G}(B.(Ind^{G}_{H}(\theta))) = 0$$

soit
$$Br^{v,G}(B).d^{v,G}(Ind^{G}_{H}(\theta)) = 0 .$$

Mais puisque $\mathcal{D}$ est à intersections triviales et réunion de p-sections, on bien $d^{v,G}(Ind^{G}_{H}(\theta))$ est nul, ou bien v a un conjugué dans $\mathcal{D}$; supposons donc que $v = u$, et on a alors

$$d^{u,G}(Ind^{G}_{H}(\theta)) = d^{u,H}(\theta) .$$

Finalement on a

$$d^{u,G}(B.Ind^{G}_{H}(\theta)) = Br^{u,G}(B).d^{u,H}(\theta)$$
$$= Br^{u,G}(B)Br^{u,H}(b).d^{u,H}(\theta) \quad \text{(par 1.20)}$$

Or il est clair que

$$Br^{u,G}(B)Br^{u,G}(Br^{G}_{H}(b)) = 0$$

et il en résulte par 1.16 que

$$Br^{u,G}(B)Br^{u,H}(b) = 0 .$$

Proposition 1.23 (Suzuki [25] Brauer [6]) *Soient u un p-élément de G et H un sous-groupe de G tels que*

$$C^{*}_{G}(u) \subset H \subset G .$$

Soient K_1 et K_2 deux classes d'involutions de G. On pose

si $\chi \in R(G)$, $\chi^{(i)} = \sum_{s \in K_i} \chi(s)$

si $\theta \in R(H)$, $\theta^{(i)} = \sum_{s \in (K_i \cap H)} \theta(s)$ $\qquad (i = 1, 2)$

Soient b_u un bloc de $C_G(u)$, $b = Br^{H}_{C_G(u)}(b_u)$ et $B = Br^{G}_{C_G(u)}(b_u)$. On a

$$\frac{1}{|H|} \sum_{\theta \in b.Irr(H)} \frac{\theta^{(1)}\theta^{(2)}}{\theta(1)} \delta^{\phi}_{\theta} = \frac{1}{|G|} \sum_{\chi \in B.Irr(G)} \frac{\chi^{(1)}\chi^{(2)}}{\chi(1)} \delta^{\phi}_{\chi}$$

pour tout élément ϕ de $b_u.Irr_p(C_G(u))$.

((δ^{ϕ}_{θ}) est la matrice de décomposition $D^{u,H}_{b}$, et (δ^{ϕ}_{χ}) est $D^{u,G}_{B}$)

Posons

$$a_H = \frac{1}{|H|} \sum_{\theta \in Irr(H)} \frac{\theta^{(1)}\theta^{(2)}}{\theta(1)}\theta \qquad \text{et} \quad a_G = \frac{1}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi^{(1)}\chi^{(2)}}{\chi(1)}\chi$$

D'après le deuxième théorème fondamental de Brauer 1.20, il suffit de démontrer que

$$d^{u,H}(a_H) = d^{u,G}(a_G) .$$

Or, si $g \in G$, $a_G(g)$ est le cardinal de l'ensemble des $(s,t) \in K_1 \times K_2$ tels que $st = g$; de même $a_H(h)$, pour $h \in H$, est le cardinal de l'ensemble des couples $(s,t) \in (K_1 \cap H) \times (K_2 \cap H)$ tels que $st = h$.

On voit que ces deux ensembles coïncident sur la p-section de u dans $C_G(u)$, en raison de l'inclusion de $C_G^*(u)$ dans H.

Nous appliquerons cette proposition dans le cas où $K = K_1 = K_2$ est une classe d'involutions de G. En utilisant une base $\{\phi\}_\phi$ du $\mathbb{Z}$-module $b_u.R_p(C_G(u))$ et les matrices de décomposition

$$D_b^{u,H} = (\delta_\theta^\phi) \ , \ D_B^{u,G} = (\delta_\chi^\phi) \ ,$$

on pose

$$A(e,\phi) = \frac{1}{|X|} \sum_{\zeta \in e.Irr(X)} \frac{\zeta(1)^2}{\zeta(1)} \delta_\zeta^\phi \qquad (X = H, \ G \ \text{ et e bloc de X})$$

et on a dans les hypothèses de 1.23

[B-Z] $$A(b,\phi) = A(B,\phi) .$$

Proposition 1.24. *Soient b un bloc de G et u un p-élément de G. Soit x un élément de G qui n'est pas dans la p-section de u. On a*

$$D_b^u\,(\chi(x))_{\chi \in b.Irr(G)} = 0 .$$

Démonstration: posons $x = vy = yv$, où v est un p-élément et y est p-régulier. On a d'après 1.20

$$\chi(x) = d^{v,G}(\chi)(y)$$

soit $$(\chi(x))_{\chi \in b.Irr(G)} = {}^t(D_b^{v,G})\,(\phi(y))_{\phi \in Br^{u,G}(b).Irr(C_G(v))}$$

On voit que 1.24 résulte de 1.21.(a).

On note $\sigma(\chi)$ l'indice de Schur-Frobenius d'un caractère irréductible χ de G.

Proposition 1.25. *(p = 2) Soit u ∈ G tel que <u> soit un 2-sous-groupe cyclique maximal de G, et soit b un 2-bloc de G. On a*

$$D_b^{u,G}(\sigma(\chi))_{\chi \in b.Irr(G)} = 0 .$$

Démonstration. Soit

$$Sh_G = \sum_{\chi \in Irr(G)} \sigma(\chi)\chi .$$

Si l'on tient compte de 1.20, on voit que la proposition affirme simplement que

$$d_b^{u,G}(Sh_G) = d^{u,G}(b.Sh_G) = 0 .$$

Il suffit donc de démontrer que $d^{u,G}(Sh_G) = 0$.

Or $Sh_G(x)$ est le cardinal de l'ensemble des $y \in G$ tels que $y^2 = x$. L'hypothèse faite sur u implique clairement que si x appartient à la 2-section de u, cet ensemble est vide; $Sh_G(x)$ est alors nul.

La théorie dite "des caractères exceptionnels" sera appliquée dans des circonstances très favorables de contrôle fort de fusion, ce qui nous conduit à énoncer la

Proposition 1.26. *Soient N un sous-groupe de G et $\mathcal{D}$ un sous-ensemble de N tels que*

si $x \in \mathcal{D}$, $g \in G$ et $x^g \in N$, alors $x^g \in \mathcal{D}$ et $g \in N$.

Soit $E = \bigcup_{g \in G} \mathcal{D}^g$. L'induction de N à G et la restriction de G à N induisent des isométries réciproques entre $R(N|\mathcal{D})$ et $R(G|E)$. Si Θ est une isométrie d'un sous-module R' de $R(N)$ contenant $R(N|\mathcal{D})$ et qui prolonge la restriction de Ind_N^G à $R(N|\mathcal{D})$, on a

si $x \in \mathcal{D}$, $\chi \in R'$, $\Theta(\chi)(x) = \chi(x)$.

Démonstration. L'hypothèse implique que $\mathcal{D}$ est à intersection triviales dans G, de normalisateur N, et que $\mathcal{D} = E \cap N$. Il est bien connu ([16],V.22.7) que dans ces conditions on a

$Ind_N^G(\zeta(x)) = \zeta(x)$ pour tout $\zeta \in R(N|\mathcal{D})$ et tout $x \in \mathcal{D}$, Ind_N^G étant isométrique sur $R(N|\mathcal{D})$. On en déduit la première assertion.

Soient $\chi \in R'$, $\zeta \in R(N|\mathcal{D})$; on a par hypothèse, et grâce à la formule de Frobenius,

$$(\mathrm{Res}_N^G(\Theta(\chi)) - \chi \ , \ \zeta) = (\Theta(\chi) \ , \ \mathrm{Ind}_N^G(\zeta)) - (\chi,\zeta) = 0.$$

Mais $R(N|\mathcal{D})$ engendre l'espace de toutes les fonctions centrales sur N et nulles hors de $\mathcal{D}$; son orthogonal dans $R(N)$ n'est autre que le module des éléments de $R(N)$ qui sont nuls sur $\mathcal{D}$. Ceci démontre la dernière assertion de 1.26.

2. LA CARACTÉRISTIQUE EST 3.

Quelques notations (définitives).

G est un groupe fini; t est une involution de G; p est un nombre premier q est une puissance de p; $q > 5$; on suppose (R1), (R2) et (R3).

On pose $C_G(t) = \langle t \rangle \times F$ (F isomorphe à $PSL_2(q)$); P est un p-groupe de Sylow de F; S est un 2-groupe de Sylow de G contenant t.

Dans ce paragraphe on étudie la structure 2-locale de G et on démontre que p est égal à 3.

(1) *q est impair; S est abélien élémentaire d'ordre 8. Toutes les involutions de G sont conjuguées dans G; tous les sous-groupes d'ordre 4 de G sont conjugués dans G.*

Soit $S_1 = S \cap F$.

Que q soit pair ou impair, S_1 est abélien élémentaire et il existe un sous-groupe cyclique T, d'ordre $(|S_1| - 1)$, de F tel que

$$N_G(S) \cap F = S_1.T$$

et T opère régulièrement sur $(S_1 - \{1\})$.

Soit X un complément de S dans $N_G(S)$, contenant T (il en existe en raison d'un théorème fondamental de Zassenhaus). Il résulte de la proposition 1.4 et de l'hypothèse (R2) que t n'est pas central dans $N_G(S)$; donc X est différent de T et on voit que tous les éléments de $(S - \{1\})$ sont conjugués sous l'action de X. Autrement dit toutes les involutions de G sont conjuguées dans G. En outre si U est un sous-groupe non trivial de T, le groupe $N_X(U)$ normalise $C_X(U) = \langle t \rangle$, et donc $N_X(U) = T$. Ainsi X est un groupe de Frobenius de complément T.

(a) Supposons q puissance de 2 : $q = 2^n$.

Le groupe de Frobenius X, d'ordre impair, est représenté fidèlement et irréductiblement en caractéristique 2 et dimension $(n + 1)$, sur S.

On a donc $n + 1 \geqslant |T|$, soit $n + 1 \geqslant 2^n - 1$,

ce qui contredit l'hypothèse $q > 5$.

(b) Selon (a) q est impair et S_1, diédral et abélien, est d'ordre 4. Donc $S = \langle t \rangle \times S_1$ est d'ordre 8. Le groupe T est d'ordre 3, X est nécessairement d'ordre 21; son noyau est engendré par un élément d'ordre 7, lequel opère régulièrement sur les involutions de S, comme sur les sous-groupes d'ordre 4 de S. L'assertion (1) est démontrée.

Notations [1]

Puisque S est abélien, on a $q \equiv 1 \pmod 4$ ou $q \equiv -1 \pmod 4$. Soit $e \in \{1,-1\}$ tel que $q - e \equiv 4 \pmod 8$.

On désigne par

C un sous-groupe cyclique d'ordre $(q + e)/2$ de F;

D un sous-groupe cyclique d'ordre $(q - e)/2$ de F;

s l'involution de D et on suppose que s normalise C; Le groupe $C\langle s \rangle$ est diédral;

u une involution de F qui normalise et ne centralise pas D; $D\langle u \rangle$ est diédral et s et u engendrent un 2-groupe de Sylow de F;

$Q = \langle t,s \rangle$; on suppose que S contient s et u;

E le sous-groupe d'indice 2 de D;

y un générateur de C et z un générateur de D.

(2) G est simple.

Soit L un sous-groupe normal non trivial de G. Si L est d'ordre impair, selon la proposition 1.1, il existe une involution t' de G telle que $C_L(t') \neq \{1\}$. Mais puisque F est simple et les involutions de G conjuguées, $C_G(t')$ n'admet aucun sous-groupe normal non trivial d'ordre impair. Donc L est d'ordre pair. Selon l'assertion (1) L contient toutes les involutions de G, et puisque F est simple, L contient $C_G(t)$. Ainsi L, comme G, satisfait à (R1) et (R3). Ou bien L admet une image d'ordre 2 ou bien les involutions

[1] Sauf précision contraire, ces notations sont valables pour les chapitres 2, 3, 4, 5, 6 et 8 .

de L sont conjuguées dans L (assertion (1)). Dans le premier cas, $\mathbf{O}^2(L)$ est d'ordre impair et normal dans G, donc réduit à $\{1\}$. Mais ceci implique que L est un 2-groupe de Sylow de G, ce qui est absurde. Dans le second cas, L est du même ordre que G, donc égal à G.

(3) Tout sous-groupe de G d'ordre impair et normalisé par un 2-groupe de Sylow de G est conjugué d'un sous-groupe de E.

Supposons que S normalise un sous-groupe K de G d'ordre impair, et soit v une involution de S telle que $|C_K(v)|$ soit maximal. On voit dans $C_G(v)$ (isomorphe à $C_G(t)$) que $C_K(v)$ est centralisé par une autre involution w de S. Le choix de v impose $C_K(v) = C_K(w) = C_K(vw)$. Mais selon 1.1, appliqué à K normalisé par $\langle v,w\rangle$, on a $K = C_K(v)$. L'assertion (3) résulte alors du fait que dans $F \approx PSL_2(q)$, tout sous-groupe d'ordre impair normalisé par un 2-groupe de Sylow est conjugué d'un sous-groupe de E.

(4) On a $C_G(Q) = S.E$ *et* $N_G(Q) = C_G(Q)\langle\mu\rangle$
où μ *est un élément d'ordre 3 tel que* $C_S(\mu) = \langle u\rangle$ *et qui normalise S et E.*

Ces propriétés se lisent dans $C_G(t)$ en tenant compte de l'assertion (1). En particulier on sait qu'un sous-groupe d'ordre 4 de $PSL_2(q)$ est normalisé et non centralisé par un élément d'ordre 3.

(5) Soit E_1 *un sous-groupe non trivial de E. On a* $N_G(E_1) = N_G(E)$
et ou bien $N_G(E) = N_G(Q)$, *ou bien* $N_G(E) \approx A_5 \times E\langle u\rangle$.

Il est clair que E_1 est caractéristique dans E et E caractéristique dans $N_G(Q)$ d'où

$$N_G(Q) \subset N_G(E) \subset N_G(E_1).$$

D'autre part Q centralise mais u ne centralise pas E_1, ce qui montre que $N_G(E_1)$ contient un sous-groupe d'indice 2, N, ne contenant pas u. On voit que

$$C_N(t) = Q.E$$

et les involutions de N sont conjuguées (action de μ). Selon le résultat de Suzuki rappelé en 1.6, on bien Q est normal dans N, ou bien N est produit direct

d'un groupe isomorphe à A_5 par un groupe d'ordre impair, qui ne peut être que E. Dans le premier cas Q est caractéristique dans N, donc $N_G(E_1) = N_G(Q)$. Dans le second cas, E est caractéristique dans N, donc $N_G(E_1) = N_G(E)$; l'involution u opère sur le groupe alterné en y centralisant un 2-groupe de Sylow, donc centralise le groupe alterné.

(6) 3 ne divise pas (q - e).

Supposons que 3 divise (q - e).

Il y a alors une classe d'éléments d'ordre 3 dans $C_G(t)$. Soit T un 3-groupe de Sylow de E, et soit μ' d'ordre 3 dans T. Puisque μ centralise une involution de S, μ et μ' sont conjugués dans G; soit $g \in G$ tel que

$$\mu' = g^{-1}\mu g .$$

Il est clair que $g \notin N_G(E)$. Soit $R = T\langle\mu\rangle$; R est un 3-groupe de Sylow de $C_G(T)$ (assertion (5)).

Soit U un complément de T dans E. Si μ centralise un élément non trivial de U, μ centralise un groupe de Sylow de U, soit V (pour un certain autre premier), donc μ' centralise V^g, et $V^g \neq V$, car $g \notin N_G(E) \supset N_G(V)$. Cependant $C_G(\mu')$ est contenu dans $N_G(E)$ (assertion (5))Selon l'assertion (5) E centralise V^g (qui ne peut être que d'ordre 5), donc $N_G(V^g) = N_G(V)^g = N_G(E)^g$ contient E. Mais, comme on le voit dans $N_G(E)$, E^g rencontre alors E non trivialement, d'où l'on conclut (assertion (5)) que $N_G(E) = N_G(E)^g$, donc g normalise E, ce qui est absurde. On est donc assuré que $C_U(\mu) = \{1\}$.

(a) Supposons T d'ordre 3, donc R abélien. On a

$$C_G(R) = C_G(\mu) \cap C_G(\mu') = C_G(\mu) \cap N_G(E) = R\langle u\rangle$$

et $N_G(R)/R\langle u\rangle$ est isomorphe à un sous-groupe de $GL_2(3)$.

Supposons d'abord que $N_G(R)$ possède un unique 3-groupe de Sylow N strictement plus grand que R. Puisque R est 3-groupe de Sylow de $C_G(T)$, T n'est pas central dans N; de même, μ' étant conjugué de μ dans G, $\langle\mu\rangle$ n'est pas central dans N. Cependant $R = N \cap C_G(T)$ doit contenir Z(N).

Or l'involution u, qui normalise T, centralise μ et inverse μ'; elle doit également normaliser Z(N), ce qui est impossible.

Supposons maintenant que $N_G(R)$ possède plusieurs 3-groupes de Sylow, ce qui implique (assertion (1)) que les 2-groupes de Sylow de $N_G(R)$ sont d'ordre 4 et leurs involutions conjuguées. Alors chacune de ces involutions fixe un sous-groupe d'ordre 3 de R, et ceci est impossible dans $GL_2(3)$ (par exemple la proposition 1.1 est contredite).

Finalement R est un 3-groupe de Sylow de G.

(b) Si $|T| > 3$, R est également groupe de Sylow de G:

En effet T contient alors un sous-groupe caractéristique différent de $\{1\}$ de R, soit T', et on a

$$N_G(R) \subset N_G(T') = N_G(E),$$

ce qui montre que R est groupe de Sylow de G.

Puisque G est simple (assertion (2)), R n'est pas métacyclique (proposition 1.5), donc R est abélien, comme en (a).

Les élements μ et μ' de R, qui sont conjugués dans G, doivent l'être dans $N_G(R)$ (proposition 1.3). Ce n'est le cas ni dans l'hypothèse (a), où $\langle\mu\rangle = C_R(u)$ est normal dans $N_G(R)$, ni dans l'hypothèse (b), comme on le voit clairement dans $N_G(E)$ (assertion (5)).

(7) Soit X un sous-groupe non trivial de C. Le normalisateur de X dans G admet un 2-complément normal, Q comme 2-groupe de Sylow, et est d'ordre premier à (q - e)/4.

Les groupes C et E sont d'ordres premiers entre eux. L'assertion (3) montre que Q, qui normalise X, est un 2-groupe de Sylow de $N_G(X)$. Il est clair que t, qui centralise X, et s, qui l'inverse, ne sont pas conjuguées dans $N_G(X)$. On a donc

$$N_G(Q) \cap N_G(X) \subset C_G(Q),$$

et $N_G(X)$ admet donc un 2-complément normal (théorème de Burnside).

Soit K ce complément. On a

$$C_K(t) = C, \quad \text{d'où} \quad C_K(Q) = \{1\}.$$

Selon 1.1, $K = C.C_K(s).C_K(st)$

et $C_K(s)$, $C_K(st)$ sont abéliens. Puisque st opère sans point fixe sur $XC_K(s)$, ce dernier groupe est abélien. De même $XC_K(st)$ est abélien, et en conséquence K centralise X.

Supposons par contradiction que $N_G(X)$ admette, pour un premier r impair divisant $(q - e)$, un r-groupe de Sylow R non trivial. On peut supposer que Q normalise R; alors t opère sans point fixe sur R, et on a

$$R = C_R(s) \times C_R(ts) \quad .$$

Supposons par exemple $R_o = C_R(s)$ non trivial. Alors R_o est conjugué dans G d'un sous-groupe de $C_G(t)$, donc conjugué dans G d'un sous-groupe de E, et $N_G(R_o)$ est isomorphe à $N_G(E)$, et XR est conjugué d'un sous-groupe de $N_G(E)$. On voit (assertion (5)) que X est d'ordre 3 ou 5 et que R est cyclique, donc égal à R_o. En outre on a

$$N_K(R) = X.E_o = C_G(X) \cap N_G(R),$$ où E_o est conjugué d'un sous-groupe de E.

De même pour tout sous-groupe non trivial V de E_o, comme $N_G(E_o) = N_G(V) = N_G(R)$ on aura

$$N_K(V) = X.E_o \quad .$$

On en déduit, comme X est d'ordre premier à l'ordre de E_o, que $X.E_o/X$ est un complément de Frobenius dans K/X. Soit L/X le noyau de K/X.

Il est clair, $C_K(s)$ étant abélien, que

$$E_o = C_K(s), \text{ d'où } L = C \times C_K(ts) \quad .$$

Si $E_o.Q$ normalise un sous-groupe A de C ou de $C_K(ts)$, alors AE_o est abélien (car une involution y opère sans point fixe), et donc A est contenu dans X. Ainsi aucun sous-groupe caractéristique de L contenant strictement X n'est cyclique. C'est donc que L est isomorphe à $(C/X) \times (C/X)$, d'où

$$|L/X| = ((q + e)/2|X|)^2$$

On a $(q + e)^2/4|X|^2 \equiv 1 \pmod r$

mais aussi $q \equiv e \pmod r$.

On voit facilement que ces congruences sont incompatibles pour $|X| \in \{3,5\}$.

(8) Si μ ne centralise pas E, il existe un caractère irréductible de G, de 2-groupe de défaut Q et degré m tel que

$$G = mq^3(q - e)$$

Les propositions 1.17 et 1.18 montrent que l'ensemble des blocs de groupe défaut Q de G est en bijection avec l'ensemble des orbites selon $N_G(Q)$ opérant sur l'ensemble des caractères de défaut nul de $C_G(Q)/Q$. Puisque $C_G(Q)/Q$ est isomorphe au groupe diédral $E\langle u\rangle$, ses caractères de défaut nul sont les caractères irréductibles de degré 2.

Si μ ne centralise pas E, il existe 3 caractères de défaut nul de $C_G(Q)/Q$ qui sont permutés par μ; chacun d'eux définit un bloc e_j ($j = 1, 2, 3$) de $C_G(Q)$ et il existe un unique bloc e de $N_G(Q)$, de groupe défaut Q, tel que

$$Br_{C(Q)}^{N(Q)}(e') = e \quad \text{si et seulement si} \quad e' \in \{e_1, e_2, e_3\} .$$

Soient $b_j = Br_{C_G(Q)}^{C_G(t)}(e_j)$ les blocs de groupe défaut Q de $C_G(t)$ obtenus par 1.18.

Soit $B = Br_{N_G(Q)}^{G}(e)$.

De la proposition 1.16 il résulte que pour tout bloc e' de $C_G(Q)$, on a

$$Br_{N_G(Q)}^{G}(Br_{C_G(Q)}^{N_G(Q)}(e')) = Br_{C_G(t)}^{G}(Br_{C_G(Q)}^{C_G(t)}(e')) .$$

On en déduit que, si b est un bloc de $C_G(t)$, on a

$$Br_{C_G(t)}^{G}(b) = B \quad \text{si et seulement si} \quad b \in \{b_1, b_2, b_3\}$$

Chacun des blocs b_j est de la forme b_{σ_j} (notations de l'appendice). Soit $\sigma \in \{\sigma_1, \sigma_2, \sigma_3\}$ et posons

$$\psi_\sigma = \mathrm{Ind}_{C_G(t)}^{G}(\tilde{\psi}_\sigma) .$$

On sait (proposition 1.22) que ψ_σ se décompose uniquement sur des caractères irréductibles du bloc B, la 2-section de t dans $C_G(t)$ étant à intersections triviales dans G. En outre ψ_σ est de carré 4 et nulle en 1, donc ψ_σ se décompose sur 4 caractères distincts, éléments de B.Irr(G).Ceci démontre que B.Irr(G) est de cardinal au moins 4; selon 1.14, B.Irr(G) est de cardinal 4.

La matrice de décomposition généralisée $D_B^{t,G} = A$ satisfait donc aux conditions suivantes (propositions 1.20, 1.21 et 1.24), où $B.Irr(G) = \{\xi_j\}_{1 \leqslant j \leqslant 4}$,

(1) A est une matrice (3,4) à coefficients dans $\mathbb{Z}$

(2) $A.{}^{T}A = 4Id_3$

(3) $A(\xi_j(1)) = 0$

Ces conditions déterminent A au signe près (et à une permutation des ξ_j près)

On obtient

$$A = \delta \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad \text{où} \quad \delta \in \{1,-1\} .$$

Il en résulte, d'après la troisième condition, que les éléments de B.Irr(G) ont même degré, soit $m = \xi_j(1)$.

