# SUR UNE FAMILLE DE GROUPES DE PERMUTATIONS DOUBLEMENT TRANSITIFS

RIMHAK REE

**Introduction.** Dans **(6)**, l'auteur a défini, pour chaque entier $n \geqslant 0$, un groupe fini $G_n$ d'ordre $q^3(q-1)(q^3+1)$, où $q = 3^{2n+1}$. Les groupes $G_1, G_2, \ldots$ sont simples, tandis que $G_0'$ est simple.

En réalisant $G = G_n$ comme un groupe de permutations, opérant à droite, de l'ensemble de $q^3+1$ classes à droite modulo le normalisateur $N(P)$ d'un 3-sous-groupe de Sylow de $G$, on voit aisément que $G$ satisfait aux conditions (0.1)–(0.4) suivantes :

(0.1) *$G$ est un groupe de permutations doublement transitif d'un ensemble $E$ de $m+1$ lettres, où $m \geqslant 3$;*

(0.2) *si* **a** *et* **b** *sont deux lettres distinctes quelconques de $E$, le sous-groupe formé de la totalité des permutations dans $G$ qui laissent invariantes* **a** *et* **b** *contient une, et une seule, permutation $\neq 1$ qui laisse au moins 3 lettres invariantes;*

(0.3) *toute involution dans $G$ laisse au moins 3 lettres invariantes (une involution dans un group est par définition un élément d'ordre 2);*

(0.4) *$m$ est impair.*

Notons que, en vertu de la condition (0.2), la condition (0.3) est équivalente à dire que toutes les involutions dans $G$ sont conjuguées entre elles.

Le but de cet article est d'étudier les groupes de permutations satisfaisants aux conditions (0.1)–(0.4) ci-dessus. Nous démontrerons que $m = q^3$, où $q = 3^{2n+1}$ avec un entier $n \geqslant 0$, que le groupe $G$ a l'ordre $q^3(q-1)(q^3+1)$, et que $G$ est isomorphe à $G_0$ dans le cas $n = 0$. Nous démontrerons également que si $n > 0$ le groupe $G$ satisfait aux "axiomes" donnés par H. N. Ward **(8)**, ce qui permettra, entre autres, de calculer tous les caractères de $G$ et de dériver plusieurs propriétés des 3-sous-groupes de Sylow de $G$ **(8)**. It est probable que ces propriétés de $G$ sont suffisantes pour identifier $G$ avec $G_n$, mais on manque encore la démonstration.

Si l'on remplace la condition (0.4) par la condition

(0.4′) *$m$ est pair,*

on se trouve dans un cas tout à fait différent, et on ignore s'il existe un groupe qui satisfait aux conditions (0.1)–(0.3) et (0.4′).

*Notations.* Si $B$ est une partie d'un ensemble $A$, le complément de $B$ dans $A$ sera noté $A - B$. Si $A$ est un ensemble fini, le nombre des éléments dans

Reçu le 8 novembre, 1963.

$A$ sera noté $|A|$. Si $G = \{a, b, \ldots\}$ est un groupe, et si $S, T, \ldots$ sont des parties de $G$, on notera $a^b = b^{-1}ab$, $S^b = \{s^b | s \in S\}$. On notera $C_S(T)$, $N_S(T)$, respectivement, le centralisateur et le normalisateur de $T$ dans $S$. On écrira simplement $C(T)$, $N(T)$ au lieu de $C_G(T)$, $N_G(T)$. Le sous-groupe engendré par $S$ (par $a$) sera noté $\langle S \rangle$ (par $\langle a \rangle$).

**1. Généralités.** Soit $G$ un groupe de permutations satisfaisant aux conditions (0.1)–(0.4), et soit $B$ le sous-groupe de $G$ formé de la totalité des permutations dans $G$ qui laissent invariante une lettre fixée **a**. Alors on a

$$|G| = (m + 1)|B|. \tag{1.1}$$

L'intersection de tous les conjugués de $B$ dans $G$ se réduit à $\{1\}$, et $G$ est d'ordre pair en vertu de la condition (0.1). On peut donc trouver une involution $\omega$ dans $G - B$, et on déduit aisément de la condition (0.1) que

$$G = B \cup B\omega B, \qquad B \cap B\omega B = \emptyset. \tag{1.2}$$

Posons $\mathbf{b} = \mathbf{a}^\omega$. On a $\mathbf{b} \neq \mathbf{a}$. Ecrivons

$$H = B \cap B^\omega. \tag{1.3}$$

Alors $H$ est le sous-groupe formé de toutes les permutations dans $G$ qui laissent invariantes les lettres **a** et **b**, d'où il résulte que

$$|B| = m|H|. \tag{1.4}$$

En vertu de (1.1) et (1.4), on a

$$|G| = m(m + 1)|H|. \tag{1.5}$$

Puisque $\omega$ est une involution, il résulte de (1.3) que

$$H^\omega = H. \tag{1.6}$$

D'après la condition (0.2), le sous-groupe $H$ contient un et un seul élément $h_0 \neq 1$ qui laisse invariantes au moins 3 lettres. Il est clair que $h_0$ est une involution dans le centre de $H$. Des conditions (0.2)–(0.3) on déduit aisément la

PROPOSITION 1.7. *L'élément $h_0$ est la seule involution dans $H$.*

D'après (1.6), $h_0$ est une involution dans $H$. On a donc la

PROPOSITION 1.8. $h_0\omega = \omega h_0$.

Comme nous avons déjà remarqué dans l'introduction, les conditions (0.2)–(0.3) entraînent également la

PROPOSITION 1.9. *Toutes les involutions dans $G$ sont conjuguées entre elles.*

Ecrivons $H_0 = \{1, h_0\}$. Alors $H_0$ est un sous-groupe dans le centre de $H$, et, d'après (0.2), on a la

PROPOSITION 1.10. *$H \cap H^x \subseteq H_0$ pour tout élément $x$ dans $B - H$.*

D'après un théorème de Wielandt **(9**, Satz 2**)**, la proposition 1.10 implique qu'il existe un sous-groupe distingué $\bar{U}$ de $B$ tel que

$$B = \bar{U}H, \qquad \bar{U} \cap H = H_0. \tag{1.11}$$

Alors $B/\bar{U} \cong H/H_0$, et, d'après (1.4), on a $|\bar{U}| = 2m$. Puisque $m$ est impair d'après la condition (0.4), $\bar{U}$ contient un sous-groupe distingué $U$ d'ordre $m$ tel que

$$\bar{U} = UH_0, \qquad U \cap H_0 = \{1\}. \tag{1.12}$$

Il est clair que $U$ est distingué dans $B$ et que

$$B = UH, \qquad U \cap H = \{1\}. \tag{1.13}$$

On a donc, d'après (1.3),

$$UH \cap U^\omega = \{1\}. \tag{1.14}$$

La proposition suivante se déduit aisément de la proposition (1.2), de (1.13), et de (1.14).

PROPOSITION 1.15. *On a*

$$G = UH \cup UH\omega U, \quad UH \cap UH\omega U = \emptyset.$$

*Tout élément dans $UH$ se met d'une, et d'une seule, manière sous la forme $uh$, où $u \in U$ et $h \in H$. Tout élément dans $UH\omega U$ se met d'une, et d'une seule manière sous la forme $u_1 h \omega u_2$, où $u_i \in U$ $(i = 1, 2)$ et $h \in H$.*

PROPOSITION 1.16. *$N(U) = UH$.*

Evidemment $UH$ normalise $U$. Supposons donc que $x \in G - UH$ normalise $U$; écrivons, d'après la proposition 1.15, $x$ sous la forme $u_1 h \omega u_2$, où $u_i \in U$ $(i = 1, 2)$ et $h \in H$. Il en résulte que $\omega$ normalise $U$, ce qui est une contradiction avec (1.14).

PROPOSITION 1.17. *Si $u \in U - \{1\}$, on a $C(u) \subseteq UH$.*

En effet, supposons que $x \in G - UH$ centralise $u$; écrivons $x$ sous la forme $u_1 h \omega u_2$, où $u_i \in U (i = 1, 2)$ et $h \in H$. La relation $u_1 h \omega u_2 \; u = u u_1 h \omega u_2$ entraîne, d'après la proposition 1.15, que $u_1 = u u_1$, $u = 1$, ce qui est absurde.

PROPOSITION 1.18. *Si $h \in H - H_0$, l'application $u \to u^h$ est un automorphisme sans point fixe de $U$.*

En effet, $h$ laisse invariantes les lettres **a** et **b**. Si $u^h = u$, $h$ laisse invariante aussi la lettre $\mathbf{c} = \mathbf{b}^u = \mathbf{a}^{\omega u}$. Puisque $h \in H - H_0$, $h$ laisse invariantes exactement deux lettres d'après la condition (0.2). Or, on a $\mathbf{c} \neq \mathbf{a}$ parce que $\omega u \notin UH$. On doit donc avoir $\mathbf{c} = \mathbf{b}$, ce qui entraîne $u = 1$ en vertu de (1.14).

PROPOSITION 1.19. *Etant donné $h \in H - H_0$ et $x \in G$, on a $x \in H \cup H\omega$ si $h^x \in H$.*

https://doi.org/10.4153/CJM-1964-077-2 Published online by Cambridge University Press

Posons $h' = h^x$, et remarquons d'abord que $h' \in H - H_0$. En effet, d'après la proposition 1.17, $h$ n'est pas une involution, et par suite $h'$ ne l'est pas non plus, d'où $h' \in H - H_0$ en vertu de la proposition 1.7.

Considérons maintenant le cas où $x$ est dans $UH$; mettons $x$ sous la forme $uh_1$, où $u \in U$ et $h_1 \in H$. La relation $huh_1 = uh_1 h'$ implique, comme on voit aisément de la proposition 1.15, que $huh^{-1} = u$, ce qui entraîne, d'après la proposition 1.18, que $u = 1$, et par conséquent on a $x = h_1 \in H$.

Considérons maintenant le cas où $x$ est dans $UH\omega U$; mettons $x$ sous la forme $u_1 h_1 \omega u_2$, où $u_i \in U (i = 1, 2)$ et $h_1 \in H$. La relation $hu_1 h_1 \omega u_2 = u_1 h_1 \omega u_2 h'$ implique, d'après la proposition 1.15, que $hu_1 h^{-1} = u_1$, $h'^{-1} u_2 h' = u_2$, d'où il résulte que $u_1 = u_2 = 1$, parce que $h$ et $h'$ sont tous deux dans $H - H_0$. On a donc $x = h_1 \omega \in H\omega$.

COROLLAIRE 1.20. *Si $h \in H - H_0$, on a $C(h) \subseteq H \cup H\omega$.*

COROLLAIRE 1.21. *Si $H \neq H_0$, on a $N(H) = H \cup H\omega$.*

Posons $U_0 = \{u \in U | uh_0 = h_0 u\}$, $|U_0| = q$. Alors les $q + 1$ lettres $\mathbf{a}$ et $\mathbf{a}^{\omega u}$, pour $u$ parcourant $U_0$, sont exactement celles que $h_0$ laisse invariantes, d'où $q > 1$ en vertu de la condition (0.2).