Les valeurs des ξ_j sur la 2-section de t sont donc connues au signe près. Comme

$$d^{t,G}(\psi_{\sigma_i}) = d^{t,C_G(t)}(\tilde{\psi}_{\sigma_i}) = 4\phi_{\sigma_i} \qquad (i = 1, 2, 3)$$

les lignes de A fournissent la décomposition des ψ_{σ_j} sur B.Irr(G).

On obtient, à δ près,

$$\xi_1(t) = 3(q + e),\ \xi_2(t) = \xi_3(t) = \xi_4(t) = -(q + e) ,$$

d'où

$$A(B,\phi_\sigma) = \frac{8|G|(q + e)^2}{\delta m q^2 (q^2 - 1)^2} .$$

La proposition 1.23 fournit l'égalité de l'assertion à démontrer.

De cette assertion nous utiliserons seulement, pour démontrer que p est égal à 3, le fait que q^3 divise l'ordre de G.

(9) La caractéristique p est égale à 3.

Supposons par contradiction que p soit différent de 3.

Puisque 3 divise $q(q^2 - 1)$ et ne divise pas $q(q - e)$ (assertion (6)) 3 divise $(q + e)$. L'élément d'ordre 3 noté μ dans l'assertion (4) centralise l'involution u; il est donc conjugué d'un élément de C. Il résulte de l'assertion (7) que μ opère sans point fixe sur E. Donc μ opère sans

point fixe sur QE. D'où

$$q - e \equiv 1 \pmod 3 .$$

Puisque 3 divise (q + e), e est égal à 1. On peut donc supposer, en remplaçant éventuellement P par un conjugué dans F, que le groupe D, qui est d'ordre (q - 1)/2, normalise P. Rappelons que P.D est un groupe de Frobenius de noyau P. Selon l'assertion (3) Q est un 2-groupe de Sylow de $N_G(P)$, $\langle t \rangle$ étant un 2-groupe de Sylow de $C_G(P)$. Donc $N_G(P)$ admet un 2-complément normal, que nous noterons M. On a

$$M = C_M(t)C_M(s)C_M(st)$$

et $$C_M(t) = PE$$

d'où $$C_M(Q) = E .$$

On voit dans $C_G(s)$ et $C_G(ts)$ que

$$C_M(s) = P_s E \qquad \text{et } C_M(ts) = P_{ts} E$$

où P_s et P_{ts} sont normalisés par QE, et des p-groupes.
Puisque QE opère irréductiblement sur tout p-Sylow de $C_G(s)$ qu'il normalise P_s et P_{ts} sont d'ordres 1 ou q.

(a) Supposons que $C_M(ts) = E$.

Puisque P n'est pas groupe de Sylow de G (assertion (8)), P_s est d'ordre q. Il est clair que $N_G(PP_s)$ contient $N_G(P)$ et admet un 2-complément normal. En outre PP_s n'est pas p-groupe de Sylow de G. On en déduit facilement (toujours en utilisant 1.1) que

$$N_G(PP_s) = (P_o.E).Q \quad \text{où} \quad P_o = PP_sP' \quad (P' \text{ Sylow de } C_G(ts)).$$

Soit Z le centre de P . On a

$$Z \subset C_G(P), \text{ d'où} \quad Z \subset PP_s.$$

Sous l'opération de Q, on obtient par 1.1

$$Z = C_Z(t) \times C_Z(s) .$$

Mais QE normalise Z; on a donc $C_Z(t) = \{1\}$ ou $C_Z(t) = P$. Or P n'est pas central dans P_o; donc $C_Z(t) = \{1\}$ et par conséquent $Z = P_s$.

Mais si P_s est centralisé par P_o, P, qui est conjugué de P_s, est également centralisé par un groupe d'ordre q^3, ce qui contredit l'hypothèse (a).

(b) On a donc

$M = P_o.E$, où P_o est d'ordre q^3 et unique p-sous-groupe de Sylow de $N_G(P)$.

Puisque t opère sans point fixe sur P_o/P, ce dernier groupe est abélien, et PP_s est normal dans $N_G(P)$. Mais $N_G(PP_s)$ contient Q, donc admet un 2-complément normal, et, M étant clairement maximal parmi les groupes d'ordre impair que Q normalise (par 1.1), on a

$$N_G(PP_s) = N_G(P) \quad \text{et} \quad N_G(PP_{ts}) = N_G(P) .$$

De la même façon, P_s étant conjugué de P dans G et normalisé par Q, on a $N_G(P_s C_R(t)) = N_G(P_s)$ où R est p-groupe de Sylow de $N_G(P_s)$

En outre, ts opérant sans point fixe sur PP_s, PP_s est abélien, donc R contient P, et finalement $C_R(t) = P$. On en conclut que

$$N_G(P) = N_G(P_s) = N_G(P_{ts}),$$

et que P_o est abélien élémentaire.

Il est exclus que $N_G(P_o)$ soit égal à $N_G(P)$, car, P_o étant alors p-groupe de Sylow de G, P et P_s sont conjugués dans $N_G(P_o) = N_G(P)$ (cf 1.3) ce qui n'est pas. Mais puisque Q normalise P_o, et M est maximal comme sous-groupe d'ordre impair normalisé par Q, $N_G(P_o)$ n'a pas de 2-complément normal. Les involutions de $N_G(P_o)$ sont toutes conjuguées dans $N_G(P_o)$. On voit dans $N_G(Q)$ (assertion (4)) que $N_G(P_o)$ contient un élément d'ordre 3 qui normalise Q sans le centraliser, et est conjugué dans G d'un élément de C. Notons -le x. D'après l'assertion (7), $C_G(x)$ admet un 2-complément normal et $N_G(\langle x\rangle)$ un 2-Sylow d'ordre 4. Dans son opération sur P_o, x permute P, P_s et P_{ts}, donc $C_{P_o}(x)$ n'est pas trivial. Par conséquent un 2-groupe de Sylow de $N_G(\langle x\rangle)$ opère sur un p-groupe de Sylow non trivial de $C_G(x)$. Selon 1.1, il existe dans $C_G(x)$ un élément d'ordre p centralisé par une involution de $N_G(\langle x\rangle)$.

Notons y'cet élément: y'est d'ordre p et centralise une involution, donc y' est conjugué d'un élément de P. Or si Y est un sous-groupe non trivial de P, $N_G(Y)$ contient $P \circ Q$ et admet Q comme 2-groupe de Sylow (assertion (3)). Puisque t centralise Y et s l'inverse, $N_G(Y)$ admet un 2-complément normal. De 1.1 il résulte que l'ordre de $N_G(Y)$ divise $q^3(q - 1)$, donc est premier à 3. Cependant x, d'ordre 3, centralise y! Cette contradiction achève la démonstration de l'assertion (9).

(10) On a $e = -1$; si E_1 est un sous-groupe non trivial de E, $N_G(E_1) = N_G(Q)$.

Les 2-Sylow de $PSL_2(q)$ sont abéliens, donc q est une puissance impaire de 3. On en déduit $e = -1$. Comme 5 ne divise pas l'ordre de $C_G(t)$, le second cas de l'assertion (5) est exclus.

3. Les 2-blocs de défaut non nul de G.

On détermine la structure r-locale de G pour les premiers impairs r qui divisent $(q^2 - 1)$ (assertions (2) et (3) de ce chapitre : la r-fusion dans G est contrôlée par $N_G(Q)$ ou par $N_G(C) = C.Q$. Les isométries correspondantes jointes à la connaissance de $C_G(t)$ (i.e. de la structure 2-locale) permettent de calculer les matrices de décomposition généralisées relatives à t pour les 2-blocs de G. Les propositions 1.23, 1.24 et 1.25 permettent de lever les ambigüités et de calculer l'ordre de G, ainsi que les degrés des caractères irréductibles de 2-défaut non nul.

(1) Si x est un élément d'ordre 3 de G qui centralise une involution, x n'est pas réel. Le 2-groupe Q ne normalise aucun 3-groupe différent de $\{1\}$. Si X est un sous-groupe de C différent de $\{1\}$, $N_G(X)$ est un 3'-groupe.

Supposons x élément de P. Les 2-groupes de Sylow de $C_G^*(x)$ étant abéliens, $C_G(t)$ contient un 2-groupe de Sylow de $C_G^*(x)$. La première assertion se lit donc dans $C_G(t)$. La seconde se déduit de la première par 1.1. La troisième se déduit de la seconde, sachant que $N_G(X)$ contient Q et admet un 2-complément normal (assertion (7) du paragraphe 2).

(2) μ opère sans point fixe sur E; $N_G(Q)/Q$ est un groupe de Frobenius.

Rappelons que μ est introduit dans l'assertion (4) du paragraphe 2.

Posons $T = \langle \mu \rangle$ et $E_o = C_E(T)$.

Supposons par contradiction que $E_o \neq \{1\}$.

Puisque T est conjugué d'un sous-groupe de P, $C_G(T)$ admet $\langle u \rangle$ pour 2-groupe de Sylow et un 2-complément normal K. En outre $P_o = K \cap C_G(u)$ est isomorphe à P. Si E_1 est un sous-groupe de E_o autre que $\{1\}$, on a (assertions (4), (5) et (10) du paragraphe 2)

$$N_K(E_1) = (ES)T \cap K = E_o T .$$

Puisque T et E_1 sont d'ordres premiers entre eux on a aussi

$$N_{K/T}(E_1T/T) = E_oT/T .$$

Donc K/T est un groupe de Frobenius de complément E_oT/T ; soit R son 3-groupe de Sylow. Sur R opère le groupe diédral $E_o\langle u\rangle$. Selon la proposition 1.2 on a, si r divise $|E_o|$,

$$|R| = |C_R(u)|^2 = |P_o/T|^2 = q^2/9 ;$$

d'où $q^2 \equiv 9 \pmod r$.

Or $q^2 \equiv 1 \pmod r$ puisque r divise (q + 1).

Donc r divise 8, ce qui est absurde.

(3) Pour tout sous-groupe non trivial X de C on a $N_G(X) = N_G(C) = C.Q$.

(a) Si r est un diviseur premier impair de (q - 1) ou si r = 5, $PSL_2(r)$ n'est pas sous-quotient de G.

Soient N et L deux sous-groupes de G, N normal dans L, tels que L/N soit isomorphe à $PSL_2(r)$, où r divise $5(q - 1)/2$. Pour un tel r, $PSL_2(r)$ n'est pas sous-quotientde $PSL_2(q)$, donc N est d'ordre impair.

Si r divise (q - 1), le théorème des résidus quadratiques montre que $(\frac{r}{3}) = (-1)^{(r-1)/2}$. On en déduit que 12 divise (r-1) ou (r+1). Donc $PSL_2(r)$ admet un sous-groupe diédral d'ordre 12. Le théorème de Frattini, appliqué à un 3-groupe de Sylow de N, montre que L contient un $\{2,3\}$-groupe dont un quotient est diédral d'ordre 12, ce qui contredit l'assertion (1).

Si r = 5, l'assertion (10) du paragraphe 2 montre que N est d'ordre premier à (q + 1). Si Q_o est un 2-groupe de Sylow de L, on a $C_L(Q_o) = Q_o$ et $N_L(Q_o)$ est isomorphe à A_4. On sait qu'un élément d'ordre 3 de $N_G(Q_o)$ commute à une involution de G (assertion (4) du paragraphe 1) et qu'un élément d'ordre 3 de A_5 est réel. L'assertion (1) est donc contredite.

(b) C est un sous-groupe de Hall de G.

Soit r un diviseur premier de (q - 1)/2 et soit X un r-groupe de Sylow de C. Le normalisateur de X dans G contient C.Q. Considérons donc un r-sous-

groupe R de G, normalisé par Q, et différent de $\{1\}$. Soit $N = N_G(R)$.

On va démontrer que $N/\mathbf{O}_{2',}(N)$ est d'ordre 4 ou 12.

Il existe une involution t' appartenant à Q telle que $C_R(t') \neq \{1\}$ (proposition 1.1). On a

$$C_N(t') \subset C_G(t') \cap N_G(C_R(t'))$$

donc $C_N(t')$ est isomorphe à un sous-groupe de C.Q. On en déduit $C_N(Q) = Q$. Or Q est un groupe de Sylow de N (assertion (3) du paragraphe 2).

Si les involutions de N ne sont pas toutes conjuguées dans N, N admet un 2-complément normal et on a

$$N = \mathbf{O}_{2',}(N).Q$$

Si N admet une seule classe d'involutions, la proposition 1.7 permet d'affirmer que $N/\mathbf{O}_{2',}(N)$ est isomorphe à un groupe unimodulaire $PSL_2(q')$. D'après (a) la caractéristique de ce groupe est différente de r et de 5. Il possède un groupe de Frobenius d'ordre $q'(q' - 1)/2$, lequel opère fidèlement sur R, et sur l'espace de Frattini de R. Selon la proposition 1.1, et puisque Q opère fidèlement sur R, R est engendré par 3 groupes cycliques; son espace de Frattini est de dimension au plus 3. On a donc

$(q' - 1)/2 \leqslant 3$, d'où $q' = 3$ (car q' est congru à 3 ou 5 mod 8).

Ainsi

$N/\mathbf{O}_{2',}(N)$ est isomorphe à A_4.

On en conclut que dans tous les cas Q normalise un r-groupe de Sylow de N.

Supposons maintenant que R soit maximal parmi les r-sous-groupes de G contenant X et que Q normalise: R est r-Sylow de son normalisateur, donc R est r-groupe de Sylow de G.

Pour démontrer l'assertion (b) supposons par contradiction que R soit différent de X. On a

$$R = X.C_R(s).C_R(ts) \quad \text{et} \quad R \text{ n'est pas cyclique.}$$

Supposons que le centre de R ne soit pas cyclique. Il existe alors un élément d'ordre r de Z(R) qui est centralisé par s ou par ts, donc conjugué d'un élément de X. Cette conjugaison se fait dans N (proposition 1.3), donc

N admet une seule classe d'involutions et $\Omega_1(Z(R))$ est d'ordre r^3. Sur ce dernier groupe opère un groupe T, d'ordre 3, et qui normalise Q. Il est clair que $Z = C_G(T) \cap \Omega_1(Z(R))$ est d'ordre r. Puisque $C_N(Z)$ contient T, $C_N(Z)$ et $N_N(Z)$ ont même image dans $N/\Phi_{2'}(N) \simeq A_4$, autrement dit $N_N(Z)/C_N(Z)$ est d'ordre impair. Il en résulte qu'un générateur de Z n'est pas réel (proposition 1.3). Un r-groupe de Sylow V de $C_G(T)$ contient donc des éléments non réels. Selon l'assertion (4) du paragraphe 2 et l'assertion (1) du paragraphe 3, $C_G(T)$ a un 2-groupe de Sylow d'ordre 2. Donc V est normalisé par une involution t' et $W = C_V(t') \neq \{1\}$. Finalement $C_G(W)$ contient t' et T, ce qui contredit l'assertion (1).

Le centre de R est donc cyclique. Cependant, R n'étant pas cyclique, R contient un sous-groupe normal et non cyclique, d'ordre r^2 et normalisé par Q. Soit $X = A \cap Z(R)$. Sous l'action de Q, A décompose en

$$A = X \times B$$

où X et B sont chacun centralisé par une involution, donc conjugués dans G. Soit $V = C_R(B) = C_R(A)$. Le groupe V est d'indice r dans R et normal dans R.Q. Donc $W = \Omega_1(Z(V))$ est également normal dans R.Q, abélien élémentaire d'ordre au plus r^3. Puisque B est conjugué de X, $C_G(B)$ contient un r-groupe de Sylow R' de G contenant V. Les groupes R et R' normalisent W, mais opèrent différemment (l'un centralise B, l'autre non). Le résultat démontré pour $N = N_G(R)$ précédemment s'applique à $N_G(W)$: R et R' engendrent un sous-groupe d'ordre impair de $N_G(W)$. La proposition 1.8 est contredite, ce qui démontre (b).

(c) Démonstration de (3).

Le groupe C est sous-groupe de Hall de $N_G(X)$, et on a (assertion (7) de 1)

$$N_G(X) = \Phi_{2'}(N_G(X)).Q$$

La proposition 1.1 implique que tout diviseur premier de $|N_G(X)|$ divise $q(q^2 - 1)$. Les diviseurs de $(q + 1)/4$ sont exclus par l'assertion (7), et 3 est exclus par l'assertion (1) de ce paragraphe. Donc d'après (b) on a

$$\Phi_{2'}(N_G(X)) = C$$

ce qui démontre (3).

(4) Les 2-blocs de défaut 1; valeurs des caractères sur (C - {1}).

Soient, avec les notations de l'appendice, ρ une racine d'ordre $(q-1)/2$ de l'unité et b_ρ le bloc de groupe défaut $\langle t\rangle$ de $C_G(t)$ correspondant ($\rho \neq 1$). Par la proposition 1.18 il lui est associé un bloc B_ρ de G, de groupe défaut $\langle t\rangle$. Selon la proposition 1.22, avec $H = C_G(t)$ et $\mathcal{D}$ la 2-section de t dans $C_G(t)$, $\mathrm{Ind}_{C_G(t)}^G(\tilde{\psi}_\rho)$, qui est de carré 2, se décompose sur $B_\rho.\mathrm{Irr}(G)$. D'où

$$\mathrm{Ind}_{C_G(t)}^G(\tilde{\psi}_\rho) = \chi_\rho - \chi'_\rho \quad \text{et} \quad B_\rho.\mathrm{Irr}(G) = \{\chi_\rho, \chi'_\rho\} \text{ (cf 1.14).}$$

En outre

$$d^{t,G}(\chi_\rho - \chi'_\rho) = d^{t,C(t)}(\tilde{\psi}_\rho) = 2\phi_\rho$$

donc
$$\delta^{\phi_\rho}_{\chi_\rho} = 1 \quad \text{et} \quad \delta^{\phi_\rho}_{\chi'_\rho} = -1 .$$

Posons $N = N_G(C)$ et $\mathcal{D} = C\langle t\rangle - \langle t\rangle$. Il résulte de l'assertion (3) que les hypothèses de 1.26 sont satisfaites par G, N et $\mathcal{D}$ et satisfaites aussi par $C_G(t)$, N et $\mathcal{D}$. Pour classifier les irréductibles de N, considérons N comme un produit direct du groupe diédral $C\langle s\rangle$ par $\langle t\rangle$. La même racine de l'unité ρ définit une représentation de degré 1 de C (qui envoie le générateur y de C sur ρ), donc par induction un caractère irréductible de degré 2 de $C\langle s\rangle$ d'où finalement un caractère irréductible λ_ρ de N, caractère dont le noyau contient $\langle t\rangle$. Désignons, pour toute involution t' de Q, par $\varepsilon_{t'}$ le caractère irréductible de degré 1 de N dont le noyau est $C\langle t'\rangle$. Les éléments de Irr(N) sont

$$1_N\ ,\ \varepsilon_t\ ,\ \varepsilon_s\ ,\ \varepsilon_{st}\ ,\ \lambda_\rho\ ,\ \lambda'_\rho = \varepsilon_s\lambda_\rho \quad (\text{où } \lambda_\rho = \lambda_\nu \text{ si et seulement si } \rho \in \{\nu, \nu^{-1}\})$$

Le $\mathbb{Z}$-module $R(N|\mathcal{D})$ est engendré par

$$\lambda_{\rho_1} - \lambda_{\rho_2}$$

$$\lambda'_{\rho_1} - \lambda'_{\rho_2}$$

$$\lambda_\rho - \varepsilon_t - 1_N$$

$$\lambda'_\rho - \varepsilon_{st} - \varepsilon_s \ .$$

Comme $(q-3)/4 \geqslant 6$, et du fait que

$$(\mathrm{Ind}_N^G(\lambda_\rho - \varepsilon_t - 1_N) \ , \ 1_G) = -1,$$

on voit facilement que Ind_N^G se prolonge isométriquement depuis $R(N|\mathcal{D})$ jusqu'à tout $R(N)$; plus précisément il existe des éléments distincts ζ_j $(1 \leqslant j \leqslant 4)$, $\zeta_\rho$et ζ'_ρ de Irr(G) et des entiers η , η', η_2, $\eta_3 \in \{1,-1\}$ tels que $\zeta_1 = 1_G$ et

$$((1)) \quad \begin{cases} \mathrm{Ind}_{N_G(C)}^G(\lambda_{\rho_1} - \lambda_{\rho_2}) = \eta(\zeta_{\rho_1} - \zeta_{\rho_2}) \\ \mathrm{Ind}_{N_G(C)}^G(\lambda'_{\rho_1} - \lambda'_{\rho_2}) = \eta'(\zeta'_{\rho_1} - \zeta'_{\rho_2}) \\ \mathrm{Ind}_{N_G(C)}^G(\lambda_\rho - \varepsilon_t - 1_{N_G(C)}) = \eta\zeta_\rho - \eta\zeta_4 - \zeta_1 \\ \mathrm{Ind}_{N_G(C)}^G(\lambda'_\rho - \varepsilon_{st} - \varepsilon_s) = \eta'\zeta'_\rho - \eta_2\zeta_2 - \eta_3\zeta_3 \ . \end{cases} \qquad ((1))$$

(on a tenu compte de la nullité en 1)

D'autre part, on a, pour tout $x \in \mathcal{D}$,

$$(\chi_\rho - \chi'_\rho)(x) = (\theta_\rho - \theta'_\rho)(x) = (\lambda_\rho - \lambda'_\rho)(x),$$

d'où

$$(\chi_\rho - \chi'_\rho \ , \ \eta(\zeta_{\rho_1} - \zeta_{\rho_2})) = (\mathrm{Res}_N^G(\chi_\rho - \chi'_\rho) \ , \ \lambda_{\rho_1} - \lambda_{\rho_2})$$

$$= (\lambda_\rho - \lambda'_\rho \ , \ \lambda_{\rho_1} - \lambda_{\rho_2})$$

De même

$$(\chi_\rho - \chi'_\rho \ , \ \eta'(\zeta'_{\rho_1} - \zeta'_{\rho_2})) = (\lambda_\rho - \lambda'_\rho \ , \ \lambda'_{\rho_1} - \lambda'_{\rho_2})$$

On en déduit que

$$\{\chi,\chi'_\rho\} = \{\zeta_\rho,\zeta'_\rho\} \quad \text{et} \quad \eta = \eta' \ ,$$

soit

$$\chi_\rho - \chi'_\rho = \eta(\zeta_\rho - \zeta'_\rho) \quad \text{et} \quad \eta = \delta_{\zeta_\rho}^{\Phi_\rho}$$

Les caractères irréductibles de G qui n'interviennent pas dans $\mathrm{Ind}_N^G(R(N|\mathcal{D})$ étant nuls sur $\mathcal{D}$, la proposition 1.26 nous permet d'affirmer

$$((2)) \quad \begin{cases} \text{pour tout } x \in (C\langle t\rangle - \langle t\rangle), \text{ on a} \\ \zeta_\rho(x) = \eta\lambda_\rho(x) \ ; \ \zeta'_\rho(x) = \eta\lambda'_\rho(x) \ ; \ \zeta_2(x) = \eta_2\varepsilon_s(x) \ ; \ \zeta_3(x) = \eta_3\varepsilon_s(x) \\ \zeta_1(x) = 1, \ \zeta_4(x) = \eta\varepsilon_t(x) \ \text{ et } \ \xi(x) = 0 \text{ pour tout autre élément de Irr(G).} \\ \text{On verra que } \eta = \eta_2 = \eta_3 = 1. \end{cases} \qquad ((2))$$

(5) Le bloc principal de G.

Il existe dans G un seul bloc de défaut 3, qui est le bloc principal (proposition 1.15). Il correspond au bloc principal de $C_G(t)$ (proposition 1.19). La matrice de décomposition généralisée du bloc principal de G relativement à t, sur les bases $B_o(G).Irr(G)$ et $\{\phi_1, \phi_2, \phi_3\}$ (cf appendice) sera notée D_o. D'après les résultats généraux du chapitre 1, elle satisfait aux conditions suivantes:

(1) D_o est une matrice à 3 lignes à coefficients dans $\mathbb{Z}$;

(2) la première colonne est (1,0,0) (caractère 1_G);

(3) On a
$$D_o \cdot {}^t D_o = C_{b_o} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 2 \\ 2 & 2 & 4 \end{pmatrix}$$

(4) On a $D_o(\xi(1)) = 0$ $(\xi \in B_o(G).Irr(G))$

Ces conditions définissent deux classes de matrices. A permutation des caractères près, dans chaque classe, les coefficients sont connus au signe près: il existe en effet $\delta_j \in \{1,-1\}$ $(1 \leqslant j \leqslant 8)$ tels que

((3))
$$D_o = \begin{pmatrix} 1 & \delta_2 & \delta_3 & \delta_4 & 0 & 0 & 0 \\ 0 & \delta_2 & 0 & \delta_4 & \delta_5 & 0 & \delta_7 \\ 0 & 0 & \delta_3 & \delta_4 & 0 & \delta_6 & \delta_7 \end{pmatrix} \qquad ((3))$$

ou bien

((4))
$$D_o = \begin{pmatrix} 1 & \delta_2 & \delta_3 & \delta_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & \delta_5 & \delta_6 & 0 & 0 \\ 0 & 0 & \delta_3 & \delta_4 & 0 & 0 & \delta_7 & \delta_8 \end{pmatrix} \qquad ((4))$$

Les quatre premiers caractères de $B_o(G)$ sont non nuls en ty; ils coïncident donc avec les caractères ζ_j rencontrés au paragraphe (4). Posons

$$d = \zeta_\rho(1) .$$

Des formules ((1)) et ((2)) on déduit facilement

((5))
$$d = \zeta_4(1) + \eta. \qquad ((5))$$

et
$$\zeta_4(ty) = \eta \text{ , d'où}$$

((6))
$$\delta^{\phi_1}_{\zeta_4} = \eta \qquad ((6))$$

On a de même

((7)) $$\eta d = \eta_2\zeta_2(1) + \eta_3\zeta_3(1) \qquad ((7))$$

et $\zeta_2(ty) = -\eta_2$ et $\zeta_3(ty) = -\eta_3$, d'où

((8)) $$\delta_{\zeta_2}^{\phi_1} = -\eta_2 \quad \text{et} \quad \delta_{\zeta_3}^{\phi_1} = -\eta_3 \qquad ((8)).$$

En considérant les valeurs en $\mathbf{y}$, on obtient par ((1)) et ((2))

((9)) $$\zeta_2(\mathbf{y}) = \eta_2 \ , \quad \zeta_3(\mathbf{y}) = \eta_3 \quad \text{et} \quad \zeta_4(\mathbf{y}) = \eta \ . \qquad ((9))$$

(a) Supposons que D_o soit donnée par ((3)), $B_o(G)$ contenant 7 irréductibles.

Les deuxième et troisième irréductibles de $B_o(G)$ sont conjugués, non réels; les caractères induits considérés en ((1)) sont tous à valeurs réelles. Il s'agit donc de ζ_2 et ζ_3. Le quatrième est ζ_4, qui est à valeurs réelles. On a

$$\zeta_4(t) = \delta_4(\phi_1(1) + \phi_2(1) + \phi_3(1)) = \delta_4 q \ , \text{ entier impair.}$$

L'indice de Schur-Frobenius de ζ_4 est par conséquent égal à 1, celui de ζ_2 est nul comme celui de ζ_3. De la proposition 1.25 il résulte

$$1 + \delta_4 = 0$$

d'où, en tenant compte de ((5)) et ((6)),

$$\zeta_4(1) = d + 1 \ , \quad \text{et } d \text{ est pair.}$$

Puisque ζ_2 et ζ_3 sont conjugués algébriques, on a, par ((7)) et ((8))

$$\eta_2 = \eta_3 = \eta = -1$$

$$\delta_2 = \delta_3 = 1$$

$$d = 2\zeta_2(1) = 2\zeta_3(1) \ .$$

Il nous est donc possible de calculer $A(B_o(G),\phi_1)$ (notations de la proposition 1.23) en fonction de d. On obtient

$$\zeta_2(t) = \zeta_3(t) = (q+1)/2 \quad \text{et} \quad \zeta_4(t) = -q$$

d'où $$A(B_o(G),\phi_1) = \frac{|G|\,(d+q+1)^2}{q^2(q^2-1)^2 d(d+1)}$$

Mais de l'assertion (8) du paragraphe 2 et de l'assertion (2) du paragraphe 3 on déduit qu'il existe un entier n tel que $|G| = nq^3(q^2-1)$, et (1.23) implique donc

((10)) $$qn(d+q+1)^2 = (q^2-1)(q-1)d(d+1) \qquad ((10))$$

Cette dernière égalité montre que q divise d(d+1).

Si q divise (d+1), q divise (d+q+1), donc q^3 divise (d+1). Or

ω_{ζ_3}(classe de t) = $|G|\zeta_3(t)/q(q^2-1)\zeta_3(1) = nq^2(q+1)/d$

doit être un entier algébrique, donc d, qui est premier à q, divise n(q+1).

d'où $n(q+1) \geqslant d \geqslant q^3 - 1$

soit $n \geqslant q^2 - q + 1$.

On a aussi $qn < (q^2 - 1)(q - 1)$, d'après ((10)).

Ces deux inégalités conduisent à $2q < 1$, ce qui est impossible.

Supposons donc que q divise d; alors (d+1), qui est premier à q, divise n. En outre, ζ_4 étant constant sur $(C - \{1\})$, (q-1)/2 divise $\zeta_4(1) - \zeta_4(y) = d + 2$, donc (q-1) divise (d+2). Il existe donc un entier $n' \geqslant 1$ tel que

$$d = n'q(q - 1) - 2q .$$

Sachant que $d + 1 \leqslant n < (q^2 - 1)q - 1)/q$,

on voit que $n' = 1$, $n = d + 1$, $d = q^2 - 3q$, et finalement, dans ((10))

$$q(q + 1) = q(q - 3) \ldots$$

Par cette contradiction l'absurdité de (a) est démontrée et D_o est donnée par ((4)).

(b) Ordre de G et degrés des caractères du bloc principal.

Notons ξ_j (j = 1, 2, ..., 7, 8 et $\xi_1 = 1_G$) les éléments de $B_o(G).Irr(G)$ ordonnés selon les colonnes de D_o dans ((4)).

La proposition 1.24 (avec x = y) et ((2)) impliquent

$$\delta_3\xi_3(y) + \delta_4\xi_4(y) = 0 .$$

En comparant à ((6)), ((8)) et ((9)), on en déduit que $\zeta_4 \in \{\xi_3, \xi_4\}$ et on peut supposer que $\zeta_4 = \xi_4$, d'où, avec une numérotation convenable

((11)) $\zeta_j = \xi_j$ pour j = 1, 2, 3 et 4. ((11))

Posons $d'_j = \delta_j\xi_j(1)$.

La proposition 1.23 implique

$$A(B_o(G),\phi_1) = \frac{|G|}{q^2(q^2-1)^2}\left(1 + \frac{1}{d_2'} + \frac{q^2}{d_3'} + \frac{q^2}{d_4'}\right) = q - 1 \qquad ((12))$$

D'autre part, d'après l'assertion (3) de ce paragraphe, on a

$$q - 1 = \frac{|G|}{q^2(q^2-1)^2} \sum_{\zeta \in \mathrm{Irr}(G)} \frac{|\zeta(t)|^2 \zeta(\mathbf{y})}{\zeta(1)}$$

soit, par ((2)), ((6)), ((8)), ((9)) et ((11))

$$q - 1 = \frac{|G|}{q^2(q^2-1)^2}\left(-\frac{2(q+1)^2}{\eta d} + 1 + \frac{q^2}{d_4'} - \frac{1}{d_2'} - \frac{q^2}{d_3'}\right)$$

Par comparaison on en déduit

$$2(q+1)^2/\eta d + 2/d_2' + 2q^2/d_3' = 0 .$$

En tenant compte de ((7)) (i.E. $\eta d + d_2' + d_3' = 0$), on en déduit

$$d_3' = qd_2' \text{ , d'où } \delta_3 = \delta_2 \text{ et } \xi_3(1) = q\xi_2(1).$$

Par ((6)) et ((7)) on a

$$\eta = \delta_4 = -\delta_2 \quad \text{et} \quad \xi_4(1) = (q+1)\xi_2(1) - \delta_4$$

Les caractères ξ_2, ξ_3 et ξ_4 sont réels (car d'après ((1)) et ((11)) ξ_3 et ξ_4 ne sont pas conjugués l'un de l'autre). Ils sont de degrés impairs, car $\xi_2(t) = \delta_2 q$ est impair. Leurs indices de Schur-Frobenius sont égaux à 1. On a donc par 1.25,

$$1 + \delta_2 + \delta_3 + \delta_4 = 0.$$

d'où on déduit

$$\delta_2 = \delta_3 = -1 \quad \text{et} \quad \delta_4 = 1 \; ; \; \chi_\rho = \zeta_\rho \; ; \; \chi_\rho' = \zeta_\rho' \; . \qquad ((13))$$

Posons $d_j = \xi_j(1)$ $(j = 2, 3, \ldots, 8)$

Puisque ξ_2 est constant sur $(C - \{1\})$, $(q-1)/2$ divise (d_2-1). En tenant compte des précisions précédentes la formule ((12)) devient

$$|G|(d_2 - 1)^2 = q^2(q-1)^3(q+1)d_2d_4 \qquad ((14))$$

Puisque $(q-1)$ divise (d_2-1), d_4 est premier à (q^2-1); donc d_4 divise $|G|/(q^2-1) = nq^3$. Donc ((14)) s'écrit

$$\left(\frac{nq^3}{d_4}\right)(d_2 - 1)^2 = q^2(q-1)^2 d_2$$

Il existe donc un entier b tel que $d_2 - 1 = b(q-1)$ et b divise q. Mais on voit aussi dans ((14)) que, q^3 divisant $|G|$, q divise d_2d_4. Or d_2 et d_4

sont premiers entre eux. On bien q divise d_2, ou bien q divise d_4. Si q divise d_2, b est égal à 1. Les involutions de G étant conjuguées, 8 divise $\xi_2(1) - \xi_2(t) = d_2 - \delta_2 = b(q-1) + 2$, ce qui interdit b = 1. C'est donc que q divise $d_4 = (q+1)d_2 - 1 = b(q^2 - 1) + q$, ce qui impose b = q. En conclusion on a

((15)) $\xi_2(1) = q^2 - q + 1$, $\xi_3(1) = q(q^2 - q + 1)$

$\xi_4(1) = q^3$ $\zeta_\rho(1) = q^3 + 1$ ((15))

((16)) $|G| = q^3(q^3 + 1)(q - 1)$ ((16))

((17)) $m = (q - 1)(q^2 - q + 1)$ ((17))

Selon 1.24 (avec x = 1) on a

$$d'_3 + d'_4 + d'_5 + d'_6 = 0$$

soit $d'_5 + d'_6 = - q^2 + q$.

La proposition 1.23 permet de déterminer d'_5 et d'_6. On a en effet

$$\xi_5(t) = \delta_5(q-1)/2 \ , \ \xi_6(t) = \delta_6(q-1)/2$$

d'où

$$A(B_o(G), \phi_2) = - \frac{1}{q+1} + \frac{q(q-1)^2(q^2-q+1)}{4d'_5d'_6} = \frac{3q - 1}{q + 1}$$

soit $d'_5d'_6 = -q(q^2-q+1)(q-1)^2/12$

Supposons la numérotation telle que $\delta_5 = -1$ et $\delta_6 = 1$. On obtient, en posant $q = 3q_o^2$,

((18)) $d_5 = (q-1)(q_o(q+1) + q)/2$

$d_6 = (q-1)(q_o(q+1) - q)/2$ ((18))

Par conjugaison complexe, on peut supposer ξ_5 et ξ_7 conjugués et ξ_6, ξ_8 conjugués. D'où

((19)) $d_5 = d_7$; $\delta_5 = \delta_7 = -1$; $d_6 = d_8$; $\delta_6 = \delta_8 = 1$ ((19))

(6) Isométries depuis $N_G(E)$; valeurs des caractères sur $(E - \{1\})$.

La proposition 1.26 est utilisable avec $N = N_G(E)$ et $\mathcal{D} = EQ - Q$ (en conséquence des assertions (5) et (10) du paragraphe 2) et ces notations seront adoptées provisoirement.

(a) Les 2-blocs de défaut 2.

Les irréductibles de G de groupe défaut Q sont classifiés par l'assertion (2) de ce paragraphe et la description faite en (8) du paragraphe 2. On obtient ainsi (q-3)/24 blocs et (q-3)/6 caractères irréductibles de G, tous de même degré $m = (q-1)(q^2-q+1)$.

A toute racine de l'unité σ d'ordre (q+1)/4 de 1 ($\sigma \neq 1$) correspond un caractère λ_σ de degré 1 de E, qui envoie le générateur z^2 de E sur σ. Le groupe cyclique d'ordre 6 engendré par u et μ opère sur (E - {1}) comme, dualement, sur (Irr(E) - $\{1_E\}$), et par ce biais (z^2 étant fixé), opère aussi sur les racines (q+1)/4-ièmes de 1. A chaque orbite $\Sigma = \{\sigma, \sigma^{-1}, \sigma', \sigma'^{-1}, \sigma'', \sigma''^{-1}\}$ correspond un bloc B_Σ de groupe défaut Q. Le calcul de la matrice de décomposition généralisée $D_{B_\Sigma}^{t,G}$ fait en 2.(8) montre que les 4 éléments de B_Σ.Irr(G) peuvent être caractérisés comme suit

soit $\phi_\sigma \in b_\sigma.\mathrm{Irr}_p(C_G(t))$ (on a $\phi_\sigma = \phi_{\sigma^{-1}}$)

ξ_Σ est caractérisé par $\delta_{\xi_\Sigma}^{\phi_\sigma} = 1$ pour tout $\sigma \in \Sigma$;

ξ_σ est caractérisé par $\delta_{\xi_\sigma}^{\phi_\tau} = 1$ si et seulement si $\sigma \in \{\tau, \tau^{-1}\}$;

On pose $\psi_\sigma = \mathrm{Ind}_{C_G(t)}^{G}(\tilde{\psi}_\sigma)$

et on a $\psi_\sigma = \xi_\Sigma + \xi_\sigma - \xi_{\sigma'} - \xi_{\sigma''}$.

(b) Isométrie depuis $N_G(E)$.

Les caractères irréductibles de N sont les suivants

$\gamma_\Sigma = \mathrm{Ind}_{EQ}^{N}(\lambda_\sigma \otimes 1_Q)$ où $\sigma \in \Sigma$

$\gamma_\sigma = \mathrm{Ind}_{EQ}^{N}(\lambda_\sigma \otimes \varepsilon_t)$

6 caractères de degré 1, dont le noyau contient EQ; on note ε l'élément de Irr(N) tel que $\varepsilon(1) = 1$ et $\varepsilon(u) = -1$.

$\nu = \mathrm{Ind}_{ES}^{N}(1_{E<u>} \otimes \varepsilon_t)$

$\nu' = \varepsilon\nu$

Le $\mathbb{Z}$-module $R(N|\mathcal{D})$ est engendré par les éléments de la forme

$\gamma_{\sigma_1} - \gamma_{\sigma_2}$; $\gamma_\sigma - \nu - \nu'$

$\gamma_{\Sigma_1} - \gamma_{\Sigma_2}$; $\gamma_\Sigma - \mathrm{Ind}_{EQ}^{N}(1_{EQ})$

Pour tout $\theta \in R(N|\mathcal{D})$ et tout $\psi \in R(G)$, on a $(\mathrm{Ind}_N^G(\theta),\psi) = (\theta,\mathrm{Res}_N^G(\psi))$ et ce produit scalaire ne dépend donc que des valeurs de ψ sur $\mathcal{D}$; si en outre ψ est nul sur les éléments 2-réguliers, ce produit ne dépend que des valeurs de ψ sur $t(E - \{1\})$. Posons donc (notations de l'appendice)

$$\psi_i = \mathrm{Ind}_{C_G(t)}^G(\tilde{\psi}_i) \quad (i = 1, 2, 3).$$

Le caractère ψ_i est décomposé dans $B_o(G)$ selon la i-ème ligne de D_o, comme on le constate en calculant $d^{t,G}(\psi_i) = d(\tilde{\psi}_i)$. On a donc, d'après (5)

$$\psi_1 = \xi_1 - \xi_2 - \xi_3 + \xi_4$$

$$\psi_2 = -\xi_3 + \xi_4 - \xi_5 + \xi_6$$

$$\psi_3 = -\xi_3 + \xi_4 - \xi_7 + \xi_8$$

et $\psi_1(x) = 0$ pour tout $x \in \mathcal{D}$

$\psi_2(x) = \psi_3(x) = -4 = (\nu - 31_N)(x)$ pour tout $x \in \mathcal{D}$

Enfin on a aussi

$$\psi_\sigma(x) = (\gamma_{\sigma'} + \gamma_{\sigma''} - \gamma_\sigma - \gamma_\Sigma)(x) \quad \text{pour tout } x \in \mathcal{D} \ .$$

En utilisant les égalités précédentes et la conservation du produit scalaire, on obtient facilement

((20)) $$\mathrm{Ind}_N^G(\gamma_{\sigma_1} - \gamma_{\sigma_2}) = \xi_{\sigma_2} - \xi_{\sigma_1} \qquad ((20))$$

(on utilise ici $(q-3)/6 > 3$)

L'élément $m_\sigma = \mathrm{Ind}_N^G(\gamma_\sigma - \nu - \nu')$ doit vérifier, par isométrie:

$$m_\sigma \in R(G) \ ; \ (m_\sigma,m_\sigma) = 3 \ ;$$

$$m_\sigma(1) = 0$$

$$(m_\sigma \ , \ \xi_{\sigma_2} - \xi_{\sigma_1}) = (\gamma_\sigma \ , \ \gamma_{\sigma_1} - \gamma_{\sigma_2})$$

$$(m_\sigma \ , \ 1_G) = 0$$

$$(m_\sigma \ , \ \psi_1) = 0$$

$$(m_\sigma \ , \ \psi_2) = (m_\sigma \ , \ \psi_3) = -1 \ .$$

On en déduit facilement

((21)) $$m_\sigma = -\xi_\sigma + \xi_3 - \xi_2 \ . \qquad ((21))$$

De même, posant $m_\Sigma = \mathrm{Ind}_N^G(\gamma_\Sigma - \mathrm{Ind}_{EQ}^N(1_{EQ})$, on a

$$m_\Sigma \in R(G) ;\ (m_\Sigma, m_\Sigma) = 7 ;$$

$$m_\Sigma(1) = 0 ;$$

$$(m_\Sigma, \psi_{\sigma_1}) = (\gamma_\Sigma, -\gamma_{\Sigma_1}) \quad \text{si} \quad \sigma_1 \in \Sigma_1 ;$$

$$(m_\Sigma, \psi_1) = 0 ;$$

$$(m_\Sigma, \psi_2) = (m_\Sigma, \psi_3) = 3 ;$$

$$(m_\Sigma, 1_G) = -1 ;$$

$$(m_\Sigma, \xi_{\sigma_1} - \xi_{\sigma_2}) = 0 .$$

Ces conditions impliquent

((22)) $$m_\Sigma = -\xi_\Sigma - 1_G + \xi_4 - \xi_5 + \xi_6 - \xi_7 + \xi_8 \qquad ((22))$$

Enfin, pour $q > 27$, les conditions

$$(\mathrm{Ind}_N^G(\gamma_{\Sigma_1} - \gamma_{\Sigma_2}) , m_\Sigma) = (\gamma_{\Sigma_1} - \gamma_{\Sigma_2} , \gamma_\Sigma)$$

imposent

((23)) $$\mathrm{Ind}_N^G(\gamma_{\Sigma_1} - \gamma_{\Sigma_2}) = \xi_{\Sigma_2} - \xi_{\Sigma_1} \quad . \qquad ((23))$$

En conclusion l'isométrie $\mathrm{Ind}_N^G : R(N|\mathcal{D}) \longrightarrow R(G|E)$ se prolonge en une isométrie définie sur tout $R(N)$ (ce prolongement n'est pas unique). On en déduit (proposition 1.26)

((24)) $$\begin{cases} \text{Pour tout } x \in (EQ - Q),\ \xi_\sigma(x) = -\gamma_\sigma(x) ;\ \xi_\Sigma(x) = -\gamma_\Sigma(x) ; \\ \qquad\qquad \xi_j(x) = -\delta_j \quad (j = 4, 5, 6, 7, 8) \\ \qquad\qquad \xi_2(x) = -\xi_3(x) = \nu(x) \\ (\text{soit } \xi_2(x) = 3 = -\xi_3(x) \text{ si } x \in (E - \{1\}) \end{cases} \qquad ((24))$$

4. Sur les 3-groupes de Sylow de G.

(1) Soient U un 3-groupe de Sylow de G contenant P, et B = $N_G(U)$. Le centre Z de U est abélien élémentaire d'ordre q. Pour tout x ∈ (P - {1}) $C_U(x) = P \times Z$ et (P × Z) est un sous-groupe normal de B, U/(P × Z) étant abélien élémentaire d'ordre q. On a

$$B = U.H \quad \text{où} \quad H = C.\langle t \rangle$$

et U.C est un groupe de Frobenius de noyau U et complément C.

(a) Soit x ∈ G d'ordre impair et divisible par 3. L'ordre de $C_G(x)$ divise $2q^3$.

Puisque $\xi_4(1) = q^3$, ξ_4 est de défaut nul. On a donc

((25)) $$\xi_4(x) = 0$$ ((25))

Selon ((1)) avec $\delta_4 = \eta = 1$, on a

$$\zeta_\rho(x) = 1 .$$

Le caractère ω_{ζ_ρ} a donc pour valeur sur la classe de x (cf ((15)) et ((16)))

$$|G:C_G(x)|\zeta_\rho(x)/\zeta_\rho(1) = q^3(q-1)/|C_G(x)|$$

donc $|C_G(x)|$ divise $q^3(q-1)$. Mais un élément différent de 1 dont l'ordre divise (q - 1)/2 est conjugué dans G d'un élément de (C - {1}), et ne centralise aucun élément d'ordre 3 (assertion (3) du paragraphe 3). Donc $|C_G(x)|$ divise $2q^3$.

(b) Si x est d'ordre impair et divisible par 3, on a

$$\zeta_\rho(x) = \zeta'_\rho(x) = 1 \ ; \ \xi_\sigma(x) = \xi_\Sigma(x) = 2\xi_3(x) - 1 \ ; \ \xi_2(x) + \xi_3(x) = 1 .$$

On sait déjà que $\zeta_\rho(x) = 1$. Or x est 2-régulier et n'est conjugué d'aucun élément de EQ. On en déduit

$$\psi_1(x) = (\zeta_\rho - \zeta'_\rho)(x) = \psi_\sigma(x) = m_\sigma(x) = m_\Sigma(x) = 0$$

pour tout σ, tout Σ, d'où (b) par ((8)), ((11)) et ((13)), ((25)), ((20)),

(c) Si x est conjugué dans G d'un élément de (P - {1}), l'ordre de $C_G(x)$ divise $2q^2$ et on a

$$\xi_3(x) = 0 .$$

Le groupe C admet 2 orbites sur $(P - \{1\})$, l'une contenant μ, l'autre contenant μ^{-1}. Si $\chi \in Irr(G)$ est à valeurs réelles, χ est constant sur $(P - \{1\})$ et on a donc

$$\chi(x) \equiv \chi(1) \pmod{q} .$$

D'où $\xi_3(x) \equiv 0 \pmod{q}$.

Comme $\xi_3(xt) = \delta_3(\phi_1 + \phi_2 + \phi_3)(x) = 0$

on a aussi $\xi_3(x) \equiv 0 \pmod{2}$.

Il existe donc $a \in \mathbb{Z}$ tel que $\xi_3(x) = 2aq$ .D'après l'assertion (b) précédente

$$\xi_\sigma(x) = 4aq - 1 .$$

On a alors

$$\sum_\sigma |\xi_\sigma(x)|^2 + \sum_\Sigma |\xi_\Sigma(x)|^2 = (4aq - 1)^2(q - 3)/6 .$$

L'assertion (a) impose

$$(4aq - 1)^2(q - 3)/6 < 2q^3$$

soit $a = 0$ et $\xi_\sigma(x) = -1$.