Des propositions 1.8 et 1.15, on déduit aisément la

PROPOSITION 1.22. $C(h_0) = U_0 H \cup U_0 H\omega U_0$.

COROLLAIRE 1.23. $|C(h_0)| = q(q + 1)|H|$.

PROPOSITION 1.24. *Le groupe $H/H_0$ opère, par l'application $u \to u^h$, dans le groupe $U_0$ comme un groupe d'automorphismes sans point fixe.*

En effet, il est clair que $H$ normalise $U_0$, parce que $h_0$ est dans le centre de $H$ (proposition 1.7). Alors, notre assertion résulte immédiatement de la proposition 1.18.

PROPOSITION 1.25. *Pour tout nombre premier $p$, les $p$-sous-groupes de Sylow de $H$ sont cycliques.*

Soit, en effet, $S$ un $p$-sous-groupe de Sylow de $H$. Si $p \neq 2$, la proposition 1.18 montre que $S$ opère, par l'application $u \to u^h$, dans $U$ comme un groupe d'automorphismes sans point fixe. Alors, d'après Burnside **(2**, p. 336**)**, $S$ est cyclique.

Il reste à considérer le cas $p = 2$. D'après la proposition 1.7, $S$ contient une, et une seule, involution, à savoir, $h_0$. Alors, d'après Burnside **(2**, p. 336**)**, ou $S$ est cyclique, ou c'est un groupe de quarternions généralisé. La dernière possibilité s'élimine comme suit : si $S$ était un groupe de quarternions généralisé, $S/H_0$ contiendrait un quatre-group comme un sous-groupe. Cependant, c'est impossible en vertu de la proposition 1.24 (un quatre-group est par définition un 2-groupe élémentaire d'ordre 4).

PROPOSITION 1.26. *En associant à tout élément $x$ dans $C(h_0)$ la permutation*

https://doi.org/10.4153/CJM-1964-077-2 Published online by Cambridge University Press

*$U_0 Hy \to U_0 Hyx$ de l'ensemble des classes à droite modulo $U_0 H$ dans $C(h_0)$, on obtient une réalisation fidèle du groupe $C(h_0)/H_0$ comme un groupe de permutations de $q+1$ lettres (classes), qui possède les propriétés suivantes :*

(i) *$C(h_0)/H_0$ est doublement transitif;*

(ii) *l'élément neutre de $C(h_0)/H_0$ est la seule permutation dans $C(h_0)/H_0$ qui laisse invariante au moins 3 lettres (classes);*

(iii) *le sous-groupe $H/H_0$ se compose de la totalité des permutations dans $C(h_0)/H_0$ qui laissent invariantes les deux lettres (classes) $U_0 H$ et $U_0 H\omega$;*

(iv) *le sous-groupe $U_0 H/H_0$ se compose de la totalité des permutations dans $C(h_0)/H_0$ qui laissent invariante la lettre (classe) $U_0 H$.*

En effet, les propriétés (i) et (ii), ainsi que le fait que la réalisation du $C(h_0)/H_0$ est fidèle, se déduisent aisément des propositions 1.18–1.24. Les propiétés (iii) et (iv) sont triviales.

Démontrons maintenant la

PROPOSITION 1.27. *Désignant par $n$ le nombre d'involutions dans la partie $H\omega$ de $G$, on a*

$$m = (qn + n + 1)q.$$

En effet, montrons d'abord que toute involution dans $UH$ est conjuguée à $h_0$ dans $UH$, ce qui impliquera evidemment que le nombre d'involutions dans $UH$ est égale à

$$(UH : UH \cap C(h_0)) = (UH : U_0 H) = (U : U_0) = mq^{-1}.$$

Si, en effet, $x$ est une involution dans $UH$, $x$ laisse invariante la lettre **a**. $x$, étant une involution, laisse invariante une autre lettre **c** d'après la condition (0.3). D'autre part, $G$ étant doublement transitif, on peut trouver un élément $y$ dans $G$ qui laisse **a** invariante et qui applique **c** sur **b**. On a alors $y \in UH$ et $x^y \in H$, parce que $x^y$ laisse invariante **a** et **b**. $x^y$ est donc une involution dans $H$, et d'après la proposition 1.7, on a $x^y = h_0$.

Comptons maintenant le nombre d'involutions dans $UH\omega U$. Soit $x = u_1 h\omega u_2$, une involution où $u_i \in U$ $(i = 1, 2)$ et $h \in H$. Alors $u_1 h\omega u_2 u_1 h\omega u_2 = 1$ implique, en vertu de (1.14), que $u_2 u_1 = 1$. Il en résulte que $UH\omega U$ contient $mn$ involutions. On en conclut que $G$ contient $mq^{-1} + mn$ involutions. Puisque toute involution dans $G$ est conjuguée à $h_0$, on a, d'après (1.5) et (1.23),

$$(mq^{-1} + mn)q(q+1)|H| = m(m+1)|H|$$

d'où $m = (qn + n + 1)q$.

**2. L'indice** $(H{:}H_0)$. Nous allons démontrer dans ce numéro que l'indice $(H : H_0)$ est impair. Citons d'abord deux théorèmes, dûs à Schur, dont nous allons faire usage dans ce qui suit.

LEMME 2.1 **(7**, p. 119**)**. *Soient $q > 0$ une puissance d'un nombre premier impair, $X$ un groupe, et $Y$ un sous-groupe d'ordre 2 contenu dans le centre de*

*$X$. Si $X/Y$ est isomorphe à* $\mathrm{PSL}(2, q)$, *alors ou $X$ est isomorphe à* $\mathrm{SL}(2, q)$, *ou c'est un produit direct de $Y$ par un groupe isomorphe à* $\mathrm{PSL}(2, q)$.

LEMME 2.2 **(7**, p. 122**)**. *Soient $q > 0$ une puissance d'un nombre premier tel que $q \equiv -1 \pmod 4$, $X$ un groupe, et $Y$ un sous-groupe d'ordre 2 contenu dans le centre de $X$. Si $X/Y$ est isomorphe à* $\mathrm{PGL}(2, q)$, *et si $X$ contient plus d'une involution, alors $X$ est isomorphe au sous-groupe* $\mathrm{SL}^*(2, q)$ *de* $\mathrm{GL}(2, q)$ *formé de la totalité des matrices dans* $\mathrm{GL}(2, q)$ *dont le déterminant est égale à* $\pm 1$.

Notons que le group $\mathrm{PSL}(2, q)$ (le group $\mathrm{PGL}(2, q)$) est par définition le groupe quotient de $\mathrm{SL}(2, q)$ (de $\mathrm{GL}(2, q)$) sur son centre.

PROPOSITION 2.3. *L'indice $(H : H_0)$ est impair.*

Nous déduirons une contradiction de l'hypothèse que $(H : H_0)$ soit pair. Le groupe $H/H_0$ étant alors d'ordre pair, un théorème de Zassenhaus **(10**, p. 39**)** s'applique au groupe $C(h_0)/H_0$ en vertu de la proposition 1.26; il en résulte que $q$ est une puissance d'un nombre premier impair, et que $C(h_0)/H_0$ est isomorphe soit à $\mathrm{PSL}(2, q)$, soit à $\mathrm{PGL}(2, q)$, soit au groupe noté par $M_q$ dans **(10**, p. 36**)**. Dans tous ces cas, $H$ contient un sous-groupe $H_1 \supseteq H_0$ d'indice 1 (dans le cas $C(h_0)/H_0 \cong \mathrm{PSL}(2, q)$) ou 2 (dans les autres cas) tel que

$$C_1(h_0) = U_0 H_1 \cup U_0 H_1 \omega U_0$$

soit un sous-groupe d'indice 1 (dans le cas $C(h_0)/H_0 \cong \mathrm{PSL}(2, q)$) ou 2 (dans les autres cas) de $C(h_0)$, et tel que $C_1(h_0)/H_0$ soit isomorphe à $\mathrm{PSL}(2, q)$. Le groupe $C_1(h_0)$ ne peut être isomorphe à $\mathrm{SL}(2, q)$, parce que $C_1(h_0)$ contient plus d'une involution, à savoir $h_0$ et $\omega$, tandis que $\mathrm{SL}(2, q)$ ne contient qu'une seule. Alors le lemme 4.1 montre que $C_1(h_0) = L \times H_0$, où $L$ est un sous-groupe de $C_1(h_0)$ isomorphe à $\mathrm{PSL}(2, q)$. On a donc

$$H_1 = H_1 \cap C_1(h_0) = (H_1 \cap L) \times H_0,$$

d'où il résulte que $(H_1 : H_0)$ est impair, parce que les 2-sous-groupes de Sylow de $H_1$ sont cycliques en vertu de la proposition 1.25. Puisque $(H : H_0)$ est pair, il s'ensuit que $(H : H_1) = 2$ et que $C_1(h)/H_0$ est isomorphe soit à $\mathrm{PGL}(2, q)$, soit à $M_q$. Dans tous ces cas, le group $H/H_0$ est d'ordre $q - 1$. Puisque $\frac{1}{2}(H : H_0)$ est impair, il en résulte que $q \equiv -1 \pmod 4$, donc $q$ ne peut être un carré, ce qui montre que le groupe $M_q$ n'existe pas pour ce nombre $q$ **(10**, p. 37**)**. On conclut donc que $C(h_0)/H_0$ est isomorphe à $\mathrm{PGL}(2, q)$. Le groupe $C(h_0)$ possédant plus d'une involution, à savoir $h_0$ et $\omega$, le lemme 2.2 s'applique à $C(h_0)$, et il en résulte que $C(h_0)$ est isomorphe à $\mathrm{SL}^*(2, q)$ (pour la notation, voir le lemme 2.2). Soit $\phi : C(h_0) \to \mathrm{SL}^*(2, q)$ un isomorphisme. Le groupe $C(h_0)$, ayant l'ordre $2q(q^2 - 1)$, contient $U_0$ comme un sous-groupe de Sylow. On peut donc supposer que $\phi(U_0)$ se compose des matrices $\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$,

pour $\beta$ parcourant le corps $F_q$ de $q$ éléments. Or, il est facile de voir que $U_0 H$ est le normalisateur de $U_0$ dans $C(h_0)$. Il s'ensuit que $\phi(U_0 H)$ se compose des matrices $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$, où $\alpha$, $\beta$, $\gamma \in F_q$ et $\alpha\gamma = \pm 1$. On a donc

$$H \cong \phi(H) \cong \phi(U_0 H)/\phi(U_0) \cong \bar{H},$$

le dernier groupe étant par définition celui formé des matrices $\begin{pmatrix} \alpha & 0 \\ 0 & \gamma \end{pmatrix}$, où $\alpha, \gamma \in F_q$, $\alpha\gamma = \pm 1$. Il est clair que $\bar{H}$ contient deux involutions distinctes, à savoir, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. L'isomorphisme $H \cong \bar{H}$ implique donc une contradiction en vertu de la proposition 1.7, d'où notre assertion.

**3. Le cas** $(H:H_0) = 1$. Nous verrons que le cas $(H:H_0) = 1$ mérite un traitement spécial. Nous montrerons dans ce numéro que $G \cong G_0$ (pour la notation, voir l'introduction) si $(H : H_0) = 1$.

Supposons $(H : H_0) = 1$ dans ce numéro. D'après la proposition 1.26, le groupe $C(h_0)/H_0$ se réalise comme un groupe de permutations doublement transitif d'un ensemble de $q + 1$ lettres tel que l'identité est le seul élément qui laisse invariantes au moins 2 lettres. Alors, appliquant un théorème de Zassenhaus **(10**, p. 32**)** au groupe $C(h_0)/H_0$, on voit que $q + 1$ est une puissance d'un nombre premier et que $C(h_0)/H_0$ possède un sous-groupe distingué d'ordre $q + 1$. Comme $q$ est impair en tant que diviseur de $m$, on a $q + 1 = 2^\alpha$ pour un entier $\alpha \geqslant 2$. Puisque $|C(h_0)/H_0| = q(q + 1)$, on a

$$|C(h_0)| = 2^{\alpha+1}(2^\alpha - 1). \tag{3.1}$$

Soit $T/H_0$ le sous-groupe distingué d'ordre $q + 1$ de $C(h_0)/H_0$. Alors, $T$ est un sous-groupe distingué d'ordre $2^{\alpha+1}$ de $C(h_0)$. Montrons la

PROPOSITION 3.2. *$T$ est un 2-sous-groupe de Sylow de $C(h_0)$, et est un 2-groupe élémentaire.*

En effet, comptons le nombre d'involutions dans $C(h_0)$. Il est clair que $U_0 H_0$ ne contient qu'une involution, à savoir $h_0$. D'autre part, $U_0 H_0 \omega U_0$ contient seulement les $2q$ involutions $u^{-1}\omega u$ et $u^{-1}h_0 \omega u$, pour $u$ parcourant $U_0$. $C(h_0)$ contient ainsi $2q + 1 = 2^{\alpha+1} - 1$ involutions. De plus, toute involution dans $C(h_0)$ est dans $T$, parce que $T$ est le seul 2-sous-groupe de Sylow de $C(h_0)$. Il en résulte que tout élément $\neq 1$ de $T$ est une involution, ce qui montre que $T$ est un 2-groupe élémentaire.

Puisque $H\omega = H_0 \omega$ contient seulement 2 involutions, à savoir $h_0 \omega$ et $\omega$, on a, d'après la proposition 1.27,

$$\begin{aligned} m &= (2^\alpha - 1)(2^{\alpha+1} + 1), \\ |G| &= 2^{\alpha+1}(2^\alpha - 1)(2^{\alpha+1} - 1)(2^{\alpha+1} + 1), \end{aligned} \tag{3.3}$$

d'où il résulte que $T$ est un 2-sous-groupe de Sylow de $G$.

https://doi.org/10.4153/CJM-1964-077-2 Published online by Cambridge University Press

PROPOSITION 3.4. *Le normalisateur $N(T)$ de $T$ permute, par l'application $t \to t^x$ (où $t \in T, x \in N(T)$), les éléments dans l'ensemble $T - \{1\}$ transitivement.*

En effet, soit $t \in T - \{1\}$. D'après la proposition 1.9, il existe un élément $x$ dans $G$ tel que $t^x = h_0$. Alors $T^x \subseteq C(t)^x = C(h_0)$, d'où $T^x = T$, parce que $T$ est le seul 2-sous-groupe de Sylow de $C(h_0)$. On a donc $x \in N(T)$.

Le raisonnement ci-dessus montre aussi la

PROPOSITION 3.5. $T \cap T^x = \{1\}$ *pour tout* $x \in G - N(T)$.

PROPOSITION 3.6. $|N(T)| = 2^{\alpha+1}(2^\alpha - 1)(2^{\alpha+1} - 1)$.

En effet, d'après la proposition 3.4, tout élément dans $T - \{1\}$ se met sous la forme $h_0{}^x$ pour $x \in N(T)$. On a $h_0{}^x = h_0{}^y$ si, et seulement si, $xy^{-1} \in C(h_0)$, d'où $(N(T) : C(h_0)) = |T| - 1 = 2^{\alpha+1} - 1$. Alors notre assertion résulte de (3.1).

Le groupe $T$, étant distingué dans $C(h_0)$, est normalisé par $U_0$. Puisque $T$ est un 2-groupe élémentaire, et puisque $(|U_0|, 2) = 1$, on peut, en vertu de la réductibilité complète, mettre $T$ sous la forme $T = H_0 \times T_0$, où $T_0$ est un groupe normalisé par $U_0$. Par ailleurs, $C(h_0)/H_0$ étant un groupe de Frobenius, il est évident que $U_0$ opère, par l'application $t \to t^u$ (ou $t \in T$, $u \in U_0$), dans $T/H_0$, et par suite dans $T_0$, comme un groupe d'automorphismes sans point fixe. De plus, on a $|T_0| = 2^\alpha = |U_0| + 1$. Il en résulte que, pour un élément quelconque $\omega_0$ dans $T_0 - \{1\}$, tout élément de $T_0 - \{1\}$ se met sous la forme $\omega_0{}^u$ avec $u \in U_0$. Prenons dans ce qui suit comme $\omega_0$ un élément dans $T_0$ tel que $\omega\omega_0 \in H_0$. Alors $\omega_0$ est une involution distincte de $h_0$, et on a

$$C(h_0) \cap C(\omega_0) = C(h_0) \cap C(\omega).$$

Ceci dit, établissons la

PROPOSITION 3.7. *Soient $t_1$ et $t_2$ deux éléments distincts quelconques de $T - \{1\}$. Alors on a $C(t_1) \cap C(t_2) = T$.*

Démontrons d'abord notre assertion dans le cas spécial où $t_1 = h_0$ et $t_2 = \omega_0$. Soit $x \in C(h_0) \cap C(\omega_0)$. On a $C(h_0) = U_0 H_0 \cup U_0 H_0 \omega U_0$. Si $x$ est dans $U_0 H_0$, (1.14) montre que $x = h_0$. Si $x$ est dans $U_0 H_0 \omega U_0$, on a $x = u_1 h \omega_0 u_2$, où $u_i \in U$ $(i = 1, 2)$ et $h \in H_0$. De la condition $x \in C(\omega_0)$ on a $\omega_0 u_1 \omega_0 u_2 = u_1 \omega_0 u_2 \omega_0$. Par ailleurs, $T$ étant abélien, on a $\omega_0 u_1 \omega_0 u_1^{-1} = u_1 \omega_0 u_1^{-1} \omega_0$. On a donc

$$\omega_0 u_1 \omega_0 u_2 = \omega_0 u_1 \omega_0 u_1^{-1} u_1 u_2 = u_1 \omega_0 u_1^{-1} \omega_0 u_1 u_2 = u_1 \omega_0 u_2 \omega_0$$

et par suite $\omega_0 u_1 u_2 = u_1 u_2 \omega_0$, d'où $u_1 u_2 = 1$ en vertu de (1.14). Donc $x = u_1 h \omega_0 u_1^{-1} \in T$.

Démontrons maintenant notre assertion dans le cas général. D'après la proposition 3.4, on a $h_0 = t_1{}^a$ avec $a \in N(T)$. Posons $t = t_2{}^a$. Soit $x \in C(t_1) \cap C(t_2)$. Alors on a $x^a \in C(h_0) \cap C(t)$. Puisque $t \in T = T_0 \times H_0$, on a $t = t_0 h$ avec $t_0 \in T_0$ et $h \in H_0$. Alors on a $x^a \in C(h_0) \cap C(t_0)$. Comme on l'a vu plus haut, $t_0 \in T_0$ se met sous la forme $\omega_0{}^u$ avec $u \in U_0$. Donc $x^a \in C(h_0)$

$\cap C(\omega_0{}^u)$, d'où $ux^a u^{-1} \in C(h_0) \cap C(\omega_0)$, parce que $u \in U_0 \subseteq C(h_0)$. Alors, d'après ce que nous avons montré ci-dessus, on a $ux^a u^{-1} \in T$, d'où $x^a \in T$ et $x \in T$, parce que $u$ et $a$ sont tous deux dans $N(T)$.

COROLLAIRE 3.8. $C(T) = T$.

PROPOSITION 3.9. *$N(T)$ ne contient aucun sous-groupe distingué, sauf $\{1\}$, de $G$.*

En effet, soit $D \subseteq N(T)$ un sous-groupe distingué de $G$. Supposons $|D|$ pair. Alors $D$ contient une involution $t$. On a $t^x \in D \subseteq N(T)$ pour tout $x \in G$. $T$ étant le seul 2-sous-groupe de Sylow de $N(T)$, il résulte que $t^x \in T$ pour tout $x \in G$. Alors $T \cap T^x = \{1\}$, et on a, en vertu de la proposition 3.5, $x \in N(T)$ pour tout $x \in G$, d'où $N(T) = G$, ce qui est une contradiction avec (3.3) et avec la proposition 3.6. On peut donc conclure que $|D|$ est impair. Alors $D \cap T = \{1\}$, et il en résulte que $D$ centralise $T$, parce que $D$ et $T$ sont tous deux distingués dans $N(T)$. Alors, d'après le corollaire 3.8, $D \subseteq T$, d'où $D = \{1\}$, parce que $|D|$ est impair.

PROPOSITION 3.10. *Soit $a$ un élément quelconque de $G - N(T)$. Alors tout conjugué de $T$, sauf $T$ lui-même, dans $G$ se met d'une, et d'une seule, manière sous la forme $T^{at}$, pour $t$ parcourant $T$.*

En effet, d'après (3.3) et la proposition 3.6, il y a $2^{\alpha+1} + 1$ conjugués de $T$ dans $G$. D'abord, il est clair que $T^{at} \neq T$ pour tout $t \in T$. Il suffit donc de montrer que $T^{at} = T^{at'}$, où $t, t' \in T$, implique $t = t'$. Or, on a $t't^{-1} \in N(T^a)$, d'où $t't^{-1} \in T^a \cap T$ et $t't^{-1} = 1$, parce que la proposition 3.5 montre que $T^a \cap T = \{1\}$.

Associons à tout élément $x$ dans $G$ la permutation $T^y \to T^{yx}$ de l'ensemble des conjugués de $T$ dans $G$. On obtient ainsi une réalisation de $G$ comme un groupe de permutations de l'ensemble des $2^{\alpha+1} + 1$ conjugués de $T$ dans $G$; cette réalisation de $G$ est fidèle en vertu de la proposition 3.9. Montrons maintenant la

PROPOSITION 3.11. *La réalisation fidèle, définie ci-dessus, de $G$ comme un groupe de permutations d'un ensemble de $2^{\alpha+1} + 1$ lettres possède les propriétés suivantes :*

(i) *$G$ est triplement transitif;*

(ii) *aucune permutation, sauf l'identité, dans $G$ ne laisse invariantes plus de 3 lettres;*

(iii) *$G$ n'est pas exactement triplement transitif;*

(iv) *le sous-groupe $G_1$ formé de la totalité des permutations dans $G$ qui laissent invariante une lettre donnée quelconque possède un sous-groupe distingué d'ordre $2^{\alpha+1}$ de $G_1$.*

Prenons un élément $a$ dans $G - N(T)$. D'après la proposition 3.10, tout conjugué $\neq T$ de $T$ dans $G$ se met sous la forme $T^{at}$, où $t \in T$.