La constante de structure de $Z(\mathbb{Z}G)$ relative à la classe de y dans le carré de la classe de x est égale à

$$\frac{|G|}{|C_G(x)|^2} \sum_{\chi \in Irr(G)} \frac{|\chi(x)|^2 \chi(y)}{\chi(1)} = \frac{(q-1)(q^2+1)q^4}{|C_G(x)|^2}$$

Donc $|C_G(x)|$ divise $2q^2$.

(d) Démonstration de (1).

Considérons d'abord $C_G(P)$: selon (c) les 2-groupes de Sylow de $C_G(P)$ sont d'ordre 2 (t centralise P); donc $C_G(P)$ contient un 2-complément normal soit M, et M est un 3-groupe qui contient Z(U) sans être un 3-groupe de Sylow de G. Le groupe C, qui normalise P, opère sur M et, selon l'assertion (3) du paragraphe 3, M.C est un groupe de Frobenius de noyau M et complément C. On en déduit que M contient, outre P, un et un seul autre facteur C-irréductible, abélien élémentaire d'ordre q; ce facteur ne peut être que Z et on a donc $M = P \times Z$.

Considérons maintenant $N_G(M)$. Ce groupe contient encore C et t et admet un 2-complément normal, groupe dont M n'est pas groupe de Sylow. On voit

comme précédemment que C est un complément de Frobenius dans ce complément; le noyau, qui est nilpotent, se réduit à un 3-groupe (cf l'assertion (a)), et il admet 3 facteurs C-irréductibles, c'est donc un 3-groupe de Sylow de G. On a donc $N_G(M) = (U.C).\langle t\rangle$. Il est clair que U/M est abélien élémentaire, comme C-groupe irréductible. Si $x \in (P - \{1\})$, selon l'assertion (c), $C_G(x)$ se réduit à $M.\langle t\rangle$.

(2) L'opération de G sur G/B est deux fois transitive. Les 3-groupes de Sylow de G sont à intersections triviales dans G.

Posons

$$\Theta = \mathrm{Ind}_B^G(1_B) \quad \text{et} \quad m_j = (\Theta, \xi_j) \quad (1 \leqslant j \leqslant 8).$$

On a $\Theta(1) = 1 + q^3$ d'où $(\Theta, \zeta_\rho) = (\Theta, \zeta'_\rho) = 0$.

Les éléments y et ty normalisent B et sBs; on a donc $\Theta(y) \geqslant 2$ et $\Theta(ty) \geqslant 2$.

Or $\Theta(y) = 1 + m_2 + m_3 + m_4$ et $\Theta(ty) = 1 - m_2 - m_3 + m_4$ (d'après ((2)))

Il en résulte $m_4 \geqslant 1$, et par conséquent, puisque $\xi_4(1) = q^3$,

$$\Theta = 1_G + \xi_4 .$$

Ceci démontre la double transitivité de G sur les classes modulo B. En outre, puisque $H \subset B \cap sBs$ et $|G/B| = |U| + 1$, U opère régulièrement sur $(G/B - \{B\})$; autrement dit les 3-groupes de Sylow de G sont à intersections triviales.

(3) Posons $U' = P \times Z$. Si $y \in (U - U')$, y est d'ordre 9 et on a

$$C_G(y) = Z.\langle y\rangle .$$

On a aussi $U' = [U,U] = \Phi(U)$ *et* $[U,U'] = Z$. (1)

(a) Soit $z \in (Z - \{1\})$. On a

$\xi_5(z) = \xi_7(z) = -(q+q_o)/2$; $\xi_6(z) = \xi_8(z) = (q-q_o)/2$; $\xi_2(z) = 1-q$

$\xi_3(z) = q$; $\zeta_\rho(z) = 1$; $\xi_\sigma(z) = \xi_\Sigma(z) = 2q-1$; $\xi_5(z) = \xi_7(z) = (q+q_o)/2$

Puisque $|C_B(\mu)| = 2q^2$, μ admet $(q^2-q)/2$ conjugués dans B, appartenant à U', car U' est normal dans B. En outre on a

$$C_G^*(\mu) = C_B^*(\mu) = C_B(\mu) .$$

(1) on abandonne ici les notations "y générateur de C" et "z générateur de D".

donc μ et μ^{-1} ne sont pas conjugués dans G. Ainsi (U' - Z) rencontre deux classes de conjugaison de G, celle de μ et celle de μ^{-1}. On a donc, pour tout $x \in (U' - Z)$, $C_U(x) = U'$.

D'autre part, les éléments de $(Z - \{1\})$ sont conjugués sous l'action de H. Pour tout $\chi \in R(G)$, l'entier

$$q^2(\mathrm{Res}^G_{U'}\chi \ , \ 1_{U'}) = \chi(1) + (q-1)\chi(z) + (q^2-q)(\chi(\mu) + \chi(\mu^{-1}))/2$$

est divisible par q^2.

De même l'entier

$$q(\mathrm{Res}^G_P\chi \ , \ 1_P) = \chi(1) + (q-1)(\chi(\mu) + \chi(\mu^{-1}))/2 \quad \text{est divisible par } q \ .$$

De ces deux congruences il résulte

$$\chi(z) \equiv \chi(1) \pmod{q^2} \ .$$

D'autre part, si $\chi \in \mathrm{Irr}(G)$, on a aussi

$$|\chi(z)|^2 < |C_G(z)| = q^3 \ .$$

Ces deux conditions déterminent $\chi(z)$ à partir de $\chi(1)$ pour tous les éléments de Irr(G) déjà exhibés.

(b) Soit $y \in (U - U')$; on a $\xi_2(y) = 1$.

Soit $Y = \bigcup_{g \in G} (U - U')^g$. D'après (2) G contient $(q^3-1)(q^3+1)$ 3-éléments différents de 1, dont $|G|/q^2$ sont conjugués de μ ou de μ^{-1}, et $|G|/q^3$ sont conjugués d'un élément de Z. On en déduit

$$|Y| = q^2(q^3+1)(q-1)$$

Les valeurs de ξ_2 sont connues sur $C_G(t)$ et sur U' (par ((2)) et ((24))) comme sur E et C. En calculant la somme des $|\xi_2(g)|^2$ quand g parcourt l'ensemble des conjugués d'un élément de $C_G(t) \cup U' \cup E \cup C$, on obtient exactement $(|G| - |Y|)$; Comme ξ_2 est de norme 1 dans R(G), on a

$$\sum_{g \in Y} |\xi_2(g)|^2 \leqslant |Y| .$$

Mais ξ_2 étant à valeurs rationnelles, et les éléments de Y des 3-éléments, on a $\xi_2(y) \equiv \xi_2(1) \pmod 3$, soit $\xi_2(1) \equiv 1 \pmod 3$.

L'assertion (b) est démontrée.

(c) Soit $y \in (U - U')$ tel que $tyt = y^{-1}$. On a $C_U(y) = Z.\langle y \rangle$.

D'après (1)(b) et l'assertion précédente on a

$$\xi_3(y) = 0 \quad \text{et} \quad \xi_\sigma(y) = \xi_\Sigma(y) = -1 \ .$$

La fonction ψ_2 étant nulle en y, et y réel par hypothèse, on a aussi

$$\xi_5(y) = \xi_6(y) = \xi_7(y) = \xi_8(y) \ .$$

Tous les caractères de défaut non nul (pour le premier 2) étant connus, il est possible de calculer la constante de structure relativement aux classes de y, z et t en fonction du rationnel $A = \xi_5(y)$: on obtient

$$\frac{|G|}{|C_G(y)||C_G(z)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(y)\chi(z)\chi(t)}{\chi(1)} = q(q^2-1)(q+6q_oA)/|C_G(y)|$$

Ce nombre est le cardinal de l'ensemble des couples (y',z') tels que $t = y'z'$, y' étant conjugué de y et z' conjugué de z. Le centralisateur dans G d'un tel couple est un 3-groupe; d'après (1), si x est un 3-élément différent de 1 de $C_G(t)$, $C_G(x)$ ne rencontre pas la classe de y. On en conclut que $C_G(t)$ opère semi-régulièrement sur l'ensemble des couples (y',z'). Donc $|C_G(y)|$ divise $(q + 6q_oA)$.

Puisque $C_G(y)$ contient $Z.\langle y \rangle$, il existe un entier a tel que

$|C_G(y)| = 3aq$ d'où $A = bq_o$, 3a divisant l'entier $(1 + 2b)$.

On a aussi

$$\sum_{5 \leqslant j \leqslant 8} |\xi_j(y)|^2 = 4A^2 < 3aq$$

soit $4b^2 < 9a \leqslant 3(1 + 2b)$

ce qui impose b = 1 et a = 1 et l'assertion (c) en résulte.

(d) Démonstration de (3).

Le groupe dérivé de U est normal dans B et en particulier stable par H. Il est donc égal à U' ou à Z. Puisque (si y est comme en (c))

$$|[y,U]| = |U:C_U(y)| = q^2/3 \ ,$$

on a $[U,U] = U'$, d'où $\Phi(U) = U'$.

Le groupe [U,U'] est également normal dans B, différent de {1} et de U' : c'est Z.

Soit $y \in (U - U')$. Comme $[x,y]$ est central pour tout $x \in U'$, l'application qui envoie x sur $[x,y]$ est un morphisme de U' dans Z. Son image est d'ordre $|U':C_{U'}(y)| = q$; on a donc

$$[U',y] = [P,y] = Z \ .$$

Pour la même raison, U/Z étant de classe 2, l'application

$(x \in U)$ $xZ \longrightarrow [x,y]Z$ est un endomorphisme de U/Z.

D'après l'égalité précédente, $[U,y]$ est un sous-groupe de U contenant Z et d'ordre $|U:C_U(y)|$. La classe de y dans U est $y[U,y]$.

Soit maintenant $u \in U'$. Pour tout $x \in U$, on a

$$[x,uy] = [x,y][x,u]^y \ ,$$

mais, puisque $[x,u] \in Z$, il existe $v \in P$ tel que $[x,u] = [v,y]$, d'où

$$[x,uy] = [x,y][v,y] = [xv,y] \ .$$

Il en résulte que

$$[U,uy] = [U,y] \quad \text{pour tout } u \in U' \ .$$

En particulier, si y est inversé par t, $[U,uy]$ est d'ordre $q^2/3$ donc $C_U(uy)$ est d'ordre 3q, ce qui implique $C_U(uy) = Z.\langle uy\rangle$. La classe de conjugaison de uy dans U est $uy[U,y]$, contenue dans yU', et yU' est réunion de 3 classes de conjugaison de U. Sous l'action de H, yU' parcourt U/U', ce qui démontre finalement que

$$C_U(y) = Z.\langle y\rangle \text{ pour tout } y \in (U - U').$$

Si l'un des éléments y de $(U - U')$ est d'ordre 3, uy est d'ordre 3 pour tout u de U', et finalement, sous l'action de H, tout élémént de $(U - U')$ est d'ordre 3. Donc U est alors d'exposant 3. Dans un tel groupe un élément commute à ses conjugués, ce qui n'est pas le cas de y, car $|[y,U]| < |C_U(y)|$.

L'assertion (3) est démontrée.

(4) Présentation de B.

Les assertions (1) et (3) permettent de montrer que la structure de B est déterminée par un certain automorphisme σ du corps fini $\mathbb{F}_q$ (cf [28] ,I) Plus généralement ([1]), il est possible de classifier les p-groupes de classe 3 admettant un groupe cyclique d'automorphismes d'ordre (q-1) et opérant irréductiblement sur chacun des facteurs de la suite centrale descendante, (p étant un premier impair). Un tel groupe est d'ordre $q^{5/2}$, $q^{7/3}$ ou q^3. S'il est d'ordre q^3, σ^2 n'est pas l'identité et, pour σ donné, il existe deux types de groupes, selon que, lorsqu'un élément n'est pas dans le groupe dérivé, son centralisateur dans le groupe dérivé se réduit au centre ou non. L'assertion (3) élimine donc un type. Soit $K = \mathbb{F}_q$ et soit $K^\times$ son groupe multiplicatif. On montre qu'il existe un isomorphisme de $K^\times$ sur H - qui sera noté ici ($w \longrightarrow \lceil w \rceil$) et une bijection de K^3 sur U tels que le produit semi-direct B = U.H soit ainsi isomorphe au produit semi-direct $(K^3).K^\times$ défini par les lois

$$(x,y,z).(x',y',z') = (x+x'+y'z+z'^{\sigma}z^2+z'z^{\sigma+1}-z'^2z^{\sigma} \ , \ y+y'+z'z^{\sigma}-z'^{\sigma}z \ , \ z+z')$$

$$w.(x,y,z).w^{-1} = (w^{\sigma+2}x \ , \ w^{\sigma+1}y \ , \ wz)$$

($(x,y,z) \in K^3$, $(x',y',z') \in K^3$ et $w \in K^\times$). ([2])

Dans le chapitre 5, U sera identifié à K^3 muni du produit précédent, on distinguera cependant entre élément de $K^\times$ et élément de H. On écrira donc

$$\lceil w \rceil (x,y,z) \lceil w \rceil^{-1} = (w^{\sigma+2}x \ , \ w^{\sigma+1}y \ , \ wz) \ .$$

On a clairement $t = \lceil -1 \rceil$. Le centre de U est l'ensemble des (x,0,0); le centralisateur de t dans U, P, est l'ensemble des (0,y,0). Puisque H opère

([1]) cf M. Enguehard, "Obstructions et p-groupes de classe 3", même fascicule.

([2]) Les automorphismes de K ainsi que les éléments de l'anneau $\mathbb{Z}[\sigma]$, considéré comme anneau d'endomorphismes de $K^\times$, sont notés en exposant.

"sans point fixe" sur Z(U) (assertion (1)), $(\sigma+2)$ est une bijection. Il existe donc b (dans l'anneau des endomorphismes de K^x et prolongé en 0 par $0^b = 0$) tel que

$$b(\sigma+2) = (\sigma+2)b = 1$$

et cette notation sera utilisée dans les chapitres 5 et 6.

Puisque $C_B(t)/\langle t\rangle$ est isomorphe à l'image dans $PSL_2(q)$ du groupe des matrices (2,2) triangulaires unimodulaires, $(K^x)^{\sigma+1}$ est le groupe des carrés de K^x. Il existe donc a tel que

$$a(\sigma+1) = 2 .$$

On peut supposer que

$$(-1)^a = 1 ,$$

et cette notation sera utilisée dans les chapitres 5 et 6.

Enfin, si $w^\sigma = w$, selon les lois du produit $(0,0,wz)$ et $(0,0,z)$ se centralisent. Selon (3) w est dans le corps premier. Autrement dit, <u>le corps des points fixes de</u> σ <u>est</u> $\mathbb{F}_3$.

5. Premiers divisant $(q^2 - q + 1)$.

(1) G admet des sous-groupes de Hall abéliens A et B, d'ordres respectifs $(q - 3q_o + 1)$ et $(q + 3q_o + 1)$. Si $x \in (A - \{1\})$, $C_G(x) = A$; Si $y \in (B - \{1\})$, $C_G(y) = B$; en outre x et y sont réels.

Remarquons que les entiers $q(q^2-1)$, $(q-3q_o+1)$ et $(q+3q_o+1)$ sont premiers entre eux deux à deux, leur produit étant l'ordre de G. Soient r un nombre premier divisant $(q-3q_o+1)$ et ℓ un nombre premier divisant $(q+3q_o+1)$; soient x un élément de G dont l'ordre est divisible par r et y un élément de G dont l'ordre est divisible par ℓ. Les caractères irréductibles ζ_ρ, ξ_σ, ξ_2 et ξ_3 sont de défaut nul pour r et pour ℓ, ils sont donc nuls en x et en y. On voit aussi par le même argument que

$$\xi_6(x) = \xi_8(x) = 0 \quad \text{et} \quad \xi_7(y) = \xi_5(y) = 0 .$$

Puisque x et y sont d'ordres impairs, on a

$$\psi_1(x) = \psi_2(x) = \psi_1(y) = \psi_2(y) = 0 ,$$

d'où $\xi_4(x) = \xi_4(y) = -1$; $\xi_5(x) = \xi_7(x) = -1$ et $\xi_6(y) = \xi_8(y) = 1$.

Si $\chi \in \mathrm{Irr}(G)$, le produit $\chi(t)\chi(x)$ n'est non nul que pour les 4 caractères 1_G, ξ_4, ξ_5 et ξ_7, ce qui permet de calculer le nombre des involutions qui appartiennent à $C_G^*(x)$, soit

$$\frac{|G|}{|C_G(t)|^2} \sum_j \frac{\xi_j(t)^2 \xi_j(x)}{\xi_j(1)} = q - 3q_o + 1$$

Donc $C_G^*(x)$ contient au moins une involution. Les centralisateurs des éléments de $C_G(t)$ sont tous connus; on voit ainsi qu'aucun élément de $C_G(x)$ autre que 1 ne centralise d'involution. Une involution de $C_G^*(x)$ opère sans point fixe sur $C_G(x)$, qui est nécessairement abélien; en outre $C_G(x)$ est d'ordre $(q - 3q_o + 1)$. C'est ainsi un groupe de Hall de G; notons-le A. Le raisonnement précédent s'applique à tout élément de $(A - \{1\})$ comme à x. On a donc $C_G(x') = A$ pour tout $x' \in (A - \{1\})$.

De la même façon on démontre que $C_G(y)$ contient $(q + 3q_o + 1)$ involutions, ce qui implique que $B = C_G(y)$ est abélien d'ordre $(q + 3q_o + 1)$

(2) Tout élément de G dont l'ordre est premier à 3 est réel.

Cette assertion est une conséquence immédiate de (1) et de la structure de $C_G(t)$.

(3) $N_G(A)$ est un groupe de Frobenius de noyau A et complément cyclique d'ordre 6; $N_G(B)$ est un groupe de Frobenius de noyau B et complément cyclique d'ordre 6.

Tout élément de G est conjugué d'un élément de la réunion des groupes $C_G(t)$, A, B et U. Il est donc possible de calculer l'ordre de $\bigcup_{g \in G} (A \cup B)^g$. On obtient $1 + (q^4(q^2-1)(q-2)/3)$.

L'assertion (1) implique que $N_G(A)$ est un groupe de Frobenius de noyau A, complément cyclique d'ordre 2a ($a \in \mathbb{N}$) et $N_G(B)$ un groupe de Frobenius de noyau B, complément cyclique d'ordre 2b ($b \in \mathbb{N}$). On a alors

$$\left| \bigcup_{g \in G} (A \cup B)^g \right| = 1 + \frac{(q-3q_o)q^3(q^2-1)(q+3q_o+1)}{2a} + \frac{(q+3q_o)q^3(q^2-1)(q-3q_o+1)}{2b}$$

d'où l'on déduit

$$\frac{2}{3} = \frac{1}{a} + \frac{1}{b} + \frac{a-b}{ab(q-2)q_o}$$

Selon un théorème de Sylow,

$$|G:N_G(A)| \equiv 1 \pmod{r},$$

soit $$q^3(q^2-1)(q+3q_o+1) \equiv 2a \pmod{r},$$

ce qui, compte-tenu de

$$q-3q_o+1 \equiv 0 \pmod{r}$$

conduit à $$a \equiv 3 \pmod{r}.$$

Comme a est impair et r divise (q^3+1), $3 \not\equiv -1 \pmod{r}$; donc on a $a \geqslant 3$.

On démontre de même que $b \geqslant 3$.

On voit alors, dans l'égalité précédente liant a et b, que nécessairement $a = b = 3$.

6. Sur l'automorphisme σ. La condition de Thompson.

Nous reprenons ici pour l'essentiel un article de Thompson [28],II. Cependant la présentation et les notations sont légèrement différentes (les matrices sont multipliées "à la française", ce qui modifie les relations dans le groupe linéaire); en outre les calculs ont été simplifiés.

(1) Le groupe ${}^2G_2(3)$ est contenu dans G.

Le groupe ${}^2G_2(3)$ est identifié dans G grâce à son isomorphisme avec le groupe $P\Gamma L_2(8)$.

On a démontré dès le paragraphe 2, assertions (1) à (4), qu'un 2-Sylow S de G est abélien élémentaire d'ordre 8, son propre centralisateur dans G et de normalisateur $N_G(S) = S.L.\langle\mu\rangle$, où μ, d'ordre 3, centralise t dans S, et L est d'ordre 7, transitif sur l'ensemble des involutions de S ([1]). Selon l'assertion (2) du paragraphe 5, tout élément de L est réel; le groupe $N_G(L)/C_G(L)$ est donc abélien d'ordre 6 et, puisque μ normalise L, le groupe $(C_G(\mu) \cap N_G(L))/(C_G(\mu) \cap C_G(L))$ est également abélien d'ordre 6. Puisque μ appartient à U, $C_G(\mu)$ est contenu dans B (assertions (1) et (2) du paragraphe 4), et on en déduit qu'il existe une involution v qui centralise μ et normalise L, de telle sorte que

$$N_G(L) = C_G(L)\langle\mu v\rangle .$$

Nous allons démontrer que le groupe engendré par $(S \cup L \cup \{\mu v\})$ est isomorphe à $P\Gamma L_2(8)$.

(a) Soit $G_o = SL \cup SLvS$. C'est un sous-groupe de G isomorphe à $PSL_2(8)$.

Supposons que $S \cap vSv$ soit distinct de $\{1\}$. Alors v centralise une involution appartenant à S; plus précisément, puisque v normalise L (qui est transitif sur $(S - \{1\})$) et centralise μ, v normalise S et centralise t. Or on voit dans $C_G(\mu) = C_B(\mu) = C_U(\mu)\langle t\rangle$ que deux involutions

([1]) l'élément noté ici μ ne coïncide pas avec μ du ch.2, (3), qui centralisait u et non t.

distinctes de $C_G(\mu)$ ne se centralisent pas. Mais v et t sont distinctes, car t ne normalise pas L. Cette contradiction montre que $S \cap vSv = \{1\}$. On en déduit que $S.L \cap v(S.L)v = L$. Comme vt, élément de $C_U(\mu) = [U,U]$ est d'ordre 3, on a, pour $y \in L$,

$$vt^{y^{-1}}v = (vtv)^y = (tvt)^y = t^{y}y^{-2}vt^y$$

d'où $vSv \subset (\{1\} \cup SLvS)$.

On voit que G_o est un sous-groupe d'ordre 7.8.9 de G, décomposé en deux doubles classes SL et SLvS selon SL. On a donc $SL = N_{G_o}(SL)$ et G_o est deux fois transitif sur G_o/SL ; comme $N_{G_o}(S) \cap N_{G_o}(vSv) = L$, G_o est exactement 3 fois transitif sur G_o/SL; G_o est donc isomorphe à $PSL_2(8)$ opérant sur la droite projective sur $\mathbb{F}_8$.

(b) $G_1 = \langle G_o, \mu \rangle$ est isomorphe à $P\Gamma L_2(8)$. Ajustement.

Il est clair que μ normalise G_o, mais que μ n'appartient pas à G_o (μ normalise SL et $N_{G_o}(SL) = SL$). Donc μ induit un automorphisme d'ordre 3 de $PSL_2(8)$, si bien que G_1 est isomorphe au groupe des "transformations projectives semi-linéaires" sur le corps $\mathbb{F}_8$, $P\Gamma L_2(8)$.