Démontrons d'abord que $G$ est doublement transitif. Il suffit de montrer

que pour deux conjugués distincts quelconques $T_1$ et $T_2$ de $T$ on peut trouver un élément $x$ dans $G$ tel que $T^x = T_1$, $T^{ax} = T_2$. $G$ étant evidemment transitif, on peut supposer sans nuire à la généralité que $T_1 = T$. Alors $T_2$ se met sous la forme $T^{at}$ pour $t \in T$, parce que $T_2 \neq T_1 = T$. Alors on peut prendre $t$ comme $x$.

$G$ étant doublement transitif, le groupe

$$S = \{x \in G | T^x = T, T^{ax} = T^a\} = N(T) \cap N(T)^a$$

est d'ordre $|G|/(2^{\alpha+1} + 1)2^{\alpha+1} = (2^\alpha - 1)(2^{\alpha+1} - 1)$. Il en résulte de la proposition 3.6 que $N(T) = ST$, $S \cap T = \{1\}$, et, compte tenu de la proposition 3.4, on voit que tout élément de $T - \{1\}$ se met sous la forme $h_0^s$ avec $s \in S$.

Ceci dit, démontrons maintenant que $G$ est triplement transitif. Il suffit de montrer que pour trois conjugués distincts quelconques $T_1$, $T_2$ et $T_3$ de $T$ on peut trouver un élément $x$ dans $G$ tel que $T^x = T_1$, $T^{ax} = T_2$, $T^{ah_0x} = T_3$. $G$ étant doublement transitif, on peut supposer sans nuire à la généralité que $T_1 = T$, $T_2 = T^a$. Alors, d'après la proposition 3.10, $T_3$ s'écrit sous la forme $T^{at}$ avec un $t \in T - \{1\}$. Alors on peut prendre comme $x$ un élément $s$ dans $S$ tel que $h_0^s = t$, ce qui est toujours possible comme on vient de voir ci-dessus.

Démontrons (ii). Soient $T_i$ $(1 \leqslant i \leqslant 4)$ quatre conjugués distincts de $T$, et soit $x$ un élément dans $G$ tel que $T_i^x = T_i$ $(1 \leqslant i \leqslant 4)$; nous allons démontrer que $x = 1$. $G$ étant triplement transitif, il suffit de considérer le cas où $T_1 = T$, $T_2 = T^a$, et $T_3 = T^{ah_0}$. Alors, d'après la proposition 3.10, $T_4$ se met sous la forme $T^{at}$ avec $t \in T - H_0$. Alors, les relations $T_i^x = T_i$ $(i = 1, 2)$ impliquent d'abord que $x \in S$. Ecrivons $h_0^x = t_1$, $t^x = t_2$. Puisque $x \in S \subseteq N(T)$, on a $t_i \in T$ $(i = 1, 2)$. Or, les relations $T_i^x = T_i$ $(i = 3, 4)$ deviennent $T^{at_1} = T^{ah_0}$ et $T^{at_2} = T^{at}$. Il en résulte de la proposition 3.10 que $t_1 = h_0$ et $t_2 = t$. Autrement dit, on a $h_0^x = h_0$ et $t^x = t$, donc $x \in T$ en vertu de la proposition 3.7. On a donc $x \in S \cap T = \{1\}$, $x = 1$.

(iii) suit immédiatement de (3.3), et (iv) suit du fait que $N(T)$ possède le sous-groupe distingué $T$ d'ordre $2^{\alpha+1}$.

La proposition 3.11 nous permet d'appliquer à $G$ un théorème de Feit qui a déterminé tous les groupes de permutations satisfaisant aux conditions (i)–(iv) de la proposition 3.11. D'après Feit, un tel groupe est isomorphe au groupe designé par $P_r$ dans **(3**, p. 185**)**, où $r = \alpha + 1$ est un nombre premier. De plus, $P_r$ est d'ordre $r(2^r - 1)2^r(2^r + 1)$. Comparant cet ordre avec celui de $G$ donné dans (3.3), on déduit que $\alpha = 2$, $r = 3$. Puisque le groupe $G_0$ mentionné dans l'introduction satisfait à la condition $(H : H_0) = 1$ ainsi qu'aux (0.1)–(0.4), on conclut que $G_0 \cong P_3$. De plus, (3.3) montre que $m = 3^3$ et $|G| = 2^3 \cdot 3 \cdot 7 \cdot 3^2$. On a donc le

THÉORÈME 3.12. *Si* $(H : H_0) = 1$, *on a* $m = 3^3$, $|G| = 3^3(3 - 1)(3^3 + 1)$, *et* $G \cong G_0$.

**4. Le cas** $(H:H_0) > 1$. Dès maintenant nous supposerons toujours que $(H : H_0) > 1$, même sans le spécifier. Dans ce numéro, nous montrerons que $C(h_0) = L \times H_0$, où $L$ est un groupe isomorphe à $\mathrm{PSL}(2, q)$, et en tirerons quelques conséquences. Citons d'abord un lemme, dû à Wielandt, dont nous allons faire usage dans ce qui suit.

LEMME 4.1 **(4, Lemme 1).** *Soient $X$ et $Y$ deux sous-groupes finis d'un groupe, et soit $X$ résoluble. Supposons que $X$ normalise $Y$ et que $(|X|, |Y|) = 1$. Alors, pour chaque diviseur premier $p$ de $|Y|$, $X$ normalise un $p$-sous-groupe de Sylow de $Y$.*

D'après la proposition 1.26, le groupe $C(h_0)/H_0$ se réalise comme un groupe de permutations doublement transitif de l'ensemble de $q + 1$ lettres tel que aucune permutation, sauf l'identité, dans $C(h_0)/H_0$ ne laisse invariantes plus de 2 lettres. Montrons la

PROPOSITION 4.2. *$C(h_0)/H_0$ ne possède pas de sous-groupe distingué d'ordre $q + 1$.*

En effet, on va tirer une contradiction en supposant le contraire. Supposons donc que $C(h_0)/H_0$ possède un sous-groupe distingué d'ordre $q + 1$. D'après (iii) de la proposition 1.26, l'hypothèse $(H : H_0) > 1$ implique que $C(h_0)/H_0$ n'est pas exactement doublement transitif. D'après un théorème de Feit, $G$ est alors isomorphe au groupe noté par $A_\alpha$ dans **(3**, p. 184**)**, $\alpha$ étant un nombre premier tel que $q + 1 = 2^\alpha$. Puisque

$$|A_\alpha| = \alpha 2^\alpha (2^\alpha - 1) \quad \text{et} \quad |C(h_0)/H_0| = q(q+1)(H : H_0),$$

il en résulte que

$$(H : H_0) = \alpha, \qquad |C(h_0)| = \alpha 2^{\alpha+1}(2^\alpha - 1). \tag{4.2.1}$$

D'après la proposition 2.3, $(H : H_0)$ est impair. Donc $\alpha$ est un nombre premier impair. (4.2) montre alors que $H$ est cyclique.

$A_\alpha$ est le groupe formé de toutes les permutations de la forme $x \to ax^\theta + b$, où : $a$, $b$ et $x$ parcourent le corps $F_{q+1}$ de $2^\alpha$ $(=q+1)$ éléments; $a \neq 0$; $\theta$ parcourt tous les automorphismes de $F_{q+1}$. Les permutations $x \to x^\theta$ sont exactement celles dans $A_\alpha$ qui laissent invariants 0 et 1 de $F_{q+1}$, et la permutation $x \to x + 1$ est une involution permutant 0 et 1. En vertu de la proposition 1.26, ces propriétés de $A_\alpha$ s'expriment dans $C(h_0)/H_0$ comme suit: l'élément $\omega H_0 \in C(h_0)/H_0$ centralise $H/H_0$. Il en résulte que $\omega$ centralise $H$, donc que $H\omega$ ne contient que 2 involutions (à savoir, $\omega$ et $h_0\omega$). Alors la proposition 1.27 montre que $m = (2q + 3)q$, et par conséquent on a

$$|G| = \alpha 2^{\alpha+1}(2^\alpha - 1)(2^{\alpha+1} - 1)(2^{\alpha+1} + 1) \tag{4.2.2}$$

en vertu de (1.5) et (4.2.1).

Soit $H_1$ le sous-groupe d'ordre $\alpha$ de $H$. Alors on a

$$N(H_1) = C(H_1) = H \cup H\omega. \tag{4.2.3}$$

https://doi.org/10.4153/CJM-1964-077-2 Published online by Cambridge University Press

En effet, soit $h_1$ un générateur de $H_1$, et soit $x \in N(H_1)$. Si $x$ est dans $UH$, écrivons $x = uh$ avec $u \in U$ et $h \in H$. Alors la relation $h_1 x = x h_1^r$ implique $u^{h_1} = u$, d'où $u = 1$, car $h_1$ est dans $H - H_0$; par conséquent on a $x = h \in H$. Si $x$ est dans $UH\omega U$, écrivons $x = u_1 h \omega u_2$, où $u_i \in U$ $(i = 1, 2)$ et $h \in H$. Alors la relation $h_1 x = x h_1^r$ implique que $h_1 u_i h_1^{-1} = u_i$, et par suite on a $u_i = 1$ $(i = 1, 2)$, d'où $x = h\omega \in H\omega$. En résumé, on a $C(H_1) \subseteq N(H_1) \subseteq H \cup H\omega$. En outre, il est clair que $H \cup H\omega \subseteq C(H_1)$, d'où (4.2.3).

Lorsque $\alpha \neq 3, 5$, on voit aisément de (4.2.2) que $H_1$ est un $\alpha$-sous-groupe de Sylow de $G$; et d'après Burnside **(2**, p. 327**)** (4.2.3) implique que $G$ possède un sous-groupe distingué $G_1$ d'ordre

$$2^{\alpha+1}(2^\alpha - 1)(2^{\alpha+1} - 1)(2^{\alpha+1} + 1).$$

De plus, d'après le lemme 4.1, $G_1$ possède, pour tout nombre premier $p \neq \alpha$, un $p$-sous-groupe de Sylow $S_p$ normalisé par $H_1$. Puisque $H_1$ est un groupe cyclique engendré par $h_1$, (4.2.3) montre que $|C(h_1)| = 4\alpha$; il en résulte que si $p \neq 2$, $H_1$ induit un groupe d'automorphismes sans point fixe de $S_p$, d'où $|S_p| \equiv 1 \pmod{\alpha}$. Ceci étant pour tout diviseur premier $p \neq 2$ de $|G_1|$, on a

$$(2^\alpha - 1)(2^{\alpha+1} - 1)(2^{\alpha+1} + 1) \equiv 0 \pmod{\alpha},$$

d'où $\alpha = 7$. Alors $|G_1| = 2^8 \cdot 3 \cdot 5 \cdot 17 \cdot 127 \cdot 257$, et on voit que $p = 3$ ne satisfait pas à $|S_p| \equiv 1 \pmod{\alpha}$. Il reste donc à considérer le cas où $\alpha = 3$ ou 5.

D'après (4.2.2) on a

$$|G| = \begin{cases} 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 & (\text{si } \alpha = 3), \\ 2^6 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 31 & (\text{si } \alpha = 5). \end{cases}$$

Il en résulte que les $\alpha$-sous-groupes de Sylow de $G$ ont l'ordre $\alpha^2$; ils sont alors abéliens. Mais c'est une contradiction avec la relation $|C(H_1)| = 4\alpha$, parce que $\alpha \neq 2$. La proposition 4.2 est démontrée.

D'après la proposition 1.26, l'hypothèse $(H : H_0) > 1$ implique que $C(h_0)/H_0$ n'est pas exactement doublement transitif. Alors, d'après la proposition 4.2 et les théorèmes de Feit **(3**, Théorème 1**)** et Ito **(5)**, on peut conclure que $q$ est une puissance d'un nombre premier impair et que l'indice $(H : H_0)$ est égale soit à $\frac{1}{2}(q - 1)$, soit à $q - 1$; la dernière possibilité s'écarte parce que $(H : H_0)$ est impair en vertu de la proposition 2.3. On a donc

$$|H| = q - 1, \qquad q \equiv -1 \pmod{4}. \tag{4.3}$$

La proposition 1.26 et (4.3) montrent alors que $C(h_0)/H_0$ est isomorphe à $\mathrm{PSL}(2, q)$ **(**voir **1**, p. 739**)**. Puisque $C(h_0)$ contient plus d'une involution, il en résulte du lemme 2.1 que $C(h_0) = L \times H_0$, où $L$ est un groupe isomorphe à $\mathrm{PSL}(2, q)$. En outre, l'hypothèse $(H : H_0) > 1$ et (4.3) montrent que $q > 3$, et il s'ensuit que $L$ est simple. Désignant par $C'(h_0)$ le groupe dérivé de $C(h_0)$, on a donc $C(h_0) = C'(h_0) \times \langle h_0 \rangle$. Puisque toutes les involutions dans $G$ sont conjuguées mutuellement dans $G$, on a la

PROPOSITION 4.4. *Si* $(H : H_0) > 1$, *pour toute involution* $\tau$ *dans* $G$, *on a* $C(\tau) = C'(\tau) \times \langle\tau\rangle$, *où* $C'(\tau)$ *désigne le groupe dérivé de* $C(\tau)$; $C'(\tau)$ *est isomorphe à* $\mathrm{PSL}(2, q)$.

Puisque $C(h_0)/H_0$ est isomorphe à $\mathrm{PSL}(2, q)$, on voit, d'après la proposition 1.26, que $H/H_0$ est cyclique et que $h^\omega = h^{-1}$ pour tout élément $h$ dans $H$. Il en résulte que $H$ est cyclique et que $H = H_1 \times H_0$, où $H_1$ est un groupe d'ordre impair $\frac{1}{2}(q-1)$. $H_1$ étant caractéristique dans $H$, on a $H_1{}^\omega = H_1$ et par suite $h^\omega = h^{-1}$ pour tout $h \in H$. On a donc la

PROPOSITION 4.5. *$H$ est cyclique, et on a $h^\omega = h^{-1}$ pour tout $h$ dans $H$.*

PROPOSITION 4.6. $|U| = q^3$, $|G| = q^3(q-1)(q^3+1)$.

En effet, la proposition 4.5 montre que tout élément dans $H\omega$ est une involution. Puisque on a $|H| = q - 1$ d'après (4.3), il résulte de la proposition 1.27 que $m = q^3$. La deuxième partie de la proposition 4.6 est alors immédiate de (1.5) et de (4.3).

PROPOSITION 4.7. $q \equiv 3 \pmod 8$.

En effet, soit $\tau$ une involution dans $G$. D'après la proposition 4.4, on a $C(\tau) = C'(\tau) \times \langle\tau\rangle$. Soit $\tau'$ une involution dans $C'(\tau)$. Alors,

$$C(\tau) \cap C(\tau') = (C'(\tau) \cap C(\tau')) \times \langle\tau\rangle.$$

Puisque $C'(\tau)$ est isomorphe à $\mathrm{PSL}(2, q)$, avec $q \equiv -1 \pmod 4$, $C'(\tau) \cap C(\tau')$ est un groupe dihédral d'ordre $q+1$, contenant $\tau'$ dans son centre. Si $\frac{1}{4}(q+1)$ était pair, il y aurait un élément $x$ dans $C'(\tau) \cap C(\tau')$ tel que $x^2 = \tau'$. Par ailleurs, on a $C(\tau') = C'(\tau') \times \langle\tau'\rangle$ d'après la proposition 4.4. Puisque $x \in C(\tau')$, on aurait $x^2 \in (\tau')$, c'est-à-dire, $\tau' \in C'(\tau')$, ce qui est absurde. L'entier $\frac{1}{4}(q+1)$ est donc impair, donc notre assertion.

**5. 2-sous-groupes de Sylow de $G$.** Dans ce numéro on établira quelques propriétés des 2-sous-groupes de Sylow de $G$. On supposera toujours que $(H : H_0) > 1$.

PROPOSITION 5.1. *Les 2-sous-groupes de Sylow de $G$ sont élémentaires, et ont l'ordre* 8.

En effet, soit $\tau$ une involution dans $G$. D'après la proposition 4.4, $C(\tau) = C'(\tau) \times \langle\tau\rangle$, $C'(\tau)$ étant isomorphe à $\mathrm{PSL}(2, q)$. Puisque $q \equiv 3 \pmod 8$ d'après la proposition 4.7, il en résulte que les 2-sous-groupes de Sylow de $C'(\tau)$ sont quatre-groupes. Il en résulte que les 2-sous-groupes de Sylow de $C(\tau)$, et par conséquent ceux de $G$, sont élémentaires, ayant l'ordre 8.

PROPOSITION 5.2. *Si $T$ est un 2-sous-groupe de Sylow de $G$, on a $C(T) = T$.*

En effet, soit $\tau \in T - \{1\}$; on a $C(\tau) = C'(\tau) \times \langle\tau\rangle$, et par suite $T = T_0 \times \langle\tau\rangle$, où $T_0 = T \cap C'(\tau)$ est un 2-sous-groupe de Sylow de $C'(\tau)$. $C'(\tau)$

étant isomorphe à $\mathrm{PSL}(2, q)$, le centralisateur de $T_0$ dans $C'(\tau)$ est $T_0$, d'où $C(T) = T_0 \times \langle\tau\rangle = T$.

PROPOSITION 5.3. *Soit $T$ un 2-sous-groupe de Sylow de $G$. Alors, pour tout élément $\tau$ dans $T - \{1\}$, il existe un élément d'ordre 3 dans $N(T) \cap C(\tau)$. De plus, $N(T)/C(T)$ est un groupe non-abélien d'ordre 21.*

En effet, on a $C(\tau) = C'(\tau) \times \langle\tau\rangle$ et $T = T_0 \times \langle\tau\rangle$, ou $T_0 = T \cap C'(\tau)$. $T_0$ étant un 2-sous-groupe de Sylow de $C'(\tau)$, il existe dans $C'(\tau)$ un élément d'ordre 3 qui normalise $T_0$, parce que $C'(\tau)$ est isomorphe à $\mathrm{PSL}(2, q)$.

Pour démontrer la deuxième partie de notre assertion, remarquons d'abord que $N(T)/C(T)$ est isomorphe à un sous-groupe du groupe linéaire général $\mathrm{GL}(3, 2)$ d'ordre $8 \cdot 3 \cdot 7$. Alors, le nombre $(N(T) : C(T))$, étant impair, est un diviseur de 21. Il est clair de la première partie de notre assertion que $N(T)/C(T)$ contient plus d'une sous-groupe d'ordre 3; donc $N(T)/C(T)$ est un groupe non-abélien d'ordre 21.

PROPOSITION 5.4. *Soit $T$ un 2-sous-groupe de Sylow de $G$. Alors on peut trouver une base $\{\tau_1, \tau_2, \tau_3\}$ de $T$ et deux éléments $a$ et $b$, d'ordres respectives 3 et 7, dans $N(T)$ tels que*

$$\tau_1{}^a = \tau_1, \qquad \tau_2{}^a = \tau_3, \qquad \tau_3{}^a = \tau_2\tau_3,$$

$$\tau_1{}^b = \tau_2, \qquad \tau_2{}^b = \tau_3, \qquad \tau_3{}^b = \tau_1\tau_2,$$

*et tels que $b^a = b^2$.*

En effet, soit $A$ un sous-groupe d'ordre 21 de $N(T)$, et soit $b$ un élément d'ordre 7 dans $A$. Alors, l'application $t \to t^b$ est un automorphisme de $T$ sans point fixe. Soit $\tau_1$ un élément quelconque de $T - \{1\}$. Posons $\tau_2 = \tau_1{}^b$, $\tau_3 = \tau_2{}^b$. Alors $\tau_2 \neq \tau_1$, et l'élément $\tau_3$ n'appartient pas au groupe $\langle\tau_1, \tau_2\rangle$, parce que $b$ ne peut normaliser aucun sous-groupe d'ordre 4 de $T$. De même, on a $\tau_3{}^b \in T - \langle\tau_2, \tau_3\rangle$. Donc $\{\tau_1, \tau_2, \tau_3\}$ est une base de $T$, et on a $\tau_3{}^b = \tau_1\tau$ avec $\tau \in \langle\tau_2, \tau_3\rangle$. Si $\tau = 1$, on aurait $b^3 \in A \cap C(T) = \{1\}$, ce qui est impossible. Si $\tau = \tau_2\tau_3$, on aurait $b^{-3}\tau_1 b^3 = \tau_1$, ce qui est aussi impossible, parce que $b$ est d'ordre 7. On a donc $\tau = \tau_2$ ou $\tau = \tau_3$. Montrons que l'on peut supposer sans nuire à la généralité que $\tau = \tau_2$. En effet, si $\tau = \tau_3$, on a

$$b^{-5}\tau_1 b^5 = \tau_1\tau_2, \qquad b^{-5}(\tau_1\tau_2)b^5 = \tau_1\tau_3, \qquad b^{-5}(\tau_1\tau_3)b^5 = \tau_1(\tau_1\tau_2),$$

ce qui montre que l'on peut prendre $\tau_1$, $\tau_1\tau_2$, $\tau_1\tau_3$ et $b^5$ au lieu de $\tau_1$, $\tau_2$, $\tau_3$ et $b$ respectivement. Supposons donc que $\tau = \tau_2$, c'est-à-dire que $\tau_3{}^b = \tau_1\tau_2$.

D'après la proposition 5.3, on peut trouver un élément $a$ d'ordre 3 dans $N(T) \cap C(\tau_1)$. Puisque $N(T) = TA$, $a$ se met sous la forme $ta$ avec $t \in T$, $a \in A$. Il est clair que $1 \neq a \in C(\tau_1)$. Puisque $a \in A$, l'ordre de $a$ est ou 3 ou 7. D'autre part, puisque $\tau_1{}^a = \tau_1$, $a$ ne peut être d'ordre 7. Donc $a$ est d'ordre 3. Or, on voit aisément que $\langle b\rangle$ est distingué dans $A$. $a$ étant d'ordre 3, on a soit $b^a = b^2$, soit $b^a = b^4$. Remplacant $a$ par $a^2$ si $b^a = b^4$, on peut

supposer que $b^a = b^2$. Alors ${\tau_1}^a = \tau_1$, ${\tau_2}^a = {\tau_1}^{ba} = {\tau_1}^{ab^2} = {\tau_1}^{b^2} = \tau_3$, ${\tau_3}^a = {\tau_2}^{ab^2} = {\tau_3}^{b^2} = \tau_2\tau_3$, d'où notre assertion.