Posons pour simplifier $X = P\Gamma L_2(8)$ et $Y = PSL_2(8)$ considérés comme groupes de transformations homographiques sur $(\mathbb{F}_8 \cup \{\infty\})$ et soit ϕ un isomorphisme de G_1 sur X,

Un 3-Sylow de Y est cyclique d'ordre 9, un 3-Sylow de X est non abélien d'ordre 27; il en résulte que (X - Y) contient une seule classe de conjugaison de sous-groupes d'ordre 3. En modifiant éventuellement ϕ par un automorphisme intérieur de Y, on peut supposer que $\phi(\mu)$ est de la forme $(x \longrightarrow x^{\tau})$ où τ est égal à 2 ou 4. Puisque $C_X(\phi(\mu))$ est diédral d'ordre 6, on peut également supposer que $\phi(t)$ est la transformation $(x \longrightarrow x+1)$. L'involution s centralise t, et les involutions s, $\mu s \mu^{-1}$, $\mu^{-1} s \mu$ engendrent un groupe d'ordre 4; on en déduit qu'il existe un élément c du corps $\mathbb{F}_8$, de trace nulle ($c + c^2 + c^4 = 0$) tel que $\phi(s)$ soit la transformation $(x \longrightarrow x+c)$. Soit enfin $\tilde{\eta}$ la transformation

$(x \longrightarrow (c^2x + c)/(cx + c^4))$; c'est un élément d'ordre 9 de Y, inversé par $\phi(t)$ et tel que $\phi(\mu)\tilde{\eta}\phi(\mu^{-1}) = \tilde{\eta}^{-2}$ ou $\tilde{\eta}^4$ selon que τ est 2 ou 4. Soit $\eta = \phi^{-1}(\tilde{\eta})$. Puisque η et μ engendrent un 3-groupe, η appartient à U; reprenons la présentation de B introduite au chapitre 4, assertion (4): $t = [-1]$ et t inverse η, donc η est de la forme (d,0,b) où d, b $\in$ K. Dans cette présentation $\mu = (0,1,0)$ [1] d'où $\mu\eta\mu^{-1} = (d - b\ ,\ 0\ ,\ b)$. Puisque η est d'ordre 9, b n'est pas nul et l'égalité $\mu\eta\mu^{-1} = \eta^{1\pm3}$ s'écrit $-b = \pm b^{\sigma+2}$, soit $b^{\sigma+1} = \pm 1$; mais -1 n'est pas dans l'image de $(\sigma+1)$, donc $b^{\sigma+1} = 1$, soit b = 1 ou b = -1 . On a donc $\mu\eta\mu^{-1} = \eta^{-2}$, ce qui montre que τ est égal à 2. Il est encore possible de modifier ϕ par l'automorphisme intérieur selon $\phi(t)$: $\phi(t)$ centralise $\phi(s)$, $\phi(\mu)$ et transforme $\phi(\eta)$ en $\phi(\eta^{-1})$; celà permet d'échanger éventuellement η et η^{-1}, donc de supposer que b = 1.

En résumé:

$\mu = (0,1,0)$ et $\phi(\mu)$ est $(x \longrightarrow x^2)$

$t = [-1]$ et $\phi(t)$ est $(x \longrightarrow x+1)$

$\phi(s)$ est $(x \longrightarrow x+c)$ (où $c + c^2 + c^4 = 0$)

$\eta = (d,0,1)$ et $\phi(\eta)$ est $(x \longrightarrow (c^2x + c)/(cx + c^4))$

L'incertitude sur l'élément d ne sera levée qu'une fois démontrée l'assertion "σ est une racine carrée du Frobenius".

(2) Le groupe G comme extension de B : une condition en σ.

On peut considérer G comme une extension transitive de B, opérant sur l'ensemble Ω des classes modulo B dans G (cf l'assertion (2) du chapitre 4. Le sous-groupe B de G est le fixateur de $B \in \Omega$ et il possède un sous-groupe normal U, régulier sur $(\Omega - \{B\})$; en outre le fixateur de deux points B et sB de Ω est un complément H de U dans B. Cette situation a été envisagée par J.Tits [29] ; il note (théorème 7) que G est alors déterminé par B et les deux applications notées ω et ρ ci-dessous, l'existence de G dépendant essentiellement d'une relation en ω et ρ exprimant que la

(1) il existe une seule classe de sous-groupes d'ordre 3 dans $C_G(t)$; nous pouvons donc supposer que S est choisi de telle sorte que μ normalise S.

loi de produit est associative dans G ([1]).

On a en effet $G = B \cup UsB$ (réunion disjointe) et la loi de groupe est déterminée par la connaissance de l'application $(u \longrightarrow sus)$ de $(U - \{1\})$ dans UsB. Plus précisément s détermine une permutation ω de $(U - \{1\})$ et une application ρ de $(U - \{1\})$ dans H telles que

((1)) $\quad sus = \omega(u)s\rho(u)\pi(u)$ où $u \in (U - \{1\})$, $\rho(u) \in H$, $\pi(u) \in U$, $\omega(u) \in U$ ([2])

Puisque s inverse tout élément de H, on a nécessairement

((2)) $\quad \omega(huh^{-1}) = h^{-1}\omega(u)h$ et $\pi(huh^{-1}) = h^{-1}\pi(u)h$ où $h \in H$ et $u \in (U - \{1\})$

Des relations précédentes on déduit facilement, par inversion et opération de H

((3)) $\quad \rho(huh^{-1}) = h^2\rho(u)$

((4)) $\quad \rho(\omega(u)) = \rho(u)^{-1}$

((5)) $\quad \rho(u^{-1}) = \rho(u)$

((6)) $\quad \pi(u) = \omega(u^{-1})^{-1} = \rho(u)^{-1}\omega(\omega(u)^{-1})\rho(u)$.

Nous allons calculer ω sur le groupe dérivé de U et en déduire une propriété de σ dite "condition de Thompson". Ce calcul est possible car les fonctions ω, ρ, π sont connues sur $(U \cap G_1)$.

L'élément $s\mu$ étant d'ordre 3, on a $s\mu s = \mu^{-1}s\mu^{-1}$, soit

$$\omega(\mu) = \mu^{-1} = \pi(\mu) \; ; \; \omega(\mu^{-1}) = \mu = \pi(\mu^{-1}) \; ; \; \rho(\mu) = 1 = \rho(\mu^{-1}) \; .$$

Le groupe H ayant deux orbites sur $(P - \{0\})$, on en déduit par ((1)), ((2))

([1]) Dans [29] les hypothèses sont plus générales, l'ensemble Ω n'est pas supposé fini et l'existence d'une involution qui échange deux conjugués de B n'est pas assurée.

([2]) Nous reprenons dans ce chapitre une numérotation des formules, indépendamment de la numérotation des formules des chapitres 3 et 4. Il en sera de même au chapitre 7.

et ((3)) que si y est non nul on a

$$\omega((0,y,0)) = (0,-y^{-1},0) = \pi((0,y,0)) \quad \text{et} \quad \rho((0,y,0)) = \lceil y \rceil^a$$

(nous reprenons évidemment les notations introduites à la fin du chapitre 4)

Ces égalités seront utilisées sans rappel; on retrouve en fait les applications ω, ρ et π propres au groupe $PSL_2(K)$.

D'autre part, grâce à l'isomorphisme ϕ, on connait sus si $u \in (U \cap G_1)$ on a par exemple

((7)) $\qquad s\eta^3\mu s = \eta^2 s t \eta^3 \mu$.

Posons, pour tout $x \in (K - \{0\})$,

((8)) $\qquad u(x) = (1,x,0)$; $f(x) = \omega(u(x))$, $g(x) = \pi(u(x))$ et $h(x) = \rho(u(x))$

La formule ((1)) s'écrit dans ce cas $su(x)s = f(x)sh(x)g(x)$ et ((7)) nous donne

((7')) $\qquad f(1) = \eta^2 = (-d+1, 0, -1)$

$$g(1) = \eta^3\mu = u(1)$$

$$h(1) = t = \lceil -1 \rceil .$$

En transformant par s l'égalité $u(x) = (1,1,0)(0,x-1,0)$, (pour $x \neq 1$) on obtient

$$f(x)sh(x)g(x) = \eta^2 st(1,1,0)(0,-(x-1)^{-1},0)s\lceil x-1 \rceil^a (0,-(x-1)^{-1},0)$$

$$= \eta^2 tsu(1-(x-1)^{-1})s\lceil x-1 \rceil^a (0,-(x-1)^{-1},0) .$$

Posons

$$\zeta(x) = 1 - (x-1)^{-1} \quad \text{(pour } x \neq 1, 0) .$$

D'après ce qui précède et les notations ((8)) on a

((9)) $\qquad f(x) = \eta^2 t f(\zeta(x)) t$

((10)) $\qquad h(x) = th(\zeta(x))\lceil x-1 \rceil^a$

((11)) $\qquad g(x) = \lceil x-1 \rceil^{-a} g(\zeta(x)) \lceil x-1 \rceil^a (0,-(x-1)^{-1},0)$.

Si x est différent de 1, on a $\zeta^2(x) = x$, si bien que ((9)) peut s'écrire

((9')) $\qquad f(\zeta(x)) = \eta^2 f(x)^t$

De l'égalité évidente $u(-x)^t = u(x)^{-1}$, et de ((2)) à ((6)) il résulte

((13)) $\qquad h(-x) = h(x)$

((14)) $\qquad f(-x) = g(x)^{-t}$

Les égalités ((10)) et ((13)) impliquent que si x est différent de 0, 1 ou -1, on a $h(\zeta(-x))\lceil x+1\rceil^a = h(\zeta(x))\lceil x-1\rceil^a$. Mais $\zeta(-x) = \zeta(x)^{-1}$, d'où, en posant $y = \zeta(x)$,

((15)) $\qquad h(y^{-1}) = h(y)\lceil y\rceil^{-a} \qquad$ où $y \notin \{0,1,-1\}$.

De la même façon, des égalités ((11)) et ((14)), on déduit

$$f(-x)^{-t} = \lceil x-1\rceil^{-a} f(-\zeta(x))^{-t} \lceil x-1\rceil^a (0\ ,\ -(x-1)^{-1}\ ,\ 0)$$

Mais on a $-\zeta(x) = \zeta(x^{-1})$, d'où, d'après ((9')), $f(-\zeta(x))^{-t} = f(x^{-1})^{-1}\eta^2$.

On obtient ainsi

$$f(-x)^{-t} = \lceil x-1\rceil^{-a} f(x^{-1})^{-1}\eta^2 \lceil x-1\rceil^a (0\ ,\ -(x-1)^{-1}\ ,\ 0)$$

En répétant cette égalité, on obtient

$$f(x^{-1})^{-t} = \lceil x^{-1}+1\rceil^{-a} f(-x)^{-1}\eta^2 \lceil x^{-1}+1\rceil^a (0, (x^{-1}+1)^{-1}\ ,\ 0)$$

d'où

$$f(-x) = (0\ ,\ (x-1)^{-1}\ ,\ 0)\lceil x-1\rceil^{-a}\eta^2 f(x^{-1})^t \lceil x-1\rceil^a$$

$$= (0\ ,\ (x-1)^{-1}\ ,\ 0)\lceil x-1\rceil^{-a}\eta^2 (0\ ,\ -(x^{-1}+1)^{-1}\ ,\ 0)\lceil x^{-1}+1\rceil^{-a}\eta^{-2} f(-x) \ldots$$

$$\ldots \lceil x^{-1}+1\rceil^a \lceil x-1\rceil^a$$

Posons $w = (x^{-1}+1)(x-1) = x - x^{-1}$. Changeant x en -x ($w^2$ est invariant) :

$$\lceil w\rceil^a f(x) \lceil w\rceil^{-a} = (0\ ,\ -w^2(x+1)^{-1}\ ,\ 0)\lceil w(x+1)^{-1}\rceil^a \eta^2 (0\ ,\ (x^{-1}-1)^{-1}\ ,\ 0) \ldots$$

$$\ldots \lceil -(x^{-1}+1)\rceil^{-a}\eta^{-2} f(x)$$

$$\lceil w\rceil^a f(x) \lceil w\rceil^{-a} = u_1 f(x)$$

où $\quad u_1 = (0\ ,\ -w(1-x^{-1})\ ,\ 0)((1-x^{-1})^{\overbrace{a(\sigma+2)}^{(1-d)}}\ ,\ 0\ ,\ -(1-x^{-1})^a)(0\ ,\ x^{-1}-1\ ,\ 0)(d-1\ ,\ 0\ ,\ 1)$

$$= (\alpha_1\ ,\ \beta_1\ ,\ \gamma_1)$$

avec $\qquad \gamma_1 = 1 - (x^{-1} - 1)^a$

$$\beta_1 = (w+1)(x^{-1} - 1) - (x^{-1} - 1)^{a\sigma} + (x^{-1} - 1)^a \ .$$

Posons $\qquad \alpha_1 = d(1 - (x^{-1} - 1)^{a+2}) + \gamma_1^2 - (x^{-2} + 1)\gamma_1 - \gamma_1^{\sigma} - x^{-2} + x^{-1} + 1 \ .$

((16)) $\qquad f(x) = (\alpha(x)\ ,\ \beta(x)\ ,\ \gamma(x)) \ .$

On obtient finalement

((17)) $\qquad \gamma(x) = (x^a - (x-1)^a)((x^2 - 1)^a - x^a)^{-1}$

((18)) $\qquad \beta(x) = x^2(x^4 + 1)^{-1}(\beta_1 + \gamma_1(x)^{\sigma}\gamma(x) - \gamma(x)^{\sigma}\gamma_1(x))$

((19)) $\qquad \alpha(x) = (w^{a+2} - 1)^{-1}(\alpha_1(x) + (w^a - 1)\beta(x)\gamma(x)$

$$+ (w^{2a} + w^2 + w^{a\sigma})\gamma(x)^{\sigma+2}) \ .$$

On vérifie que les formules ((17)) et ((18)) sont également vraies pour $x = 1$ et $x = -1$.

En conjuguant $u(x)$ par un élément arbitraire de H on obtient

((20)) $$\lceil r\rceil s(r^{\sigma+2}, r^{\sigma+1}x, 0)s\lceil r\rceil^{-1} = f(x)sh(x)g(x) ,$$

ce qui définit ρ, ω et π sur $([U,U] - (Z(U) \cup P))$. Si (x,r) et (x',r') sont tels que $sg(x')f(x)\lceil rr'^{-1}\rceil$ soit connu, l'associativité du produit fournit une condition non triviale en σ. Prenons $x = -1$ et $x' = 1$. Selon ((7')), ((13)) et ((14)) on a

$$su(1)s = \eta^2 stu(1) \quad \text{et} \quad su(-1)s = u(-1)st\eta^2 .$$

Avec $r' = 1$ et $r \notin \mathbb{F}_3$ on obtient

$$\begin{aligned} & s(1+r^{\sigma+2}, 1-r^{\sigma+1}, 0)s \\ &= su(1)\lceil r\rceil u(-1)\lceil r\rceil^{-1}s \\ &= \eta^2 stu(1)(u(-1)st\eta^2)\lceil r\rceil \\ &= \eta^2\lceil r\rceil ts\lceil r\rceil u(1)\lceil r\rceil^{-1}u(-1)st\eta^2\lceil r\rceil . \end{aligned}$$

Or $$\lceil r\rceil u(1)\lceil r\rceil^{-1}u(-1) = (1+r^{\sigma+2}, -1+r^{\sigma+1}, 0) .$$

Soient donc $y, u \in K$ tels que

$$(1 + r^{\sigma+2})y^{\sigma+2} = 1 \quad \text{et} \quad (r^{\sigma+1} - 1)y^{\sigma+1} = u .$$

($(1 \pm r^{\sigma+1})$ étant non nuls et $(\sigma+2)$ bijectif, y est bien défini et u n'est pas nul) Selon ((20)) on a

$$s(1+r^{\sigma+2}, 1-r^{\sigma+1}, 0)s = \lceil y\rceil f(-u)sh(-u)g(-u)\lceil y\rceil^{-1} ,$$

et $$s(1+r^{\sigma+2}, r^{\sigma+1}-1, 0)s = \lceil y\rceil f(u)sh(u)g(u)\lceil y\rceil^{-1} .$$

On en déduit (unicité des décompositions à la Bruhat)

$$\begin{aligned} \lceil y\rceil f(-u)\lceil y\rceil^{-1} &= \eta^2\lceil r\rceil t\lceil y\rceil f(u)\lceil y\rceil^{-1} t\lceil r\rceil^{-1} \\ &= \eta^2\lceil -ry\rceil f(u)\lceil -ry\rceil^{-1} . \end{aligned}$$

Quand r parcourt $(K - \mathbb{F}_3)$, y parcourt $(K - \mathbb{F}_3)$ et inversement; quant à u, il est défini par y comme par r. Posons donc $z = -ry$. En conclusion

" Dès que $y \in (K - \mathbb{F}_3)$, $y^{\sigma+2} - z^{\sigma+2} = 1$ et $z^{\sigma+1} - y^{\sigma+1} = u$,

" on a

" ((21)) $$\lceil y\rceil f(-u)\lceil y^{-1}\rceil = \eta^2\lceil z\rceil f(u)\lceil z^{-1}\rceil .$$

Ce résultat a été obtenu par Thompson [28] II (théorème 8.1). Si on considère la troisième composante de la fonction f, on obtient une propriété d'expression simple qui suffira à démontrer que $\sigma^2 = 3$. De ((21)) on déduit en effet $y\gamma(-u) = -1 + z\gamma(u)$. D'où par ((17)) la condition de Thompson

" Sous les mêmes hypothèses on a

" ((22)) $\quad z(1-u)^a + (y-z-1)u^a - y(1+u)^a + (u^2-1)^a = 0$.

Au chapitre suivant on utilisera une forme plus faible de la condition précédente: au lieu de supposer que $y \notin \mathbb{F}_3$, on supposera que $u \notin \mathbb{F}_3$. Il est clair que si $y \in \mathbb{F}_3$, alors $u \in \mathbb{F}_3$.

Sur la fonction ω: La fonction ω est explicitée par J. Tits [29] . Le groupe U y est présenté de la façon suivante $(x,y,z,\ldots \in K)$

$$(x,y,z)_J(x',y',z')_J = (x+x' , y+y'+x^{\sigma}x' , z+z'-xy'+yx'-x^{\sigma+1}x')_J .$$

Notons $(x,y,z)_M$ l'élément générique du groupe U présenté au chapitre 4. Les applications

$$(x,y,z)_J \longrightarrow (z-xy-x^{\sigma+2} , -y-x^{\sigma+1} , -x)_M$$

$$(x,y,z)_M \longrightarrow (-z , -y-z^{\sigma+1} , x+yz)_J$$

sont des isomorphismes réciproques. Les groupes notés ici et dans [29] "H" se correspondent formellement, de même que l'application ω. Selon [29] la fonction ω transforme $(x,y,z)_J$ en $(v/w,u/w,z/w)_J$ si $(x,y,z) \neq (0,0,0)$ et où

$$u(x,y,z) = x^2y - xz + y^{\sigma} - x^{\sigma+3} ,$$

$$v(x,y,z) = x^{\sigma}y^{\sigma} - z^{\sigma} + xy^2 + yz - x^{2\sigma+3} ,$$

$$w(x,y,z) = -z^2 - xv(x,y,z) - yu(x,y,z) . \qquad ([1])$$

La fonction ω est donc connue a priori, mais l'expression formelle ci-dessus tient compte de l'égalité $\sigma^2 = 3$.

([1]) Selon les indications de l'auteur il faut rectifier dans [29]: p.210-12, les ε_i sont tous égaux à 1; en (5.2) $y_i = p_{(-i)(-i+1)}$, $y_{i'} = p_{(1-i)(-i)'}$; p.210-15, ω comme ci-dessus, (6.8) lire: $\rho_a(-\omega^{-1}(-a)) = \omega^{-1}(-\omega(a))$ et en 210-16 : $\rho_a = -w(a)^{2-\sigma}$

7. $\sigma^2 = 3$.

Dans ce chapitre on démontre que la condition de Thompson obtenue au chapitre précédent implique que le carré de σ est l'automorphisme de Frobenius, autrement dit que " $\sigma^2 = 3$ ", sauf peut-être pour un nombre fini de cas. On suit d'assez près l'article de Bombieri [1] , mais on ne suppose pas que le corps soit fini, le lemme 6 et son corollaire se substituant au lemme 3 de [1]. Pour mettre en évidence la simplicité de la méthode employée, des calculs sans intérêt propre ont été rejetés au paragraphe (3), et on a éliminé quelques raffinements employés par Bombieri pour réduire le nombre des cas exceptionnels, où un calcul direct doit suppléer à la démonstration générale.

Comme au chapitre précédent, les applications multiplicatives de K dans K, ou les endomorphismes du groupe multiplicatif de K, sont notés en exposant, ce qui donne son sens à l'égalité placée en tête de chapitre.

Théorème. *Soit* K *un corps commutatif de caractéristique* 3 *et soit* σ *un endomorphisme de* K. *On suppose que*

1) $(\sigma+2)$ *est bijectif;*

2) le corps des points fixes de σ *est le corps premier* $\mathbb{F}_3$;

3) il existe une application multiplicative a *de* K *dans* K *telle que*

$$a(\sigma+1) = 2 \ ;$$

4) Si $y, z, u \in K$ *sont tels que* $u \notin \mathbb{F}_3$ *et*

$$(E_1) \qquad y^{\sigma+2} - z^{\sigma+2} = 1$$

$$(E_2) \qquad z^{\sigma+1} - y^{\sigma+1} = u \ ,$$

on a

$$(T) \qquad z(u-1)^a + (y-z-1)u^a - y(u+1)^a + (u^2-1)^a = 0$$

Alors il existe un entier M *tel que, ou bien le carré de* σ *est l'endomorphisme de Frobenius, ou bien* K *est de cardinal au plus* M.

(1) Elimination de a, u, y.

Le but de ce paragraphe est de démontrer l'assertion

Il existe $H \in \mathbb{F}_3[Z_0,Z_1,Z_2,Z_3,Z_4]$ *tel que les hypothèses du théorème impliquent*

$$H(z,z^{\sigma},z^{\sigma^2},z^{\sigma^3},z^{\sigma^4}) = 0 \quad \textit{quel que soit} \quad z \in K .$$

Notons tout d'abord quelques conséquences très élémentaires des hypothèses 1) à 4).

Lemme 1. (a) Quel que soit $x \in K$, $x^{\sigma+1}$ est différent de -1, en particulier -1 n'est pas un carré dans K.

(b) Si $x \in K$ et $x^{\sigma+1} = 1$, $x^2 = 1$.

Si $K = \mathbb{F}_9$, les conditions 2) et 3) sont irréalisables. Comme a et σ stabilisent tout sous-corps fini de K, $\mathbb{F}_9$ n'est pas contenu dans K. Il résulte alors de la condition 2) que $\mathbb{F}_3$ est le corps des points fixes de σ^2. Or, si $x^{\sigma+1} = 1$, x est fixe par σ^2; on en déduit l'assertion (b). Si $x^{\sigma+1} = -1$, $(x^2)^{\sigma+1} = 1$, donc $x^2 \in \mathbb{F}_3$, donc $x \in \mathbb{F}_3$, ce qui démontre l'assertion (a).

Selon la condition 1), $z \neq 0$, (E_1) et (E_2) déterminent y et u. Posons donc

$$E_{\sigma} = \{z \in K / \text{ si } (E_1) \text{ et } (E_2) , u \notin \mathbb{F}_3\} .$$

Lemme 2. Si $z \in E_{\sigma}$, (E_1) et (E_2), alors $yz(y - z - 1) \neq 0$

Démonstration: Si y est nul, selon (E_1) et (E_2), $z = -1$ et $u = 1$. De même, si z est nul, on a $y = 1$ et $u = -1$.

D'autre part, (E_1) et (E_2) impliquent

((1)) $$z^{\sigma+1} = (1 + uy)/(y - z)$$

((2)) $$y^{\sigma+1} = (1 + uz)/(y - z) .$$

d'où $$z^{\sigma} - y^{\sigma} = (1 + u(y + z))/yz .$$

Si $(y - z - 1)$ est nul, $(y^{\sigma} - z^{\sigma} - 1)$ est nul, d'où $(z - 1 - u)(z - 1) = 0$ et donc $z = u + 1$ et $y = u - 1$.

En reportant dans ((1)) on obtient $(u + 1)^{\sigma+1} = (u + 1)^2$, donc $(u + 1) \in \mathbb{F}_3$.

(a) Elimination de a.

Elle s'appuie sur la condition 3), sous la forme $t^{a\sigma} = t^{2-a}$ $(t \in K^{\times})$.