PROPOSITION 5.5. *Soit $\tau$ une involution dans $G$, et soit $\tau'$ une involution dans $C'(\tau)$. Alors on a $\tau\tau' \in C'(\tau')$.*

Les éléments $\tau_i$ $(1 \leqslant i \leqslant 3)$, $a$ et $b$ étant comme dans la proposition 5.4, montrons d'abord que $\tau_2 \in C'(\tau_1)$ et que $\tau_1\tau_2 \in C'(\tau_2)$. On a en général $xx^a \in C'(\tau_1)$ pour tout $x$ dans $C(\tau_1)$. En effet, si $x \in C'(\tau_1)$, on a $x^a \in C'({\tau_1}^a) = C'(\tau_1)$, et par suite $xx^a \in C'(\tau_1)$. Si $x \in C(\tau_1) - C'(\tau_1)$, $x$ se met sous la forme $\tau_1 y$, où $y \in C'(\tau_1)$. Alors $xx^a = yy^a \in C'(\tau_1)$. En posant $x = \tau_3, \tau_2, \tau_3$, on voit que $\tau_2$ et $\tau_3$ sont dans $C'(\tau_1)$; on a alors $\tau_1\tau_2 = {\tau_3}^b \in C'({\tau_1}^b) = C'(\tau_2)$.

Démontrons maintenant la proposition 5.5. D'après la proposition 1.9, on peut supposer que $\tau = \tau_1$. Alors $\tau'$ et $\tau_2$ sont dans $C'(\tau_1)$, et par suite $\tau' = {\tau_2}^x$ avec $x \in C'(\tau_1)$, parce que $C'(\tau_1)$ est isomorphe à $\mathrm{PSL}(2, q)$. Donc, $\tau\tau' = (\tau_1\tau_2)^x \in C'({\tau_2}^x) = C'(\tau')$.

PROPOSITION 5.6. *Les notations étant comme dans la proposition* 5.4, *on a $\tau_3 \in C'(\tau_2)$ et $\tau_1\tau_2 \in C'(\tau_2) \cap C'(\tau_3)$.*

En effet, on a déjà vu que $\tau_1\tau_2 \in C'(\tau_2)$ et que $\tau_2$ et $\tau_3$ sont dans $C'(\tau_1)$. Alors on a $\tau_3 = {\tau_2}^b \in C'({\tau_1}^b) = C'(\tau_2)$ et $\tau_1\tau_2 = {\tau_3}^b \in C'({\tau_2}^b) = C'(\tau_3)$.

**6. Eléments d'ordre** $\frac{1}{4}(q+1)$. Nous démontrerons dans ce numéro que pour tout élément $s$ dans $G - \{1\}$ tel que $s^{(q+1)/4} = 1$ on a $|C(s)| = q + 1$. Nous en déduirons que $q = 3^{2n+1}$ avec un entier $n > 0$. Nous supposerons toujours que $(H : H_0) > 1$.

PROPOSITION 6.1. *Si $\tau$ et $\tau'$ sont deux involutions distinctes dans $G$ telles que $\tau\tau' = \tau'\tau$, le groupe dérivé de l'intersection $C(\tau) \cap C(\tau')$ est un groupe cyclique d'ordre* $\frac{1}{4}(q+1)$.

En effet, considérons d'abord le cas où $\tau' \in C'(\tau)$. On a

$$C(\tau) \cap C(\tau') = \langle\tau\rangle \times (C'(\tau) \cap C(\tau')),$$

et $C'(\tau) \cap C(\tau')$ est un groupe dihédral d'ordre $q+1$ contenant $\tau'$ dans son centre. Puisque $\frac{1}{4}(q+1)$ est impair, on en déduit que

$$C'(\tau) \cap C(\tau') = \langle\tau'\rangle \times D,$$

où $D$ est un groupe dihédral d'ordre $\frac{1}{2}(q+1)$. Soit $D = \langle S, \eta\rangle$, où $S$ est un groupe cyclique d'ordre $\frac{1}{4}(q+1)$, et où $\eta$ est une involution. On a alors

$$C(\tau) \cap C(\tau') = \langle\tau, \tau'\rangle \times \langle S, \eta\rangle,$$

d'où $S = (C(\tau) \cap C(\tau'))'$.

Considérons maintenant le cas où $\tau' \in C(\tau) - C'(\tau)$. On a alors $\tau\tau' \in C'(\tau)$ et $C(\tau) \cap C(\tau') = C(\tau) \cap C(\tau\tau')$. Il en résulte de ce que l'on vient de montrer que $(C(\tau) \cap C(\tau'))'$ est un groupe cyclique d'ordre $\frac{1}{4}(q+1)$.

PROPOSITION 6.2. *Soient $\tau$ et $\tau'$ deux involutions distinctes dans $G$ telles que $\tau\tau' = \tau'\tau$, et soit $S = (C(\tau) \cap C(\tau'))'$. On a alors*

$$C(s) = \langle \tau, \tau' \rangle \times S$$

*pour tout élément $s$ dans $S - \{1\}$.*

Remarquons tout d'abord que l'on peut se borner au cas où $\tau' \in C'(\tau)$: Si $\tau' \notin C'(\tau)$, on a $\tau\tau' \in C'(\tau)$, et

$$C(\tau) \cap C(\tau') = C(\tau) \cap C(\tau\tau'), \qquad \langle \tau, \tau' \rangle = \langle \tau, \tau\tau' \rangle.$$

Montrons maintenant qu'il suffit de considérer le cas spécial où $\tau = \tau_2$ et $\tau' = \tau_3$. En effet, d'après la proposition 1.9, on peut supposer que $\tau = \tau_2$. Alors $\tau'$ et $\tau_3$ sont tous deux dans $C'(\tau)$, en vertu de la proposition 5.6, et par suite on a $\tau' = \tau_3{}^x$ avec un élément $x$ dans $C'(\tau)$, parce que $C'(\tau)$ est isomorphe à $\mathrm{PSL}(2, q)$. On a donc

$$C(\tau) \cap C(\tau') = (C(\tau_2) \cap C(\tau_3))^x, \qquad \langle \tau, \tau' \rangle = \langle \tau_2, \tau_3 \rangle^x.$$

Supposons dès maintenant que $\tau = \tau_2, \tau' = \tau_3$. Par définition on a $S = (C(\tau_2) \cap C(\tau_3))'$. Puisque $C(\tau_2) = \langle \tau_2 \rangle \times C'(\tau_2)$, on a

$$C(\tau_2) \cap C(\tau_3) = \langle \tau_2 \rangle \times C'(\tau_2) \cap C(\tau_3)).$$

D'autre part, on a $C(\tau_3) = \langle \tau_3 \rangle \times C'(\tau_3)$. Puisque $\tau_3 \in C'(\tau_2)$ d'après la proposition 5.6, on a

$$C'(\tau_2) \cap C(\tau_3) = \langle \tau_3 \rangle \times (C'(\tau_2) \cap C'(\tau_3)),$$

d'où

$$C(\tau_2) \cap C(\tau_3) = \langle \tau_2, \tau_3 \rangle \times (C'(\tau_2) \cap C'(\tau_3)).$$

Puisque $C'(\tau_2) \cap C(\tau_3)$ est un groupe dihédral d'ordre $q + 1$, il en résulte que $C'(\tau_2) \cap C'(\tau_3)$ est un group dihédral d'ordre $\frac{1}{2}(q + 1)$ contenant $S$; d'après la proposition 5.6, on a $\tau_1\tau_2 \in C'(\tau_2) \cap C'(\tau_3)$, d'où

$$C'(\tau_2) \cap C'(\tau_3) = \langle S, \tau_1\tau_2 \rangle.$$

En particulier, on a

$$s^{\tau_1} = s^{-1} \qquad \text{pour tout } s \in S. \tag{6.2.1}$$

Il est clair que $\langle \tau_2, \tau_3 \rangle \times S \subseteq C(s)$; pour la démonstration de la proposition 6.2, il suffit donc de montrer que $|C(s)| = q + 1$. Montrons d'abord que

$$(|C(s)|, q) = 1. \tag{6.2.2}$$

En effet, on sait que $q$ est une puissance d'un nombre premier $q_0$. Si $(|C(s)|, q) > 1$, $C(s)$ contiendrait un élément $x$ d'ordre $q_0$. La proposition 4.6 montre que $U$ est un $q_0$-sous-groupe de Sylow de $G$, et par conséquent $x$ est conjugué à un élément dans $U - \{1\}$. Il en résulte de la proposition 1.17 que $|C(x)|$ est un diviseur de $q^3(q - 1)$. Puisque $s \in C(x)$, il en résulterait que l'ordre

de $s$ est un diviseur de $(q^3(q-1), \frac{1}{4}(q+1)) = 1$, ce qui est absurde. (6.2.2) est donc démontrée.

Montrons maintenant que

$$(|C(s)|, \tfrac{1}{2}(q-1)) = 1. \tag{6.2.3}$$

Sinon, en effet, il existerait un diviseur premier $p \neq 2$ de $q-1$ tel que $C(s)$ contienne un élément $x$ d'ordre $p$. Puisque $|H| = q-1$, la proposition 4.6 montre que $H$ contient un $p$-sous-groupe de Sylow de $G$. Il en résulte que $x$ est conjugué à un élément dans $H - \{1\}$. Le corollaire 1.20 montre alors que $|C(x)|$ est un diviseur de $2(q-1)$. Puisque $s$ est dans $C(x)$, il en résulterait que l'ordre de $s$ est un diviseur de $(2(q-1), \frac{1}{4}(q+1)) = 1$, ce qui est absurde.

Il résulte de la proposition 4.6, (6.2.2) et (6.2.3) que $|C(s)|$ est un diviseur de $2(q^3+1)$. Soit $C^*(s) = \{x \in G | s^x = s^{\pm 1}\}$. On a alors $(C^*(s) : C(s)) \leqslant 2$. D'après (6.2.1) on a $\tau_1 \in C^*(s) - C(s)$, d'où $(C^*(s) : C(s)) = 2$, ce qui montre que $|C(s)| \not\equiv 0 \pmod 8$ en vertu de la proposition 5.1. En outre, on a $q^3 + 1 \equiv 0 \pmod 4$. On peut conclure alors que

$$|C(s)| | (q^3+1) \tag{6.2.4}$$

et que $T_0 = \langle \tau_2, \tau_3 \rangle$ est un 2-sous-groupe de Sylow de $C(s)$.

Ecrivons dès maintenant $V = C(s)$, $C_0 = T_0 \times S$. $T_0$ étant un quatre-groupe, il est clair que $(N_V(T_0) : C_V(T_0)) = 1$ ou 3.

Montrons que $V = C_0$ si $(N_V(T_0) : C_V(T_0)) = 1$. Dans ce cas, $V$ possède, d'après Burnside **(2**, p. 327**)**, un 2-complément $W$ distingué dans $V$. D'après le lemme 4.1, pour tout diviseur premier $p$ de $|W|$ il existe un $p$-sous-groupe de Sylow $P$ de $W$ normalisé par $T_0$. $T_0$, étant un quatre-groupe, contient alors un élément $\tau \neq 1$ qui centralise un élément dans $P - \{1\}$. Il en résulte que $p$ est un diviseur de $|C(\tau)| = |C(h_0)| = q(q^2-1)$. Puisque $p$ est un diviseur de $q^3+1$ en tant que diviseur de $|V|$ (voir (6.2.4)), il en résulte que $p$ est un diviseur de $q+1$. Si $q+1 \not\equiv 0 \pmod 3$, on a $(q+1, q^2-q+1) = 1$, donc $|W|$ est un diviseur de $\frac{1}{4}(q+1)$. Par conséquent, $|V|$ est un diviseur de $q+1$, d'où $|V| = q+1$, $V = C_0$. Si $q+1 \equiv 0 \pmod 3$, on a $(q+1, q^2-q+1) = 3$. De plus, il est facile de voir que $q^2-q+1 \not\equiv 0 \pmod 9$. Il en résulte du raisonnement ci-dessus que $|V|$ est un diviseur de $3(q+1)$. Donc on a $|V| = 3(q+1)$ si $V \neq C_0$. On va tirer une contradiction de l'hypothèse $V \neq C_0$. Soit $3^\alpha$ la plus grande puissance de 3 divisant $q+1$. Alors $3^{\alpha+1}$ est la plus grande puissance de 3 divisant $|W|$. Soit $P_0$ un 3-sous-groupe de Sylow, d'ordre $3^\alpha$, de $C_0$, et soit $P_1$ un 3-sous-groupe de Sylow de $W$ contenant $P_0$. Alors $P_0$ est distingué dans $P_1$, parce que $(P_1 : P_0) = 3$. $P_0$ est distingué aussi dans $C_0$, parce que $C_0$ est abélien. Par ailleurs, la relation $|V| = 3(q+1)$ montre que $C_0$ et $P_1$ engendrent $V$; il en résulte que $P_0$ est distingué dans $V$, et par conséquent $P_0$ est contenu dans tous les 3-sous-groupes de Sylow de $V$. D'après le lemme 4.1, il y a un 3-sous-groupe de

Sylow $P$ de $W$ normalisé par $T_0$. On a alors $P_0 \subseteq P$, et $T_0$ opère, par l'application $x \to x^\tau$ (où $x \in P$, $\tau \in T_0$), dans le groupe $P/P_0$ d'ordre 3. $T_0$, étant un quatre-groupe, contient donc un élément $\tau \neq 1$ dont l'opération dans $P/P_0$ est triviale. Soit $c$ un élément quelconque dans $P - P_0$. Alors on a $c^\tau = cx$ avec $x$ dans $P_0$, et par suite $c = c^\tau x$, $x^2 = 1$, $x = 1$, et $c^\tau = c$. Il en résulte que $\tau$ centralise $P$; autrement dit, on a $|C(\tau)| \equiv 0 \pmod{3^{\alpha+1}}$. Puisque $|C(\tau)| = |C(h_0)| = q(q^2 - 1)$, on a $q(q^2 - 1) \equiv 0 \pmod{3^{\alpha+1}}$, ce qui est évidemment impossible. On a donc $V = C_0$.

Considérons maintenant le cas où

$$(N_V(T_0) : C_V(T_0)) = 3. \tag{6.2.5}$$

On va montrer d'abord que la condition (6.2.5) implique que $|V| = 3(q + 1)$. De (6.2.5) il résulte que $|V| \equiv 0 \pmod 3$, d'où, en vertu de (6.2.4), on a $q^3 + 1 \equiv 0 \pmod 3$ et enfin

$$q + 1 \equiv 0 \pmod 3. \tag{6.2.6}$$

Puisque $C_V(\tau_2) = V \cap C(\tau_2)$, il est clair que $|C_V(\tau_2)|$ est un diviseur de $(q^3 + 1, q(q^2 - 1)) = q + 1$. De plus on a $C_0 \subseteq C_V(\tau_2)$. Il en résulte que

$$C_V(\tau_2) = C_0. \tag{6.2.7}$$

Le quatre-groupe $T_0$ étant un 2-sous-groupe de Sylow de $V$, (6.2.5) et (6.2.7) impliquent, d'après Gorenstein et Walter **(4)**, que $V$ possède un sous-groupe distingué $N$ d'ordre impair tel que $V/N$ soit isomorphe à $\mathrm{PSL}(2, r)$, où $r$ est une puissance d'un nombre premier telle que $r \equiv 3 \pmod 8$. Le centralisateur dans $\mathrm{PSL}(2, r)$ d'un 2-sous-groupe de Sylow de $\mathrm{PSL}(2, r)$ étant le sous-groupe lui-même, on a

$$S \subseteq N. \tag{6.2.8}$$

D'après le lemme 4.1, $N$ possède, pour chaque diviseur premier $p$ de $|N|$, un $p$-sous-groupe de Sylow $P$ de $N$ normalisé par $T_0$. $T_0$, étant un quatre-groupe, contient alors un élément $\tau \neq 1$ qui centralise un élément dans $P - \{1\}$. Il en résulte que $p$ est un diviseur de

$$(q^3 + 1, q(q^2 - 1)) = q + 1.$$

Puisque $(q + 1, \frac{1}{3}(q^2 - q + 1)) = 1$, on a $(|N|, \frac{1}{3}(q^2 - q + 1)) = 1$. De plus, $|N|$ est un diviseur de $q^3 + 1$. Il en résulte que $|N|$ est un diviseur de $3(q + 1)$. Par ailleurs, on a $(V : N) = |\mathrm{PSL}(2, r)| \equiv 0 \pmod 3$. Il en résulte que $|N|$ est un diviseur de $q + 1$. Alors (6.2.8) implique que

$$N = S. \tag{6.2.9}$$

Or, le centralisateur d'une involution dans $\mathrm{PSL}(2, r)$ est d'ordre $r + 1$. Considérons donc le centralisateur de l'involution $\tau_2 N$ dans $V/N$. Soit $x$ un élément dans $V$ tel que $x^{-1}x^{\tau_2} \in N$. Puisque on a $N \subseteq C(\tau_2)$ d'après (6.2.9), l'élément $y = x^{-1}x^{\tau_2}$ satisfait $y^{\tau_2} = y = y^{-1}$ et $y^2 = 1$, d'où $y = 1$ parce que

$|N|$ est impair. Autrement dit, on a $x \in C_V(\tau_2)$. On a donc $x \in C_0$ d'après (6.2.7). Il en résulte que $C_{V/N}(\tau_2 N) = C_0/N$, d'où $|C_{V/N}(\tau_2 N)| = |C_0/S| = 4$. On a donc $r + 1 = 4$, $r = 3$, d'où $|V/N| = |P(2, 3)| = 12$. Compte tenu de (6.2.9), on a donc

$$|V| = 3(q + 1). \tag{6.2.10}$$

Supposant encore (6.2.5), on va montrer que $V = \langle C_0, a\rangle$, $a$ étant l'élément donné dans la proposition 5.4. D'après (6.2.5), il y a un élément $c$ dans $V$ tel que

$$\tau_2{}^c = \tau_3, \qquad \tau_3{}^c = \tau_2\,\tau_3. \tag{6.2.11}$$

Il est clair que $c$ normalise

$$C(\tau_2) \cap C(\tau_3) = T_0 \times \langle S, \tau_1\tau_2\rangle.$$

Puisque

$$T = \langle \tau_1, \tau_2, \tau_3\rangle \subseteq C(\tau_2) \cap C(\tau_3),$$

on a $T^c \subseteq C(\tau_2) \cap C(\tau_3)$, et par conséquent on a $T^{cx} = T$ avec un élément $x$ dans $C(\tau_2) \cap C(\tau_3)$. On voit aisément que l'élément $x$ dans $C(\tau_2) \cap C(\tau_3)$ se met sous la forme $yt$, où $y \in S$ et $t \in T$. On a $T^{cy} = T$, et ${\tau_i}^c = {\tau_i}^{cy}$ $(i = 2, 3)$. Utilisant $cy \in V$ au lieu de $c$, on voit que $V$ contient un élément $c$ satisfaisant à (6.2.11) ainsi qu'à $T^c = T$. Alors l'élément $z = ca^{-1} \in N(T)$ satisfait à ${\tau_i}^z = \tau_i$ $(i = 2, 3)$, d'où il résulte que ${\tau_1}^z = \tau_1\,\tau$ avec $\tau \in T_0 = \langle \tau_2, \tau_3\rangle$. Si $\tau \neq 1$, $zT$ serait un élément d'ordre 2 dans $N(T)/T$, ce qui est impossible, parce que $N(T)/T$ est d'ordre 21. On a donc $\tau = 1$, d'où $z \in T$ en vertu de la proposition 5.2. Montrons que $z \in T_0$. Sinon, on aurait $z \in T_0\,\tau_1$, et par suite $\tau_1\,a \in V$. On aurait alors $\tau_1 = (\tau_1\,a)^3 \in V$, ce qui est impossible en vertu de (6.2.1). On a donc $z \in T_0$, d'où $a \in V$. D'après la proposition 5.4, il est clair que $a$ normalise $C(\tau_2) \cap C(\tau_3)$. Donc $a$ normalise $S = (C(\tau_2) \cap C(\tau_3))'$ et $C_0 = T_0 \times S$. $a$ n'est pas dans $C_0$, parce que $a$ ne centralise pas $\tau_2$. On a donc $|\langle C_0, a\rangle| = 3(q+1)$. Puisque $\langle C_0, a\rangle \subseteq V$, il résulte de (6.2.10) que $V = \langle C_0, a\rangle$. On a démontré que l'hypothèse (6.2.5) implique que $C(s) = \langle C_0, a\rangle$ pour tout élément $s$ dans $S - \{1\}$.