Soient $z \in E_\sigma$, y et u définis par (E_1) et (E_2); posons

$$X = (u - 1)^a \ , \ Y = u^a \ , \ Z = (u + 1)^a \ ;$$

ainsi XYZ est non nul et la relation (T) se met sous la forme

$$(T_1) \qquad a_1X + b_1Y + c_1Z + e_1XZ = 0$$

En transformant (T_1) par σ, σ^2 et σ^3, à l'aide des relations

$$X^\sigma = (u - 1)^2X^{-1}, \ Y^\sigma = u^2Y^{-1}, \ Z^\sigma = (u + 1)^2Z^{-1}$$

on obtient trois nouvelles équations

$$(T_2) \qquad b_2Y + d_2YZ + e_2XZ + f_2XY = 0$$

$$(T_3) \qquad a_3X + b_3Y + c_3Z + e_3XZ = 0$$

$$(T_4) \qquad b_4Y + d_4YZ + e_4XZ + f_4XY = 0$$

où

$a_1 = z$ $\qquad$ $c_1 = -y$

$a_3 = z^{\sigma^2}(u - 1)^{2\sigma-2}$ $\qquad$ $c_3 = - y^{\sigma^2}(u + 1)^{2\sigma-2}$

$b_1 = y - z - 1$ $\qquad$ $e_1 = 1$

$b_2 = (u^2 - 1)^2$ $\qquad$ $e_2 = (y - z - 1)^\sigma u^2$

$b_3 = (y - z - 1)^{\sigma^2} u^{2\sigma-2}$ $\qquad$ $e_3 = (u^2 - 1)^{2\sigma-2}$

$b_4 = (u^2 - 1)^{2\sigma^2-2\sigma+2}$ $\qquad$ $e_4 = (y - z - 1)^{\sigma^3} u^{2\sigma^2-2\sigma+2}$

$d_2 = z^\sigma(u - 1)^2$ $\qquad$ $f_2 = - y^\sigma(u + 1)^2$

$d_4 = z^{\sigma^3}(u - 1)^{2\sigma^2-2\sigma+2}$ $\qquad$ $f_4 = - y^{\sigma^3}(u + 1)^{2(\sigma^2-\sigma+1)}$

Les équations (T_j) multipliées successivement par X, Y et Z fournissent douze autres équations où apparaissent également X^2, Y^2, Z^2, XYZ, X^2Y, X^2Z, XY^2, Y^2Z, XZ^2, Z^2Y, soit au total 16 équations linéaires homogènes en 16

quantités non nulles. Le déterminant Δ de la matrice des coefficients - chacun peut l'écrire - est un polynôme en les a_i, b_i, c_i, d_i, e_i et f_i et est nul. On voit immédiatement apparaître deux facteurs, déterminants (2,2) (sur les lignes (T_1) et (T_3), colonnes X et Z et sur les lignes $Y(T_2)$ et $Y(T_4)$, colonnes XY^2 et Y^2Z). Le déterminant Δ_o (12,12) qui est ainsi factorisé a la particularité suivante : les 6 colonnes relatives aux variables Y, X^2, Y^2, Z^2, X^2Y et YZ^2 ne contiennent que deux termes non nuls, répartis au total sur les 12 lignes. Il en résulte (cf la proposition démontrée en appendice) que Δ_o est égal à un déterminant (6,6) dont chaque coefficient est lui-même un déterminant (2,2) extrait de Δ_o. Plus précisément, si nous posons

$$g_1 = b_2d_4 - b_4d_2 \qquad h_1 = b_1c_3 - b_3c_1$$
$$g_2 = b_2e_4 - b_4e_2 \qquad h_2 = c_1a_3 - c_3a_1$$
$$g_3 = b_2f_4 - b_4f_2 \qquad h_3 = a_1b_3 - a_3b_1$$
$$g_4 = f_2d_4 - f_4d_2 \qquad h_4 = b_1e_3 - b_3e_1$$
$$g_5 = f_2e_4 - f_4e_2 \qquad h_5 = a_1e_3 - a_3e_1$$
$$g_6 = d_2e_4 - d_4e_2 \qquad h_6 = c_1e_3 - c_3e_1$$

nous obtenons

$$\Delta = \pm\, h_2 g_4 \Delta_o$$

$$\Delta_o = \begin{vmatrix} g_1 & g_2 & g_3 & 0 & 0 & 0 \\ 0 & 0 & -g_3 & g_4 & g_5 & 0 \\ -g_1 & 0 & 0 & -g_4 & 0 & g_6 \\ 0 & -h_2 & h_3 & 0 & h_5 & 0 \\ h_1 & 0 & -h_3 & h_4 & 0 & 0 \\ -h_1 & h_2 & 0 & 0 & 0 & h_6 \end{vmatrix}$$

On voit que Δ_o est somme algébrique de 16 termes, chacun étant un produit $g_{f(1)}g_{f(2)}g_{f(3)}h_{f(4)}h_{f(5)}h_{f(6)}$, où f est une bijection de $\{1,2,3,4,5,6\}$ et $\{f(1),f(2),f(3)\}$ est différent de $\{1,2,6\}$, $\{1,3,4\}$, $\{2,3,5\}$ et $\{4,5,6\}$.

Il est donc relativement facile d'obtenir des informations simples sur Δ_o, comme polynôme en les z^{σ^i}, y^{σ^i} et u^{σ^i}.

(b) *Elimination de* y, y^{σ^2}, y^{σ^3}, u, u^{σ}, u^{σ^2}.

Considérons toute fonction des z^{σ^i}, y^{σ^i}, u^{σ^i} (y, z et u liés par (E_1) et (E_2)) comme une fonction de z. Si F et G sont deux fonctions de K dans K ou de E_σ dans K, nous dirons que F domine G si tout zéro de G dans E_σ est un zéro de F. Nous définissons ainsi un ordre partiel.

Lemme 3 Soit F définie par

$$F(z) = (u^2 - 1)^2 zy + (1 + zy + u(z + y))(y - z - 1)u^2$$

La fonction F domine $g_4h_2h_4h_5h_6$.

Ce lemme est démontré au paragraphe 3.

Puisque F domine h_2g_4, $F\Delta_o$ est nul sur E_σ. Posons, pour simplifier l'écriture

$$((3)) \qquad \begin{cases} z_i = z^{\sigma^i} & (i = 1, 2, 3, 4, 0) \\ \zeta_j = 1 + z_{j+1}z_j^2 & (j = 0, 1, 2) \end{cases}$$

On peut éliminer les

$$y^{\sigma^i} \quad (i > 0) \quad \text{et} \quad u^{\sigma^j} \quad (j \geqslant 0)$$

grâce aux relations suivantes, qui se déduisent de (E_1), (E_2) ou ((1)) et ((2))

$$((4)) \qquad \begin{cases} y^\sigma = \zeta_o y^{-2} \\ y^{\sigma^2} = \zeta_1\zeta_o^{-2}y^4 \\ y^{\sigma^3} = \zeta_2\zeta_1^{-2}\zeta_o^4 y^{-8} \\ y^{\sigma^4} = \zeta_3\zeta_2^{-2}\zeta_1^4\zeta_o^{-8}y^{16} \end{cases}$$

$$((5)) \qquad \begin{cases} u = z_1z_o - \zeta_o y^{-1} \\ u^\sigma = z_2z_1 - \zeta_1\zeta_o^{-1}y^2 \\ u^{\sigma^2} = z_3z_2 - \zeta_2\zeta_1^{-1}\zeta_o^2 y^{-4} \end{cases}$$

Après substitution, $F\Delta_o$ est une fonction rationnelle en z_i, y et, en utilisant le développement de Δ_o donné en (a), on peut en calculer le dénominateur. On constate ainsi que

$$y^{64}\zeta_1^{12}\zeta_o^{19}u^{6\sigma}(u^{2\sigma}-1)^4 F\Delta_o = P(z_o,z_1,z_2,z_3;y)$$

est polynômiale. Autrement dit, $P \in \mathbb{F}_3[Z_o,Z_1,Z_2,Z_3;T]$ et $P(z^{\sigma^i};y)$ est nul sur E_σ.

De même on constate que $z_o^{-1}y^3F$ est un polynôme en z_o, z_1, y; soit $G \in \mathbb{F}_3[Z_o,Z_1;T]$.

Lemme 4. G est irréductible.

Le lemme 4 est démontré au paragraphe 3 ([1]).

Le terme de plus haut degré en Z_3 de P se calcule facilement. Il est de degré 12 et son coefficient est issu de

$$S(z_o,z_1,z_2;y) = b_4^3 d_2 e_2 f_2 y^{64}\zeta_1^{12}\zeta_o^{19}u^{6\sigma}(u^{2\sigma}-1)^4 F.h_4h_5h_6$$

(compte-tenu de ((4)) et ((5))).

Des facteurs irréductibles de P, on ne conserve que les facteurs maximaux pour la relation de domination. Si deux facteurs irréductibles maximaux sont équivalents, c'est-à-dire s'ils ont mêmes zéros sur E_σ, on conserve un seul d'entre eux. On suppose également qu'au cas où G est maximal, G est conservé. Le produit P_1 des irréductibles ainsi choisis est évidemment nul sur E_σ.

(c) Elimination de y.

Pour éliminer y, transformons par σ l'égalité

$$P_1(z,z^\sigma,z^{\sigma^2},z^{\sigma^3};y) = 0$$

soit

$$P_1(z^\sigma,z^{\sigma^2},z^{\sigma^3},z^{\sigma^4};y^\sigma) = 0$$

Tenant compte de ((4)), on en déduit un polynôme $P_2 \in \mathbb{F}_3[Z_o,Z_1,\ldots,Z_4;T]$ défini par

$$P_2(Z_o,Z_1,Z_2,Z_3,Z_4;T) = T^{2\deg_T P_1} P_1(Z_1,Z_2,Z_3,Z_4;(1+Z_1Z_o^2)T^{-2})$$

et tel que $P_2(z^{\sigma^i};y)$ soit nul sur E_σ.

Lemme 5. Le résultant en T de P_2 et P_1 n'est pas nul.

En effet, si P_1 et P_2 ont un facteur irréductible commun Q, Q est

([1]) Dans [1], Bombieri affirme que y^3F est irréductible, alors que F s'annule si z_o est nul.

comme P_1 indépendant de Z_4. Donc Q divise le coefficient S_1 du terme de plus haut degré en Z_4 de P_2; S_1 lui-même divise $T^{2\deg_T P} S(Z_1,Z_2,Z_3;(1+Z_1Z_o^2)T^{-2})$. Il en résulte que si $S_1(z,z^\sigma,z^{\sigma^2},z^{\sigma^3};y)$ est nul en $z \in E_\sigma$, alors $S(z^\sigma,z^{\sigma^2},z^{\sigma^3};y^\sigma)$ est nul en z. Par conséquent $S(z,z^\sigma,z^{\sigma^2};y)$ domine $Q(z,z^\sigma,z^{\sigma^2},z^{\sigma^3};y)$. Or, selon le lemme 2, les seuls facteurs de S qui s'annulent éventuellement en un point de E_σ sont F, h_4, h_5 et h_6. Selon le lemme 3 et la définition de G, $G(z,z^\sigma;y)$ domine S. Finalement G domine Q, donc G est maximal et on peut supposer que G = Q. Ainsi G diviserait P_2.

Spécialisons en $Z_1 = 0$: $G(Z_o,0;T) = (T^2 - 1)(T^2 + T + 1 - Z_o)$ diviserait $P_2(Z_o,0,Z_2,Z_3,Z_4;T) = T^{\cdots}P_1(0,Z_2,Z_3,Z_4;T^{-2})$. Mais ceci est impossible car ce dernier polynôme, qui n'est pas nul, est indépendant de Z_o, alors que $G(Z_o,0;T)$ ne l'est pas.

Les polynômes P_1 et P_2 n'ont donc aucun facteur commun, leur résultant n'est pas nul.

Soit $H_o \in \mathbb{F}_3[Z_o,Z_1,Z_2,Z_3,Z_4]$ ce résultant.

La fonction $H_o(z,z^\sigma,z^{\sigma^2},z^{\sigma^3},z^{\sigma^4})$ est nulle sur E_σ. Pour démontrer l'assertion énoncée au début de ce paragraphe il suffit donc d'exhiber $H_1 \in \mathbb{F}_3[Z_j]$ tel que $H_1(z^{\sigma^i})$ soit nulle sur $(K - E_\sigma)$.

Soient donc y, z et u liés par (E_1) et (E_2); supposons d'abord $u = 0$. On a alors $y^2 = z^2$ (lemme 1 (b)), d'où, par (E_1), $z = 1$ et $y = -1$. D'autre part, on a toujours $(y^{\sigma+2})^{\sigma+1} = (y^{\sigma+1})^{\sigma+2}$, soit $(z^{\sigma+2} + 1)^{\sigma+1} = (z^{\sigma+1} - u)^{\sigma+2}$. On en déduit que si

$$H_1 = (Z_o^2 - 1) \prod_{\varepsilon = \pm 1} (\varepsilon Z_2Z_1^2Z_o - Z_2Z_1^2 + Z_2Z_1 - \varepsilon Z_1^2Z_o^2 - Z_1Z_o^2 - Z_1Z_o - 1 - \varepsilon)$$

alors $H_1(z,z^\sigma,z^{\sigma^2})$ est nul sur $(K - E_\sigma)$.

(2) Démonstration du théorème.

(a) $\sigma^\ell = 3^\lambda$.

Pour énoncer le lemme décisif introduisons une relation de préordre

sur $\mathbb{Z}[X]$, définie à l'aide de la norme $\left\|\sum_i a_i X^i\right\|_1 = \sum_i |a_i|$.

Soient L, M $\in \mathbb{Z}[X]$; on dira que

$$L \leqslant M \quad \text{si et seulement si} \quad (\deg L < \deg M \quad \text{ou} \quad (\deg L = \deg M \quad \text{et} \quad \|L\|_1 \leqslant \|M\|_1))$$

Nous utiliserons aussi la seconde norme $\left\|\sum_i a_i X^i\right\|_2 = \sup_i |a_i|$.

Lemme 6. Soient K un corps commutatif, d un entier et σ un endomorphisme de K. Soit L un élément minimal de

$$I = \{M \in \mathbb{Z}[X] / M \neq 0, \|M\|_2 \leqslant d \text{ et } M(\sigma) = 0\}.$$

Il existe $\varepsilon \in \{-1,1\}$, $\lambda \in \mathbb{N}$, $\ell \in \mathbb{N}$ tels que

$$L = \varepsilon(p^\lambda X^\ell - 1) \quad \text{ou} \quad L = \varepsilon(X^\ell - p^\lambda)$$

où p est la caractéristique de K.

(le lemme ne dit rien si I est vide)

Démonstration du lemme 6. Soit L minimal dans I et séparons les monômes de L selon le signe du coefficient :

$$L(X) = \sum_{\alpha \in A} a_\alpha X^\alpha - \sum_{\beta \in B} a_\beta X^\beta$$

où $(A \cap B)$ est vide et $0 < a_\alpha, a_\beta \leqslant d$ quels que soient α, β.

On peut supposer que A n'est pas vide (remplaçant éventuellement L par -L) et si tout coefficient de L est positif, on pose $B = \{0\}$ et $a_0 = 0$.

Quel que soit $z \in K$, on a par hypothèse

$$(z+1)^{\sum_{\alpha \in A} a_\alpha \sigma^\alpha} = (z+1)^{\sum_{\beta \in B} b_\beta \sigma^\beta},$$

soit

$$\sum_{(k_\alpha)_\alpha} \prod_{\alpha \in A} \binom{a_\alpha}{k_\alpha} z^{\sum_\alpha k_\alpha \sigma^\alpha} = \sum_{(l_\beta)_\beta} \prod_{\beta \in B} \binom{a_\beta}{l_\beta} z^{\sum_\beta l_\beta \sigma^\beta}$$

avec $0 \leqslant k_\alpha \leqslant a_\alpha$ si $\alpha \in A$ et $0 \leqslant l_\beta \leqslant a_\beta$ si $\beta \in B$.

Il y a une simplification pour $(k_\alpha)_\alpha = (a_\alpha)_\alpha$ et $(l_\beta)_\beta = (a_\beta)_\beta$ et, si $B \neq \{0\}$, une seconde simplification pour $k_\alpha = 0 = l_\beta$ quels que soient α et β.

Si l'un des coefficients restant $\binom{a_\alpha}{k_\alpha}$ ou $\binom{a_\beta}{l_\beta}$ n'est pas nul dans K, on obtient une relation de dépendance entre caractères de $K^\times$, donc deux de ces caractères coïncident. Or les polynômes $\sum_\alpha k_\sigma X^\alpha$ et $\sum_\beta k_\beta X^\beta$ sont deux à

deux distincts et les différences sont toutes de seconde norme inférieure ou égale à $||L||_2$, donc à d. Par contre, on a

$$|| \Sigma_\alpha k_\alpha X^\alpha - \Sigma_\alpha k'_\alpha X^\alpha ||_1 = \Sigma_\alpha |k_\alpha - k'_\alpha| \leqslant \Sigma_\alpha a_\alpha \leqslant ||L||_1$$

$$|| \Sigma_\beta l_\beta X^\beta - \Sigma_\beta l'_\beta X^\beta ||_1 = \Sigma_\beta |l_\beta - l'_\beta| \leqslant \Sigma_\beta a_\beta < ||L||_1$$

$$|| \Sigma_\alpha k_\alpha X^\alpha - \Sigma_\beta l_\beta X^\beta ||_1 = \Sigma_\alpha k_\alpha + \Sigma_\beta l_\beta < \Sigma_\alpha a_\alpha + \Sigma_\beta b_\beta = ||L||_1 .$$

En outre, une égalité des premières normes suppose que, dans le premier cas, B se réduise à $\{0\}$ et $\{k_\alpha, k'_\alpha\} = \{0, a_\alpha\}$ pour tout α dans A. Il existe alors une partition $A_1 \cup A_2$ de A telle que $(\Sigma_{\alpha \in A_1} a_\alpha X^\alpha - \Sigma_{\alpha \in A_2} a_\alpha X^\alpha) \in I$, d'où $2(\Sigma_{\alpha \in A_i} a_\alpha X^\alpha) \in I$, ceci pour i = 1, 2.

On voit donc que le choix de L interdit l'égalité entre deux de ces caractères. Il en résulte que $B \neq \{0\}$ et que A et B sont des singletons.

Si la caractéristique est nulle, $a_\alpha = a_\beta = 1$, et L est de la forme $X^m - X^n$. Mais tout endomorphisme de K étant injectif, le choix de L implique que L est de la forme $\pm(X^\ell - 1)$.

Si la caractéristique est p non nulle, a_α est une puissance de p, donc L(X) est de la forme $p^\mu X^m - p^\nu X^n$; mais $L(\sigma) = 0$ implique alors $p^{\mu-\nu}\sigma^{m-n} = 1$, et le choix de L suppose que L(X) est de la forme

$$L(X) = \pm(X^\ell - p^\lambda) \quad \text{ou} \quad L(X) = \pm(p^\lambda X^\ell - 1)$$

(λ et ℓ entiers positifs ou nuls).

Corollaire du lemme 6. Soient K un corps commutatif, σ un endomorphisme de K et $H \in \mathbb{F}_p[Z_o, Z_1, \ldots, Z_r]$, non nul, tel que $H(z^{\sigma^i}) = 0$ pour tout $z \in K$. Alors il existe $\ell \leqslant r$ tel que

i) si K est de caractéristique nulle, $\sigma^\ell = 1$,

ii) si K est de caractéristique non nulle p, il existe $\lambda \in \mathbb{N}$ et $\varepsilon \in \{-1,1\}$ tel que

$$\sigma^\ell = p^{\varepsilon\lambda} \quad \text{et} \quad p^\lambda \leqslant \sup_j \deg_{Z_j} H .$$

Démonstration.

Soit $a \Pi_i Z_i^{\alpha_i}$ un monome de H. On a $a \Pi_i (z^\sigma)^{\alpha_i} = az^{L(\sigma)}$, où $L(X) = \Sigma_i \alpha_i X^i$. La relation $H(z^{\sigma^i}) = 0$ est donc une relation de

dépendance linéaire entre des fonctions multiplicatives de K^x dans K^x, c'est-à-dire entre caractères de K^x. Des caractères distincts étant linéairement indépendants, il existe deux polynômes L_1, $L_2 \in \mathbb{Z}[X]$, à coefficients positifs tels que $L_1(\sigma) = L_2(\sigma)$, soit $(L_1 - L_2)(\sigma) = 0$. Or il est clair que

$$\|L_1 - L_2\|_2 \leqslant \sup_i \deg_{Z_i} H \ .$$

L'idéal I défini dans le lemme 6 avec $d = \sup_i \deg_{Z_i} H$ est non vide et un élément minimal de I fournit l'une des relations annoncées dans le corollaire.

Remarque: Le lemme 6 n'est pas sans rapport avec un théorème d'Artin (cité par S. Lang in "Algebra", CH.VIII, §11 - Addison-Wesley 1965) selon lequel si des homomorphismes additif d'un groupe additif A (ici les puissances de $\mathfrak{F}$: $(K,+) \longrightarrow (K,+)$) dans un corps K sont algébriquement indépendants, il existe une relation de dépendance écrite à l'aide d'un polynôme additif.

(b) De $\sigma^{\ell} = 3^{\pm\lambda}$ à $\sigma^2 = 3$.

Soit H un polynôme satisfaisant à l'assertion démontrée au paragraphe 1 : on a donc $H(z,z^{\sigma},z^{\sigma^2},z^{\sigma^3},z^{\sigma^4}) = 0$ pour tout $z \in K$. Soit d un entier tel que $\sup_i \deg_{Z_i} H \leqslant 3^d$ (3^d joue le rôle de d en (a)). Selon le corollaire du lemme 6, il existe $(\ell,\lambda) \in \mathbb{N}^2$ tels que ((6)) $\ell \leqslant 4$, $\lambda \leqslant d$, $\sigma^{\ell} = 3^{\lambda}$ ou $\sigma^{\ell} 3^{\lambda} = 1$, soit $\sigma^{\ell} = 3^{\varepsilon\lambda}$. et on peut supposer ℓ minimal tel que ((6)).

Si λ est nul, comme $\mathbb{F}_3$ est le corps des points fixes de σ, K est fini d'ordre au plus égal à 3^4. On peut donc supposer $\lambda \geqslant 1$.

L'égalité ((6)) appliquée à y fournit, par l'intermédiaire de ((3)) et ((4)) un nouveau polynôme $V \in \mathbb{F}_3[Z_o,Z_1,Z_2,Z_3;T]$ tel que,

si $z \in E_{\sigma}$, $V(z^{\sigma^i};y) = 0$

Le polynôme V ainsi obtenu est de la forme $AT^{\alpha} + B$, où $A, B \in \mathbb{F}_3[Z_j]$. Plus précisément, on peut supposer que, selon les valeurs de ℓ, λ, ε, α, $A(z_j)$ et $B(z_j)$ sont (en tenant compte de ((3)))

(ℓ,ε) =	$(4,+)$, $\lambda > 2$	$(4,+)$, $\lambda \leqslant 2$	$(4,-)$	$(3,+)$
A =	$\zeta_2^2\zeta_o^8$.	$(1+z_o^{3^\lambda} z_3^2)\zeta_1^4$	$(1+z_o z_3^{2.3^\lambda})\zeta_1^{4.3^\lambda}$	ζ_1^2
α =	$3^\lambda - 16$	$16 - 3^\lambda$	$16.3^\lambda - 1$	$3^\lambda + 8$
B =	$(1+z_o^{3^\lambda} z_3^2)\zeta_1^4$	$\zeta_2^2\zeta_o^8$	$\zeta^{2.3^\lambda}\zeta_o^{8.3^\lambda}$	$(1+z_o^{3^\lambda} z_2^2)\zeta_o^4$

...	$(3,-)$	$(2,+)$, $\lambda > 1$	$(2,+)$, $\lambda = 1$	$(2,-)$
...	$\zeta_1^{2.3^\lambda}$	ζ_o^2	$1+z_o^3 z_1^2$	$1+z_o z_1^{2.3^\lambda}$
	$8.3^\lambda + 1$	$3^\lambda - 4$	1	$4.3^\lambda - 1$
...	$(1+z_o z_2^{2.3^\lambda})\zeta_o^{4.3^\lambda}$	$(1+z_o^{3^\lambda} z_1^2)$	ζ_o^2	$\zeta_o^{2.3^\lambda}$

...	$(1,+)$	$(1,-)$
...	1	1
...	$3^\lambda + 2$	$2.3^\lambda + 1$
...	$1+z_o^{3^\lambda+2}$	$1+z_o^{2.3^\lambda+1}$

Lemme 7. V est irréductible.

En effet, les diviseurs premiers de A et B sont les ζ_i et un polynôme issu de $\zeta_{\ell-1}$, à savoir

$$S = 1 + z_o^{3^\lambda} z_{\ell-1}^2 \quad \text{si} \quad \varepsilon = 1 \quad \text{ou} \quad S = 1 + z_o z_{\ell-1}^{2.3^\lambda} \quad \text{si} \quad \varepsilon = -1.$$

On voit donc que A et B sont premiers entre eux. En outre S divise AB, mais S^2 ne divise pas AB. Selon le critère d'Eisenstein, V n'admet aucun diviseur en T de degré différent de 0 ou α. Au total V est irréductible dans $\mathbb{F}_3[Z_i;T]$.

Les relations ((6)) permettent également de transformer l'égalité

$$P(z^{\sigma^i};y) = 0 .$$

Si $\varepsilon = 1$, il suffit de substituer 3^λ à σ^ℓ autant que possible. Si $\varepsilon = -1$, on considère $P(z^{\sigma^i};y)^{3^\lambda} = P(z^{\sigma^i 3^\lambda};y^{3^\lambda}) = 0$ quand $\ell > 1$ et $P(z^{\sigma^i};y)^{3^{3\lambda}} = 0$ quand $\ell = 1$.

On obtient ainsi un polynôme $U \in \mathbb{F}_3[Z_o, \ldots, Z_{\ell-1}; T]$ tel que

$$U(z^{\sigma^i}; y) = 0 \quad \text{sur } E_\sigma .$$

Lemme 8. Soient ℓ, ε et λ comme en ((6)). Le polynôme V ne divise pas U sauf si $(\ell, \varepsilon\lambda) = (2,1)$.

Une démonstration - très longue - de ce lemme est donnée au paragraphe (3).

Puisque V ne divise pas U et est irréductible, le résultant en T de U et V n'est pas nul. Il s'agit d'un polynôme en Z_j $(j \leqslant \ell-1)$, soit $Q_o \in \mathbb{F}_3[Z_j]$ tel que $Q_o(z^{\sigma^j}) = 0$ sur E_σ.

On a exhibé au paragraphe 1, $H_1 \in \mathbb{F}_3[Z_o, Z_1, Z_2]$, non nul et tel que $H_1(z, z^\sigma, z^{\sigma^2})$ soit nul sur $(K - E_\sigma)$; on ne déduit par ((6)) un polynôme non nul $Q_1 \in \mathbb{F}_3[Z_o, \ldots Z_{\ell-1}]$ tel que $Q_1(z^{\sigma^j})$ soit nul sur $(K - E_\sigma)$. On obtient ainsi un polynôme non nul $Q_{(\ell,\varepsilon,\lambda)} = Q_o Q_1$ tel que $Q_{(\ell,\varepsilon,\lambda)}(z^{\sigma^j})$ soit nul sur tout K.

Si $\ell = 1$, on a $Q_{(1,\varepsilon,\lambda)}(z) = 0$ pour tout $z \in K$, donc K est un corps fini dont le cardinal est majoré par le degré de Q. Comme λ est majoré, le cardinal de K est majoré.

Si $\ell > 1$ et $(\ell, \varepsilon\lambda) \neq (2,1)$, le corollaire du lemme 6 montre qu'il existe une autre relation

((7)) $$\sigma^m = 3^{\delta\mu} \quad \text{où} \quad \delta \in \{-1,1\}, \quad 3^\mu \leqslant \sup_j \deg_{Z_j} Q_{(\ell,\varepsilon,\lambda)} , \quad m \leqslant \ell-1 .$$

Il existe $M(\ell,\varepsilon,\lambda)$ tel que $\mu \leqslant M(\ell,\varepsilon,\lambda)$.

Des relations ((6)) et ((7)) on déduit

$$3^{\delta\mu\ell} = 3^{\varepsilon\lambda m} \quad \text{soit} \quad 3^{\delta\mu\ell - \varepsilon\lambda m} = 1 .$$

Donc K est un corps fini dont le cardinal q^n est majoré; on a en effet $n \leqslant M(\ell,\varepsilon,\lambda)\ell + \lambda(\ell - 1)$.

Le théorème est démontré.

(3) Démonstrations des lemmes 3, 4 et 8.

(a) Démonstration du lemme 3.

On voit que $g_4 = (u^2 - 1)^2 h_2^\sigma$ et que $h_2 = yz(y^{\sigma^2-1}(u + 1)^{2(\sigma-1)} - z^{\sigma^2-1}(u - 1)^{2(\sigma-1)})$. Si h_2 est nul, $y^{\sigma+1}(u + 1)^2$ et $z^{\sigma+1}(u - 1)^2$ ont même image par $(\sigma-1)$, d'où l'on déduit

que $y^{\sigma+1}(u+1)^2 = \pm z^{\sigma+1}(u-1)^2$. Mais l'image de $(\sigma+1)$ contient les carrés et non (-1) (lemme 1); par ((1)) et ((2)), il en résulte donc

((9)) $\qquad z(u+1)^2 - y(u-1)^2 + 1 = 0$

On a $h_5 = z(u-1)^{2(\sigma-1)}((u+1)^{2(\sigma-1)} - z^{\sigma^2-1})$, donc h_5 est nul si et seulement si $z^{\sigma+1} = (u+1)^2$, égalité qui, par ((1)) équivaut à ((9)).

On a encore $h_6 = y(u+1)^{2(\sigma-1)}(y^{\sigma^2-1} - (u-1)^{2(\sigma-1)})$, donc h_6 est nul si et seulement si $y^{\sigma+1} = (u-1)^2$, égalité qui, par ((2)), équivaut à ((9)).

Enfin $h_4 = (y-z-1)((u^2-1)^{2(\sigma-1)} - (y-z-1)^{\sigma^2-1}u^{2(\sigma-1)})$, donc h_4 est nul si et seulement si $(y-z-1)^{\sigma+1}u^2 = (u^2-1)^2$, égalité qui, par ((1)) et ((2)), équivaut à $F = 0$.

Mais F domine le premier membre de ((9)). En effet si ((9)) est vraie, on a $h_2 = h_5 = h_6 = 0$ et en particulier $z^{\sigma+1} = (u+1)^2$ et $y^{\sigma+1} = (u-1)^2$, d'où $z = \pm (u+1)^a = \varepsilon(u+1)^a$ et aussi $y = \pm (u-1)^a = \eta(u-1)^a$. Selon la relation (T) on a alors $(u^2-1)^a(\varepsilon - \eta + 1) = (z - y + 1)u^a$, d'où, en appliquant $(\sigma+1)$, $(u^2-1)^2 = (z-y+1)^{\sigma+1}u^2$ et cette dernière égalité équivaut à $F = 0$.

(b) Démonstration du lemme 4.

Après substitution selon les égalités ((3)), ((4)) et ((5)), on obtient $y^3F = z_o G(z_o, z_1, y)$, où $G \in \mathbb{F}_3[Z_o, Z_1, T]$, G est de degré 4 en Z_1. Posons $G = a_4 Z_1^4 + a_3 Z_1^3 + a_2 Z_1^2 + a_1 Z_1 + a_o$ et $W = T - Z_o$. On a

$$a_4 = Z_o^4 W^4$$
$$a_3 = Z_o^2 W^4 (Z_o + T - 1)$$
$$a_2 = Z_o W^2 T(- Z_o^2 T + Z_o T^2 - Z_o + T - 1)$$
$$a_1 = W(- Z_o^2 T^2 + Z_o T^3 - Z_o T - Z_o + T^2 - T)$$
$$a_o = - Z_o(T^2 - 1) + (T-1)^3(T+1).$$

Il est clair que a_4 et a_o sont premiers entre eux, donc G n'admet pas de diviseur non scalaire de degré 0 en Z_1. La spécialisation de G en $T = 0$ admet la décomposition $(G)_{T=0} = (Z_o^2 Z_1 + Z_o - 1)(Z_o^2 Z_1 + 1)^3$.

Supposons que G admette dans $\mathbb{F}_3[Z_o,Z_1,T]$ un diviseur de degré 1 en Z_1, soit $A_1Z_1 - A_o$. La spécialisation en $(T = 0)$ de A_1 est, d'après la décomposition précédente un multiple de Z_o^2. Or l'étude des valuations en W montre que A_1 est divisible par W, non par W^2. On peut donc supposer $A_1 = Z_oW$. La spécialisation de G en $(Z_o = 0)$ admet à un scalaire multiplicatif près une seule décomposition propre $(G)_{Z_o=0} = (T - 1)(T^2Z_1 + (T + 1)(T - 1)^2)$. Comme A_1 spécialise en 0, la spécialisation de A_o doit diviser $(T - 1)$. La décomposition en irréductibles de a_o est $a_o = (T - 1)(T + 1)((T - 1)^2 - Z_o)$. Donc A_o est de degré au plus 1 en T. Supposons que $(T - 1)$ divise A_o. En $(T,Z_o) = (1,-1)$, G devient $(Z_1^4 - Z_1^3 - Z_1^2)$, et la décomposition supposée de G devient donc $G = (-Z_1)(-Z_1^3 + Z_1^2 + Z_1)$. Or (a_o/A_o) n'est pas nul en ce point. Cette contradiction montre que A_o ne peut être qu'un scalaire. On obtient alors facilement une contradiction (en $Z_o = 1$ par exemple).

Supposons donc maintenant que G admette une décomposition en un produit de deux polynômes de degré 2 en Z_1: $G = (A_2Z_1^2 + A_1Z_1 + A_o)(B_2Z_1^2 + B_1Z_1 + B_o)$. On montre sans difficulté que W^2 divise A_2 et B_2. Selon la spécialisation de G en $(T = 0)$, on peut supposer que $A_2 = Z_o^2W^2 = B_2$. On sait aussi que W divise A_1 et B_1, et que Z_o divise A_1 ou B_1. On constate alors une contradiction en spécialisant en $(Z_o + T - 1 = 0)$, où a_3 est nul.

(c) Démonstration du lemme 8

Supposons que V divise U.

(i) Si $\ell \geqslant 3$.

Spécialisons en $Z_o = 0$ et $Z_3 = 0$. Si on remplace formellement z et z^{σ^3} par 0 dans Δ_o, on voit que a_1 et d_4 s'annulent, donc a_3 apparaît en facteur dans h_2, h_3, h_5 et d_2 apparaît en facteur dans g_1, g_4, g_6; ainsi Δ_o devient $d_2a_3\Lambda = z_1z_2(u^\sigma - 1)^2\Lambda$, où Λ est un déterminant (6,6) déduit de Δ_o. Ainsi $V(0,Z_1,Z_2,0;T)$ divise le polynôme R_2 issu de $y^{61}\zeta_1^{12}u^{6\sigma}(u^{2\sigma} - 1)^6z_1z_2\Lambda$ (ou de sa puissance 3^λ si $\ell = 3$ et $\varepsilon = -1$). Or ni Z_1 ni Z_2 ne divise $V(0,Z_1,Z_2,0;T)$; donc $V(0,0,0,0;T)$ divise

$(R_2/Z_1Z_2)_{Z_1=0=Z_2}$. En $z_j = 0$, Λ est aisément calculable, puisque a_3 et d_2 s'annulent. On a

$$\Lambda' = \begin{vmatrix} 0 & g'_2 & g'_3 & 0 & 0 & 0 \\ 0 & 0 & -g'_3 & 0 & g'_5 & 0 \\ b'_4 & 0 & 0 & f'_4 & 0 & e'_4 \\ 0 & -c'_1 & -b'_1 & 0 & -e'_1 & 0 \\ h'_1 & 0 & 0 & h'_4 & 0 & 0 \\ -h'_1 & 0 & 0 & 0 & 0 & h'_6 \end{vmatrix}$$

qui factorise en un produit de deux déterminants (3,3), soit

$$\Lambda' = (g'_2g'_3e'_1 - g'_3g'_5c'_1 + g'_2g'_5b'_1)(h'_4h'_6b'_4 + h'_1h'_4e'_4 - h'_1h'_6f'_4)$$

Il s'agit évidemment d'un polynôme en y ; on a

$b'_1 = y - 1$ $\quad c'_1 = - y$ $\quad e'_1 = 1$

$b'_2 = y^{-4}(y^2 - 1)^2$ $\quad f'_2 = - y^{-4}(y - 1)^2$ $\quad e'_2 = - y^{-4}(y^2 - 1)$

$b'_3 = y^6(y^4 - 1)$ $\quad c'_3 = - y^6(y + 1)^2$ $\quad e'_3 = y^4(y^2 + 1)^2$

$b'_4 = y^{-20}(y^2 - 1)^2(y^4 + 1)^2$ $\quad f'_4 = - y^{-18}(y - 1)^2(y^2 + 1)^2$ $\quad e'_4 = - y^{-22}(y^8 - 1)$

$g'_2 = y^{-26}(y^2 - 1)^6(y^4 + 1)$ $\quad h'_1 = y^6(y - 1)^4(y + 1)$

$g'_3 = y^{-24}(y - 1)^8(y + 1)^6$ $\quad h'_4 = - y^4(y - 1)^4(y^2 + 1)$

$g'_5 = - y^{-26}(y - 1)^6(y + 1)^4(y^2 + 1)$ $\quad h'_6 = - y^5(y - 1)^4$

On en déduit que

$$\Lambda' = - y^{-64}(y - 1)^{22}(y + 1)^{11}(y^2 + 1)P_1P_2$$

où $\quad P_1 = y^9 + y^8 - y^7 - y^5 - y^4 + y^2 - 1$

et $\quad P_2 = y^{11} - y^9 - y^8 + y^7 + y^4 - y^3 + y^2 + 1$

D'autre part, ζ_1 se spécialise en 1 et u^σ en $(- y^2)$.

Enfin $V(0,0,0,0;y)$ est l'un des polynômes (selon ℓ et λ)

$y^{3^\lambda - 16} - 1$; $y^{16-3^\lambda} - 1$; $y^{16.3^\lambda - 1} - 1$; $y^{3^\lambda + 8} - 1$; $y^{8.3^\lambda + 1} - 1$.

tous divisibles par $(y - 1)$, mais non par $(y - 1)^2$, ni $(y + 1)$ ou $(y^2 + 1)$

et par un travail de routine on voit que V ne divise pas $(y - 1)P_1P_2$.

(ii) Si $\ell = 2$.

Démonstration analogue au cas précédent.

Dans ce cas z_o divise a_3 ou $a_3^{3^\lambda}$ et z_1 divise d_4 ou $d_4^{3^\lambda}$ (selon la valeur de ε). Le facteur z_o apparaît dans les termes h_2, h_3 et h_5; le facteur z_1 dans les termes g_1, g_4 et g_6. Comme z_oz_1 ne divise pas V, on peut considérer $(y^{61}u^{6\sigma}(u^{2\sigma} - 1)^4(u - 1)^2\Lambda/z_oz_1)_{z_o = 0 = z_1}$ et sa divisibilité par V(0,0;y), comme polynôme en y (si par exemple $\varepsilon = 1$)

La spécialisation en $z_o = 0 = z_1$ annule (a_3/z_o) et (d_4/z_1) et Δ devient, au facteur $(u - 1)^2$ près, un déterminant (6,6) qui factorise en deux déterminants (3,3) :

$$\begin{vmatrix} -b'_4 & -f'_4 & e'_4 \\ h'_1 & h'_4 & 0 \\ h'_1 & 0 & h'_6 \end{vmatrix} = y^{-12}(y - 1)^9(y + 1)(y^2 + 1)(-P_2)$$

(rencontré en (i))

et $$\begin{vmatrix} g'_2 & g'_3 & 0 \\ 0 & -g'_3 & g'_5 \\ c'_3 & b'_3 & e'_3 \end{vmatrix} = g'_3g'_5c'_3 - g'_2g'_5b'_3 - g'_2g'_3e'_3$$

$$= y^{-46}(y - 1)^{13}(y + 1)^{11}(y^2 + 1)(- y^8 + y^6 - y^4 - 1)$$

Enfin V(0,0;y) est le polynôme

$$y^{3^\lambda - 4} - 1$$

qui ne divise pas le produit précédent si $\lambda \geqslant 2$.

(Si $\ell = 2$ et $\varepsilon = 1$, $V(0,0;y) = y - 1$)

Si ε est égal à (-1), dans $(\Lambda^{3^\lambda}/z_oz_1)_{z_o = 0 = z_1}$, les termes $a_1^{3^\lambda}/z_o$ et $d_4^{3^\lambda}/z_1$ s'annulent; au facteur

$$(u - 1)^2 = (a_3d_4)^{3^\lambda}/z_oz_1$$

près, on obtient encore un produit de deux déterminants (3,3), à savoir un déterminant déjà calculé en (i)

$$\begin{vmatrix} g'_2 & g'_3 & 0 \\ 0 & -g'_3 & g'_5 \\ -c'_1 & -b'_1 & -e'_1 \end{vmatrix} = y^{-52}(y-1)^{13}(y+1)^{10}P_1$$

et
$$\begin{vmatrix} -b'_2 & -f'_2 & -e'_2 \\ h'_1 & h'_4 & 0 \\ -h'_1 & 0 & h'_6 \end{vmatrix} = -h'_4h'_6b'_2 - h'_1h'_4e'_2 + h'_1h'_6f'_2$$

$$= y^5(y-1)^9(y+1)(y^4+y^2-y+1)$$

Comme $V(0,0;y)$ est

$y^{4.3^{\lambda}-1} - 1$

on conclut sans peine que V ne divise pas U dans ces hypothèses.

(iii) Si $\ell = 1$.

Si $\varepsilon = 1$, on a

$$V(z_o;y) = y^{3^{\lambda}+2} - z_o^{3^{\lambda}+2} - 1$$

et
$$U(z_o;y) = P(z_o, z^{3^{\lambda}}, z^{3^{2\lambda}}, z^{3^{3\lambda}}; y) .$$

Si V divise U, le terme de plus haut degré de V divise le composant homogène de plus haut degré de U. Gardons les variables z_o et y. On voit facilement que parmi les g_i, écrits comme polynômes en z_o et y, g_1, g_2 et g_3 sont de plus haut degré (par leur terme en b_4); de même, parmi les h_j, h_4, h_5 et h_6 sont de plus haut degré (par leur terme en e_3). Le terme homogène de plus haut degré de $U(z_o;y)$ est donc issu de

$$a_1b_1c_1d_2e_2f_2e_3^3b_4^3y^{64}\zeta_1^{12}\zeta_o^{19}u^{6\sigma}(u^{2\sigma}-1)^4F$$

et dans chacun de ces facteurs le terme de plus haut degré est de la forme $y^{\alpha}z_o^{\beta}(y-z_o)^{\gamma}$; leur produit n'est pas un multiple de $(y^{3^{\lambda}+2} - z_o^{3^{\lambda}+2})$

Si $\varepsilon = -1$, on a

$$V(z_o;y) = y^{2.3^{\lambda}+1} - z_o^{2.3^{\lambda}+1} - 1$$

et
$$U(z_o;y) = P(z_o^{3^{3\lambda}}, z_o^{3^{2\lambda}}, z_o^{3^{\lambda}}, z_o; y^{3^{3\lambda}})$$

Cette fois-ci, g_1, g_2 et g_3 sont de plus haut degré par leur terme

en b_2 et h_4, h_5 et h_6 par leur terme en e_1 et les considérations faites pour $\varepsilon = 1$ restent valables.

(4) Précisions.

Par une vérification sur ordinateur on peut montrer que, sous les hypothèses du théorème, σ est une racine carrée du Frobenius sans aucune exception (en appendice de [1] , "The numerical verification of Thompson's identity", par Andrew Odlyzko). Il convient pour celà de limiter au maximum le nombre des couples (K,σ) qui échappent à la démonstration précédente.

Pour appliquer le corollaire du lemme 6 (cf (2)(a)), il faut évaluer $\sup_j \deg_{Z_j} H$. On a

$$\deg_{Z_o} P_1 \leqslant \deg_{Z_o} P \leqslant 119 \qquad \deg_{Z_o} P_2 \leqslant 212$$

$$\deg_{Z_1} P_1 \leqslant \deg_{Z_1} P \leqslant 73 \qquad \deg_{Z_1} P_2 \leqslant 225$$

$$\deg_{Z_2} P_1 \leqslant \deg_{Z_2} P \leqslant 38 \qquad \deg_{Z_2} P_2 \leqslant 73$$

$$\deg_{Z_3} P_1 \leqslant \deg_{Z_3} P \leqslant 12 \qquad \deg_{Z_3} P_2 \leqslant 38$$

$$\deg_{T} P \leqslant \deg_{T} P \leqslant 106 \qquad \deg_{Z_4} P_2 \leqslant 12$$

$$\deg_{T} P_2 \leqslant 212$$

d'où il résulte

$$\deg_{Z_j} H_o \leqslant 119.212 + 106.212 = 47\ 700 ,$$

soit

$$\sup_j \deg_{Z_j} H \leqslant 47\ 706 < 3^{10}$$

On obtient donc en (a)

$$\sigma^{\ell} = 3^{\varepsilon\lambda} \quad \text{avec} \quad 1 \leqslant \ell \leqslant 4 \quad \text{et} \quad 0 \leqslant \lambda \leqslant 9 .$$

Le corps K est donc extension de degré fini du corps $\mathbb{F}_3$ des points fixes de σ. Comme (-1) n'est pas un carré, l'extension est de degré impair, et σ est d'ordre impair. On peut donc supposer que ℓ et λ ne sont pas tous deux pairs; en particulier la relation "$\sigma^4 = 1$" est exclue. Il est clair que si $\mathbb{F}_q$ fournit un contre-exemple à l'assertion "$\sigma^2 = 3$", il en est de même de l'un

au moins des sous-corps dont $\mathbb{F}_q$ est éventuellement composé. On peut donc supposer que le degré N de K sur $\mathbb{F}_3$ est puissance d'un nombre premier.

Il est possible d'évaluer les degrés des polynômes Q_o et Q (introduits en (2)(b)) en fonction de $(\ell,\varepsilon,\lambda)$. On peut montrer que

$$\sup_j \deg_{Z_j} Q_{(\ell,\varepsilon,\lambda)} < 3^{\nu(\ell,\varepsilon,\lambda)+1} \quad \text{(donc } \mu \leqslant \nu \text{ dans ((7)))}$$

avec

ℓ =	4	4	4	3	3	3	2	2	1	1	1
ε =	1	1	-1	1	1	-1	1	-1	1	1	-1
λ	$\geqslant 3$	1		$\geqslant 3$	1,2		$\geqslant 3$		$\geqslant 2$	1	
ν =	$\lambda+4$	7	$\lambda+6$	$2\lambda+2$	7	$2\lambda+6$	$2\lambda+3$	$2\lambda+6$	$4\lambda+2$	7	$4\lambda+5$

Pour (K,σ) exceptionnels, on considère un couple (ℓ,λ) tel que $\sigma^\ell = 3^{\varepsilon\lambda}$ et $1 \leqslant \lambda \leqslant 9$, ℓ étant minimal pour cette propriété.

Si $\ell = 1$, les valeurs de ν correspondantes majorent le degré de K sur $\mathbb{F}_3$.

Si $\ell \geqslant 2$, de ((6)) et ((7)) on déduit

$$\delta\mu\ell - \varepsilon\lambda m \equiv 0 \pmod{N} .$$

Supposons $\delta\mu\ell = \varepsilon\lambda m$. Si ℓ est égal à 4, λ est impair et 4 divise m, ce qui est exclus car $m < \ell$. Si ℓ est 3, m n'est pas 2 (car si $m = 2$, μ est impair) donc m est 1 et par conséquent $\lambda = 3\mu$, ce qui contredit le choix de (ℓ,λ). Si ℓ est 2, m est 1 et λ est pair, ce qui est exclu par choix de (ℓ,λ). On en conclut finalement que $(\delta\mu\ell - \varepsilon\lambda m)$ n'est pas nul, tout en étant divisible par N. Tenant compte des majorations de λ par 9 et μ par ν, on obtient ainsi une liste de 178 couples (N,σ) (où $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^N})$ pour lesquels il reste à vérifier que la condition de THompson n'est pas satisfaite. Cette liste est donnée dans [1].

8. SI $\sigma^2 = 3$, G EST ISOMORPHE A ${}^2G_2(q)$

On reprend ici la démonstration de Thompson ([28],III). C'est un théorème d'unicité qu'il s'agit de démontrer. Le corps K, supposé fini, est extension de degré impair de $\mathbb{F}_3$, l'égalité "$\sigma^2 = 3$" détermine σ; le groupe noté B aux chapitres 4, 5, 6 est donc déterminé à isomorphisme près. Le groupe G est extension transitive de B, opérant sur l'ensemble Ω des classes modulo B dans G. Comme U est régulier sur les classes autres que B, on identifie (Ω - {B}) à U; on dira donc que $g \in G$ transforme $u \in U$ en $u' \in U$ si et seulement si $gusB = u'sB$, où s est une certaine involution qui inverse tout élément de H. Le groupe G étant engendré par B et s, l'unicité de G résulte de l'unicité de l'opération de s sur Ω, donc finalement de l'unicité de ω (application définie au paragraphe (2) du chapitre 6).

On utilise essentiellement les formules ((16)) à ((21)) du chapitre 6 et l'isomorphisme ϕ exhibé en ce même chapitre. Dans ces formules on a

$$a = \sigma - 1 .$$

(1) d est nul.

L'élément d de K, introduit en 6.(1)(b) intervient dans l'expression de α_1, donc de $\alpha(x)$ (formule 19 du chapitre 6). Il intervient donc dans la formule 21 par les premières composantes, soit

$$y^{\sigma+2}\alpha(-u) = 1 - d + z^{\sigma+2}\alpha(u) - z^{\sigma+1}\beta(u) + z^{\sigma}\gamma(u)^{\sigma} + z\gamma(u) + z^2\gamma(u)^2 ,$$

(où y, z et u satisfont aux hypothèses de la formule 21) .

Cette égalité est linéaire en d, et se réduirait ([28],III) à A.d = 0,

$$A = z^{\sigma+2}(1 - (1 - u^{-1})^{\sigma+1}) - y^{\sigma+2}(1 - (1 + u^{-1})^{\sigma+1}) + 1 - (u - u^{-1})^{\sigma+1} \quad (1)$$

Le coefficient de d peut s'exprimer comme une fraction rationnelle en z et z^{σ}, car on a $(2 - \sigma)(2 + \sigma) = 1$, d'où

$$y^{\sigma+2} - z^{\sigma+2} = 1 \quad \text{implique} \quad y = (z^{\sigma+2} + 1)^2 (z^{2\sigma+3} + 1)^{-1}$$

et $$z^{\sigma+1} - y^{\sigma+1} = u \quad \text{implique} \quad u = (z^{\sigma+1} - 1)(z^{\sigma+2} + 1)^{-1}.$$

(1) la formule donnant A dans [28],III, ligne 7 de la page 163 est erronée.

degrés partiels 8 en z^{σ} et 14 en z. Si ce polynôme est nul sur $(K - \mathbb{F}_3)$, selon le corollaire du lemme 6 (chapitre 7), il existe m, entier positif au plus égal à 2 tel que $\sigma = 3^{\pm m}$, d'où $3^{2m-1} = 1$, et K est de cardinal au plus 27. Il reste à se convaincre que sur $\mathbb{F}_{27}$, le polynôme en question n'est pas nul sur E_σ. On en conclut que le coefficient de d n'est pas nul sur E_σ, donc que d est nul.

(2) Les orbites selon $C_G(t)$ *dans* Ω.

Il est clair que l'ensemble des points fixes de t sur Ω est

$$\Omega_o = P \cup \{B\}$$

et que Ω_o est une orbite selon $C_G(t)$ (celà se voit dans $C_G(t)$ lui-même).

Le groupe $C_G(t)$ opère régulièrement sur ses autres orbites. En effet, si un point u est fixe par un élément non trivial de $C_G(t)$, c'est que l'intersection de $B' = usBsu^{-1}$ avec $C_G(t)$ n'est pas $\{1\}$. Modulo l'action de $C_G(t)$ par automorphismes intérieurs, on peut supposer que $B' \cap PH \neq \{1\}$. Si $B' \cap P \neq \{1\}$, $B' = B$. Sinon on peut supposer (par conjugaison selon P) que $B' \cap H \neq \{1\}$, donc B' est fixe par un élément non trivial de H, donc aussi par t. En conclusion $B' \in \Omega_o$.

En regardant dans $\phi(G_1)$, on voit que

$$s\eta^5\mu s = \eta^5\mu st\eta .$$

Donc $\eta^5\mu$ est fixe par s (c'est-à-dire par ω). De la formule 7 du chapitre 6 on déduit

$$\mu^{-1}s\eta^2 s = \eta^3 s\mu^{-1}\eta^{-3}t \quad \text{donc} \quad (\mu^{-1}s\mu^{-1})(\mu\eta^2)s \in \eta^3 sB .$$

Comme $\mu\eta^2 = \eta^5\mu$, η^3 est dans l'orbite de $\eta^5\mu$ selon $C_G(t)$.

Puisque d est nul, les formules 16 à 19 du chapitre 6 montrent que $\omega(u(x)) = f(x)$ est déterminé pour $x \neq 0$. On a avec les mêmes notations

$$u(0) = (1, 0, 0) = \eta^3$$

et $\omega(\eta^3)$ est lisible dans $\phi(G_1)$: on a $s\eta^3 s = \mu^2\eta^2 s\mu\eta^8$, soit

$$f(0) = \omega(u(0)) = \mu^2\eta^2 \quad \text{et} \quad g(0) = \mu\eta^8 .$$

La formule 20 du chapitre 6 montre que ω est déterminé sur l'ensemble $\Delta = \{(x,y,0) / x \neq 0\} = ([U,U] - P)$. On a

$$\omega(\Delta) = \{\lceil h \rceil f(x) \lceil h \rceil^{-1} \ / \ h \in K^{x} \text{ et } x \in K\} .$$

Sous l'action de $C_G(t) = PHsP \cup PH$, l'orbite de η^3 est donc

$$\Omega_1 = \Delta \cup P.\omega(\Delta) .$$

L'application ω est déterminée sur Ω_1. On a vu qu'elle l'est sur Δ par f; elle l'est sur $\omega(\Delta)$ car $\omega^2 = 1$. Elle l'est sur $P.\omega(\Delta)$ parceque $\omega(P^*) = P^*$ et $P.\Delta \subset \Delta$:

si $a \in \Delta$, $b \in P$ et $b \neq 0$, on a $sb\omega(a)s \in \omega(b)s\rho(b)\omega(b)asB$

et $\rho(b)\omega(b)a\rho(b)^{-1} \in \Delta$.

Par dénombrement on constate qu'il reste une orbite selon $C_G(t)$ sur Ω; on a en effet

$$q^3 + 1 = q + 1 + 2(q^3 - q)/2 ,$$

soit $$|G:B| = |\Omega_o| + 2|C_G(t)|$$

Comme $\mu^2\eta^2 = \eta^{-1}\mu^2$, de $s\eta^3 s = \mu^2\eta^2 s\mu\eta^8$, on déduit

$$ts\mu\eta s = \mu\eta st\eta^6 \in \mu\eta sB$$

donc $\mu\eta$ est un point fixe de st. Or le fixateur d'un point de Ω dans G ne contient pas de groupe de type (2,2). Il en résulte que $\mu\eta$ et $\eta^5\mu$, qui sont fixes par les involutions st et t non conjuguées par $C_G(t)$, ne sont pas dans la même orbite selon $C_G(t)$. Soit donc Ω_2 l'orbite de $\mu\eta$ selon $C_G(t)$. On a

$$\Omega = \Omega_o \cup \Omega_1 \cup \Omega_2 ,$$

et il reste à démontrer que ω est déterminée sur Ω_2.

(c) Une géométrie dans Ω.

A toute involution v de G associons l'ensemble de ses points fixes sur Ω et notons-le L(v); L(v) sera une droite de la géométrie annoncée. L'intersection de deux conjugués de B contenant une seule involution, (on a $H = B \cap sBs$), par deux points de Ω il passe au plus une droite.

Montrons que la géométrie ainsi définie est unique, déterminée par l'action de B sur Ω et la restriction de ω à $(\Omega_o \cup \Omega_1)$.

On a vu que $L(t) = \Omega_o$. Le groupe $C_G(<t,s>)$ est transitif sur Ω_o. Or il existe un élément de G qui transforme (t,s) en (s,ts). Le même groupe $C_G(<t,s>)$ est donc transitif sur L(s). Comme on voit dans G_1 que $s\eta^3\mu^2 s = \eta^3\mu^2 st\eta^2$, $\eta^3\mu^2$ est un point fixe de s appartenant à Δ, et $L(s) = C_G(<t,s>).\eta^3\mu^2$ est déterminé par l'opération de B et la restriction de ω à Δ.

Quant à la droite des points fixes de l'involution st, elle est donnée par

$$L(st) = \{\mu\eta\} \cup \{\mu\eta g(x)^{-1};\ x \in K\}.$$

La fonction g a été introduite au chapitre 6; rappelons que, selon les 6, 8 et 14 de ce chapitre, on a

$$u(x)^{-1} = u(-x)^t$$

et $$f(-x)^t = \omega(u(-x)^t) = \omega(u(x)^{-1}) = \pi(u(x)^{-1}) = g(x)^{-1}$$

d'où $$\omega(g(x)^{-1}) = u(x)^{-1}.$$

On a déjà vu que $\mu\eta$ est fixe par st. D'autre part l'image u' de $\mu\eta g(x)^{-1}$ par st est définie par $u'sB = ts\mu\eta g(x)^{-1}sB$. D'après ce qui précède, on a

$$\begin{aligned} ts\mu\eta g(x)^{-1}sB &= \mu\eta ts\eta^{-3}sg(x)^{-1}sB \\ &= \mu\eta ts\eta^{-3}\omega(g(x)^{-1})sB \\ &= \mu\eta ts(-1,0,0)(-1,-x,0)sB; \end{aligned}$$

on en déduit

$$u' = \mu\eta\omega(u(-x)^t) = \mu\eta g(x)^{-1}.$$

Quand x parcourt K, les éléments g(x) sont deux à deux distincts, L(st) est donc déterminée.

Il y a 3 orbites selon B dans l'ensemble des involutions de G, contenant respectivement t, s et ts (deux involutions $u^{-1}shu$ et $v^{-1}sh'v$ écrites dans la décomposition de Bruhat sont conjuguées selon B si et seulement si $hH^2 = h'H^2$). Par translation selon B depuis L(s), L(t) et L(ts) on obtient toutes les droites de la géométrie.

(4) Conclusion.

Soit $u \in \Omega_2$. Il nous reste à démontrer que $\omega(u)$ est déterminé par la géométrie précédente et la restriction de ω à $(\Omega_o \cup \Omega_1)$.

Il existe q^2 droites contenant u, car B contient q^2 involutions. Soit $M(u)$ l'ensemble des droites passant par u et rencontrant $(\Omega_o \cup \Omega_1)$ en au plus un point. Puisque deux droites se rencontrent en au plus un point et chaque droite contient (q+1) points, on a

$$\left| \left(\bigcup_{L \in M(u)} L \right) \cap \Omega_2 \right| \geqslant 1 + |M(u)|(q - 1)$$

d'où

$$|M(u)|(q - 1) + 1 \leqslant (q^3 - q)/2$$

$$|M(u)| < q(q + 1)/2 .$$

Comme $q(q + 1)/2 < q^2 - 2$, il existe au moins deux droites L et L' passant par u et rencontrant chacune $(\Omega_o \cup \Omega_1)$ en au moins deux points. Les droites $\omega(L)$ et $\omega(L')$ sont déterminées par les images par ω de leurs intersections avec $(\Omega_o \cup \Omega_1)$, et $\omega(u)$ est l'unique point commun à $\omega(L)$ et $\omega(L')$.

APPENDICE

Caractères irréductibles et 2-blocs de $PSL_2(q)$.

Les caractères irréductibles de $PSL_2(q)$ ont été calculés par Schur [23]; on les trouvera dans le livre de Dornhoff [11]

Notations: q est une puissance de p, premier impair

$q - e \equiv 4 \pmod 8$ et $e \in \{1,-1\}$

F est isomorphe à $PSL_2(q)$

y est un élément de F d'ordre $(q + e)/2$

z est un élément de F d'ordre $(q - e)/2$

μ_1 et μ_2 sont des éléments d'ordre p de F, non conjugués

ρ est une racine d'ordre $(q + e)/2$ de 1, atre que 1

σ est une racine d'ordre $(q - e)/2$ de 1, autre que 1 et -1

Table des caractères irréductibles de F:

	1	μ_1	μ_2	y^m	z^n
θ_1	1	1	1	1	1
θ_2	$\frac{1}{2}(q + e)$	$\frac{1}{2}(e + (eq)^{1/2})$	$\frac{1}{2}(e - (eq)^{1/2})$	0	$e(-1)^n$
θ_3	$\frac{1}{2}(q + e)$	$\frac{1}{2}(e - (eq)^{1/2})$	$\frac{1}{2}(e + (eq)^{1/2})$	0	$e(-1)^n$
θ_4	q	0	0	-e	e
θ_ρ	q - e	-e	-e	$-e(\rho^m + \rho^{-m})$	0
θ_σ	q + e	e	e	0	$e(\sigma^n + \sigma^{-n})$

m varie de 1 à $(q + e - 2)/4$

n varie de 1 à $(q - e)/4$

il y a $(q + e - 2)/4$ caractère θ_ρ distincts et $(q - e - 4)/4$ caractères θ_σ distincts (on a $\theta_\rho = \theta_{\rho^{-1}}$ et $\theta_\sigma = \theta_{\sigma^{-1}}$)

F contient $2 + (3q + e)/8$ classes 2-régulières.

Les 2-blocs de F:

Les caractères θ_ρ sont de 2-défaut nul.

Les caractères θ_σ et $\theta_{-\sigma}$ coïncident sur les classes 2-régulières; ils sont donc dans un même bloc (1.11), qui est de défaut 1 (1.13) et ne contient pas d'autre irréductible (1.14).

Un 2-groupe de Sylow de F est égal à son centralisateur dans F, donc F admet un seul bloc de défaut 3, le bloc principal $b_o(F)$, lequel contient nécessairement θ_1, θ_2, θ_3 et θ_4 (1.13). On voit clairement que $(b_o(F).R(F))$ admet pour base sur $\mathbb{Z}$

$$d(\theta_1) = \phi_1 \quad d(-e\theta_2) = \phi_2 \quad \text{et} \quad d(-e\theta_3) = \phi_3 .$$

La matrice de $d_{b_o(F)}$ sur ces bases est donc

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

Caractères irréductibles et 2-blocs de $\langle t \rangle \times F = C_G(t)$.

Un caractère de F sera considéré comme un caractère de $C_G(t)$ dont le noyau contient t. Si θ est un tel caractère son produit par le caractère irréductible non trivial de $\langle t \rangle$ sera noté θ'. On a évidemment $d(\theta) = d(\theta')$.

Il résulte des résultats généraux rappelés en 1 que l'ensemble des blocs de $C_G(t)$ est en bijection avec l'ensemble des blocs de F, les modules $R_p(F)$ et $R_p(C_G(t))$ sont canoniquement isomorphes.

On obtient ainsi les blocs

b_ρ, de défaut 1, contenant θ_ρ, θ'_ρ ; $\phi_\rho = d(\theta_\rho)$ et $C_{b_\rho} = (2)$.

b_σ, de défaut 2, contenant θ_σ, θ'_σ , $\theta_{-\sigma}$, $\theta'_{-\sigma}$

$$\phi_\sigma = d(\theta_\sigma) \quad \text{et} \quad C_{b_\sigma} = (4)$$

$b_o = b_o(C_G(t))$ contenant θ_i et θ'_i (i = 1, 2, 3 et 4)

$$C_{b_o} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 2 \\ 2 & 2 & 4 \end{pmatrix}$$

Pour utiliser la formule de Brauer-Suzuki (1.23) on calcule

$$A(b_o,\phi_1) = q + e \quad ; \quad A(b_o,\phi_2) = -(3eq + 1)/(q - e); \quad A(b_\sigma,\phi_\sigma) = 8q/(q - e)$$

Soit $\mathcal{D}$ la 2-section de t dans $C_G(t)$, c'est-à-dire

$$\mathcal{D} = \{tg/\ g \in F,\ g \text{ d'ordre impair}\} .$$

On calcule aisément, pour tout bloc b de $C_G(t)$, $b.R(C_G(t)|\mathcal{D})$ (notations du paragraphe 1, cf la proposition 1.22).

$b.R(C_G(t)|\mathcal{D})$ admet pour base sur $\mathbb{Z}$

Si $b = b_o(C_G(t))$: $\{\tilde{\psi}_1, \tilde{\psi}_2, \tilde{\psi}_3\}$;

$$\tilde{\psi}_1 = \theta_1 - \theta'_1 - e(\theta_4 - \theta'_4)$$
$$\tilde{\psi}_2 = \theta_4 - \theta'_4 + \theta_2 - \theta'_2$$
$$\tilde{\psi}_3 = \theta_4 - \theta'_4 + \theta_3 - \theta'_3$$

Si $b = b_\sigma$: $\{\tilde{\psi}_\sigma\}$; $\tilde{\psi}_\sigma = \theta_\sigma - \theta'_\sigma + \theta_{-\sigma} - \theta'_{-\sigma}$

Si $b = b_\rho$: $\{\tilde{\psi}_\rho\}$; $\tilde{\psi}_\rho = \theta_\rho - \theta'_\rho$

Proposition.- Soient n, k et s des entiers naturels tels que n = ks et $A = (a_{i,j})$ une matrice (n,n). On suppose qu'il existe une partition de $\{1,2,\ldots,n\}$ en s ensembles E_α de cardinal k, ainsi que s ensembles F_α deux à deux disjoints, de cardinal (k-1) tels que

$$\text{si } j \in F_\alpha \text{ et } i \notin E_\alpha \text{ alors } a_{i,j} = 0 .$$

Posons $S = \{1,2,\ldots,n\} - \bigcup_\alpha F_\alpha = \{j_1, j_2, \ldots, j_s\}$.

Soit $d_{\alpha,\beta}$ le déterminant de la matrice carrée extraite de A sur les lignes $i \in E_\alpha$ et les colonnes $j \in (F_\alpha \cup \{j_\beta\})$, où $\alpha, \beta \in \{1,2,\ldots,n\}$. On a

$$\det(A) = \pm \det(d_{\alpha,\beta}) .$$

Démonstration. En permutant lignes et colonnes de A, on peut supposer que

$$E_\alpha = \{i \in \mathbf{N} / (\alpha-1)k < i \leqslant \alpha k\} \qquad (\alpha \in \{1,2,\ldots,s\})$$

$$F_\alpha = \{j \in \mathbf{N} / (\alpha-1)(k-1) < j \leqslant \alpha(k-1)\} (\alpha \in \{1,2,\ldots,s\})$$

d'où $S = \{ j \in \mathbf{N} / s(k-1) < j \leqslant n\}$.

Un terme du développement standard de det(A) est de la forme

$$\varepsilon(\sigma) \prod_j a_{\sigma(j),j} \qquad (\sigma \in S_n , \varepsilon \text{ est la signature}).$$

S'il est non nul, c'est que $\sigma(F_\alpha) \subset E_\alpha$ pour tout $\alpha \in \{1,2,\ldots,s\}$.

Dans ce cas il existe une bijection f_σ de $\{1,2,\ldots,s\}$ sur S telle que

$$E_\alpha = \sigma(F_\alpha) \cup \{\sigma(j_{f_\sigma(\alpha)})\} .$$

La somme des termes correspondant aux permutations σ telles que $\sigma(F_\alpha) \subset E_\alpha$ et f_σ soit fixée et égale à f est évidemment le déterminant de la matrice A_f déduite de A en annulant les coefficients d'indice (i,j) tels que $i \in E_\alpha$, $j_k \in S$ et $k \neq f(\alpha)$. Au signe près la matrice A_f est la matrice diagonale des matrices carrées $A_{f,\alpha}$ extraites de A sur le produit $E_\alpha \times (F_\alpha \cup \{j_{f(\alpha)}\})$. On obtient une matrice diagonale de blocs en permutant les colonnes de S selon f, puis en renvoyant la première de ces s colonnes au k-ième rang, etc.... La signature de la permutation envisagée est donc $\varepsilon(f) + (-1)^m$, avec $m = (k-1)s(s-1)/2$. D'où

$$\det(A_f) = (-1)^m \varepsilon(f) \prod_\alpha d_{\alpha,f(\alpha)} \quad \text{et} \quad \det(A) = \sum_f \det(A_f)$$

ce qui démontre la proposition.

Bibliographie

[1] E. Bombieri. *Thompson's problem* ($\sigma^2 = 3$). Inventiones Mathematicae 58 (1980) 77-

[2] R. Brauer. *Investigations on group characters*. Ann. of Math. 42 (1941) 936-958.

[3] R. Brauer. *On the structure of groups of finite order*. Proc. of the Intern. Congress of Math. 1954, vol. 1, Nordhoff, Gröningen; North-Holland, Amsterdam, 1957, p. 209-214.

[4] R. Brauer. *Zur Darstellungstheorie der Gruppen endlicher Ordnung*. Math. Z. 63 (1956) 406-444.

[5] R. Brauer. *Zur Darstellungstheorie der Gruppen endlicher Ordnung, II*. Math. Z. 72 (1959) 25-46.

[6] R. Brauer. *Investigations on groups of even order, I*. Proc. Nat. Acad. Sci. U.S.A. 47 (1961) 1891-1893.

[7] R. Brauer. *Some applications of the theory of blocks of characters of finite groups. I*. J. of Alg. 1 (1964) 152-157.

[8] R. Brauer et W. Feit. *On the number of irreducible characters of finite groups in a given block*. Proc. Nat. Acad. Sci. U.S.A. 45 (1959) 361-365.

[9] R. Brauer et M. Suzuki et G. E. Wall. *A characterization of the one-dimensional unimodular projective groups over finite fields*. Illinois J. of Math. 2 (1958) 718-745.

[10] M. Broué. *Radical, hauteurs, p-sections et blocs*. Annals of Math. 107 (1978) 89-107.

[11] L. Dornhoff. *Group Representation Theory, Part B*. Marcel Dekker, New-York, 1972.

[12] W. Feit et J. G. Thompson. *Solvability of groups of odd order*. Pacific J. of Math. 13 (1963) 775-1029.

[13] G. Frobenius et I. Schur. *Ueber die Darstellungen der endlichen Gruppen*. S.-B. Berlin Math. Ges. (1906) 186-208.

[14] D. M. Goldschmidt. *Lectures on Character Theory*. Publish or Perish, Berkeley, 1980.

[15] D. Gorenstein et J. H. Walter. *On finite groups with dihedral Sylow 2-subgroups*. Illinois J. of Math. 6 (1962) 553-593.

[16] B. Huppert. *Endliche Gruppen I*. Springer Verlag, Berlin, 1967.

[17] P. Hall et G. Higman. *The p-length of a p-soluble group, and reduction theorems for Burnside's problem*. Proc. London Math. Soc. (3) 7 (1956) 1-42.

[18] Z. Janko. *A new finite simple group with abelian Sylow 2-subgroups and its characterization.* J. of Alg. 3 (1966) 147-186.

[19] Z. Janko. *A characterization of the smallest group of Ree associated with the simple Lie algebra of type* (G_2). J. of Alg. 4 (1966) 293-299.

[20] Z. Janko et J. G. Thompson. *On a Class of Finite Simple Groups of Ree.* J. of Alg., 4 (1966) 274-292.

[21] R. Ree. *A family of simple groups associated with the simple Lie algebra of type* (G_2). Amer. J. of Math. 83 (1961) 432-462.

[22] R. Ree. *Sur une famille de groupes de permutations doublement transitifs.* Canad. J. of Math. 16 (1964) 797-820.

[23] I. Schur. *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene linear Substitutionen.* J. Reine Angew. Math. 132 (1907) 85-137.

[24] M. Suzuki. *On characterizations of linear groups. I.* Trans. Amer. Math. Soc. 92 (1959) 191-204.

[25] M. Suzuki. *Applications of group characters.* Proc. Symp. of Pure Math., vol. I (Finite Groups) Providence , 1959, 88-99.

[26] M. Suzuki. *On a class of doubly transitive groups.* Annals of Math. (2) 75 (1962) 105-145.

[27] M. Suzuki. *Finite groups of even order in which Sylow 2-subgroups are independant.* Annals of Math. 80 (1964) 58-77.

[28] J. G. Thompson. *Toward a characterization of* $E_2^*(q)$. *I, II, III.* J. of Alg. 7 (1967) 406-414; 20 (1972) 610-621; 49 (1977) 162-166.

[29] J. Tits. *Les groupes simples de Suzuki et de Ree.* Séminaire Bourbaki, 13ème année (1960-1961) n°210.

[30] J. H. Walter. *Character theory of finite groups with trivial intersection subsets.* Nagoya J. of Math. 27 (1966) 514-524 et 30 (1967) 309.

[31] J. H. Walter. *Finite groups with abelian Sylow 2-subgroups of order 8.* Invention. Math. 2 (1967) 332-376.

[32] J. H. Walter. *The characterization of finite groups with abelian Sylow 2-subgroups.* Annals of Math. 89 (1969) 405-514.

[33] H. N. Ward. *On Ree's series of simple groups.* Trans. Amer. Math. Soc. 121 (1966) 62-89.

[34] H. Wielandt. *Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endliche Gruppe.* Math. Z. 73 (1960) 146-158.

Michel Enguehard
54, rue de Montdauphin
77240, Cesson, France.