En résumé, on conclut que si $s \in S - \{1\}$ on a soit $C(s) = C_0$ soit $C(s) = \langle C_0, a\rangle$, et que la deuxième possibilité peut se réaliser seulement si $q + 1 \equiv 0 \pmod 3$. Donc la démonstration de la proposition 6.2 sera complète lorsqu'on aura montré que $q + 1 \not\equiv 0 \pmod 3$. Nous allons déduire une contradiction en supposant que $q + 1 \equiv 0 \pmod 3$. Or, on a $|S| = \frac{1}{4}(q + 1) \equiv 0 \pmod 3$, et $S$ contient un élément $s_0$ d'ordre 3 centralisé par $a$. On a $s_0 \in S \subseteq C'(\tau_2)$. D'autre part, on a $a \in C'(\tau_1)$. En effet on a $a \in C(\tau_1)$, $a^3 = 1$, et $(C(\tau_1) : C'(\tau_1)) = 2$, d'où $a \in C'(\tau_1)$. $\tau_1$ et $\tau_2$ étant conjuguées dans $G$, les deux groupes $C'(\tau_1)$ et $C'(\tau_2)$ sont conjugués dans $G$. De plus, $C'(\tau_1)$ étant isomorphe à $\mathrm{PSL}(2, q)$, les 3-sous-groupes de Sylow de $C'(\tau_1)$ sont cycliques. Il en résulte que $a$ est conjugué soit à $s_0$, soit à $s_0{}^2$. Par ailleur, il est clair que

$$\langle C_0, a\rangle \subseteq C(s_0) = C(s_0{}^2),$$

https://doi.org/10.4153/CJM-1964-077-2 Published online by Cambridge University Press

d'où $C(s_0) = C(s_0^2) = \langle C_0, a\rangle$. On a donc

$$C(a) \cong \langle C_0, a\rangle. \tag{6.2.12}$$

Montrons maintenant que le 2-sous-groupe de Sylow $T_0$ de $\langle C_0, a\rangle$ est caractéristique dans $\langle C_0, a\rangle$. En effet, les relations $\tau_2^{-1}\tau_2^a = \tau_2\tau_3$ et $\tau_3^{-1}\tau_3^a = \tau_2$ montrent que $T_0$ est contenu dans le groupe dérivé $\langle C_0, a\rangle'$ de $\langle C_0, a\rangle$. Le groupe $\langle C_0, a\rangle'$ étant abélien et $T_0$ étant un 2-sous-groupe de Sylow de $\langle C_0, a\rangle'$, on voit que $T_0$ est caractéristique dans $\langle C_0, a\rangle'$. Donc $T_0$ est caractéristique dans $\langle C_0, a\rangle$. Alors (6.2.12) montre que $C(a)$ possède un et un seul 2-sous-groupe de Sylow $T_1$. Puisque $\tau_1 \in C(a)$, on a $\tau_1 \in T_1$. En outre on a $s_0 \in C(a)$, et par suite $\tau_1 s_0^2 = s_0^{-1}\tau_1 s_0 \in T_1$, d'où $s_0^2 \in T_1$, ce qui est évidemment impossible, parce que $s_0^2$ est d'ordre 3. C'est une contradiction déduite de l'hypothèse que $q + 1 \equiv 0 \pmod 3$. On a donc $q + 1 \not\equiv 0 \pmod 3$, et la proposition 6.2 est démontrée.

COROLLAIRE 6.3. *Les notations étant comme dans la proposition* 5.4, *l'application* $x \to x^a$ *est un automorphisme sans point fixe de* $S = (C(\tau_2) \cap C(\tau_3))'$.

COROLLAIRE 6.4. $q = 3^{2n+1}$ *pour un entier* $n > 0$.

En effet, le corollaire 6.3 implique que $|S| = \frac{1}{4}(q + 1) \equiv 1 \pmod 3$, d'où $q \equiv 0 \pmod 3$. $q$ étant une puissance d'un nombre premier telle que $q \equiv 3 \pmod 8$, on a $q = 3^{2n+1}$ avec un entier $n > 0$.

**7. Les "axiomes" de Ward.** En essayant de caractériser les groupes $G_1, G_2, \ldots$ mentionnés dans l'introduction par quelques-unes de leurs propriétés, et en même temps de calculer leurs caractères, H. N. Ward **(8)** a considéré les groupes finis $G$ satisfaisants aux "axiomes" suivants :

(7.1) les 2-sous-groupes de Sylow de $G$ sont élémentaires, et ont l'ordre 8;

(7.2) $G$ ne possède aucun sous-groupe d'indice 2;

(7.3) $G$ contient une involution $\tau$ telle que $C(\tau)/\langle\tau\rangle$ soit isomorphe à $\mathrm{PSL}(2, q)$, où $q$ est une puissance d'un nombre premier telle que $q \geqslant 27$, $q \equiv 3 \pmod 8$.

(7.4) si $x$ est un élément dans $C(\tau) - \{1\}$ tel que $x^{(q-1)/2} = 1$, et si $x^y \in C(\tau)$, alors on a $y \in C(\tau)$;

(7.5) si $\tau'$ est une involution dans $C'(\tau)$, et si $a$ est un élément d'ordre 3 dans $N(\langle\tau, \tau'\rangle) - C(\langle\tau, \tau'\rangle)$, alors $a$ ne centralise aucun générateur du groupe cyclique $(C(\tau) \cap C(\tau'))'$.

Montrons que si un groupe de permutations $G$ satisfait aux conditions (0.1)–(0.4) ainsi qu'à la condition $(H : H_0) > 1$, il satisfait aussi aux axiomes (7.1)–(7.5) ci-dessus:

(7.1) n'est autre que la proposition 5.1.

(7.2) est, en vertu de (7.1), équivalent à dire que tous les involutions dans $G$ sont conjugués mutuellement. Alors la proposition 1.9 montre que $G$ satisfait à (7.2).

La proposition 4.4 montre que $G$ satisfait à (7.3).

Quant à (7.4), il est clair, d'après la proposition 1.9, que l'on peut supposer que $\tau = h_0$. De plus on peut se borner au cas où l'ordre de $x$ est un nombre premier. Alors la proposition 4.6 montre que $x$ est conjugué dans $C(h_0)$ à un élément dans $H - H_0$. Puisque $(x^y)^{(q-1)/2} = 1$, on voit alors que $x^y$ est conjugué dans $C(h_0)$ à un élément dans $H$. Alors (7.4) résulte aussitôt du corollaire 1.21.

(7.5) résulte tout de suite de la proposition 6.2.

En résumé, on a le

THÉORÈME 7.6. *Si* $(H : H_0) > 1$, *on a* $q = 3^{2n+1}$ *avec un entier* $n > 0$; $|G| = q^3(q-1)(q^3+1)$; $G$ *satisfait aux axiomes de Ward* (7.1)–(7.5) *ci-dessus.*

[Ajouté à l'épreuve]

**8. Le cas où $m$ est pair.** Dans ce numéro on montrera que les conditions (0.1)–(0.3) impliquent (0.4) s'il existe un groupe satisfaisant aux conditions (0.1)–(0.3). On tirera une contradition de l'hypothèse qu'il existe un groupe satisfaisant aux conditions (0.1)–(0.3) avec $m$ pair. On gardera toujours les notations introduites dans numéro 1.

Il est facile de voir que (1.1)–(1.11) ont lieu même si $m$ est pair. Posons

$$\bar{U}_0 = \{u \in \bar{U} \mid uh_0 = h_0u\}, \qquad q = (\bar{U}_0 : H_0).$$

Alors les $q+1$ lettres $\mathbf{a}$ et $\mathbf{a}^{\omega u}$, $u$ parcourant $\bar{U}_0$, sont exactement celles que fixe l'involution $h_0$. Il est clair que ces lettres se permutent entre elles par les opérations dans $C(h_0)$. Puisque $q > 1$, le groupe $c(h_0)/H_0$ ainsi se réalise fidèlement comme un groupe de permutations des $q+1$ lettres $\mathbf{a}$ et $\mathbf{a}^{\omega u}$. Les conditions (0.1)–(0.3) montrent aisément la propriété suivante:

(8.1) *$C(h_0)/H_0$ est un groupe de permutations doublement transitif de $q+1$ lettres, où $q > 1$. L'élément neutre est le seul élément dans $C(h_0)/H_0$ qui laisse fixe 3 lettres distinctes.*

De plus, utilisant (1.1)–(1.11) et poursuivant la voie de la démonstration de la proposition 1.27, on peut aisément montrer l'identité

$$m = (qn + n + 1)q, \tag{8.2}$$

où $n$ désigne le nombre d'involutions dans $H\omega$. (8.2) montre que $m$ et $q$ ont la même parité. On a donc

$$q \equiv 0 \pmod 2. \tag{8.3}$$

Nous allons maintenant considérer le cas spécial où $H = H_0$. Dans ce cas, $C(h_0)/H_0$ est exactement doublement transitif sur les $q+1$ lettres. Il en résulte que $C(h_0)$ contient un sous-groupe $Q$ d'ordre $2q$ contenant $h_0$ et $\omega$ et un sous-groupe abélien invariant $P$ d'ordre $q+1$. Le groupe $Q/H_0$ opère

dans $P$ comme un groupe d'automorphismes sans point fixe. Fixons un 2-sous-groupe $T$ de Sylow de $Q$ contenant $h_0$ et $\omega$. Le groupe $T/H_0$ opère dans $P$ comme un groupe d'automorphismes sans point fixe. Il s'ensuit que le groupe $T/H_0$ contient une et une seule involution, à savoir, $\omega H_0$. Montrons que $G$ ne contient aucun élément $x$ tel que $x^2 = h_0$. Supposons le contraire. On a $x \in C(h_0)$, et on peut trouver un élément $c$ dans $C(h_0)$ tel que $x^c \in T$. Puisque $(x^c)^2 = h_0$, on peut supposer que $x \in T$. Alors, $xH_0$ est une involution dans $T/H_0$. On a donc $xH_0 = \omega H_0$, et $x^2 = 1$, ce qui est une contradiction. Puisque $T$ est un 2-sous-groupe de Sylow de $G$ et puisque toutes les involutions dans $G$ sont conjuguées entre elles, il en résulte que $G$ ne contient aucun élément d'ordre 4, ce qui montre que $T/H_0$ ne peut être un groupe de quaternions généralisé. Le groupe $T/H_0$ est donc cyclique. $T$ est donc un quatre groupe, puisque $G$ ne contient aucun élément d'ordre 4. Le groupe $G$ n'ayant pas de sous-groupe d'indice 2, un théorème de Gorenstein et Walter **(11**, p. 10**)** s'applique au $G$: $G$ possède un sous-groupe invariant $K$ d'ordre impair tel que $G/K \simeq \mathrm{PSL}(2, r)$, où $r \equiv 3, 5 \pmod 8$.

Eliminons d'abord la possibilité $K = \{1\}$. Dans ce cas, on a $G \simeq \mathrm{PSL}(2, r)$. Il en résulte que $|C(h_0)| = r - \delta$, où $\delta = \pm 1$ et $\delta \equiv r \pmod 4$. Par ailleurs on a $|C(h_0)| = 2q(q + 1)$ et

$$|G| = 2m(m + 1) = 2q(q + 1)(2q + 1)(2q + 3),$$

puisque $m = q(2q + 3)$ en vertu de (8.2). On a donc

$$r = 2q(q + 1) + \delta, \qquad r(r^2 - 1) = 4q(q + 1)(2q + 1)(2q + 3).$$

Il est facile de voir que les équations ci-dessus n'ont pas de solutions intègres. On a donc démontré $K \neq \{1\}$.

Considérons maintenant le cas $K \neq \{1\}$. Le groupe $K$ est résoluble, puisque $K$ est d'ordre impair. Soit $P \neq \{1\}$ un $p$-sous-groupe invariant de $G$ contenu dans $K$. Alors $BP \neq B$, parce que $B$ ne contient aucun sous-groupe invariant $\neq \{1\}$ de $G$. On a alors $G = BP$ puisque $B$ est un sous-groupe maximal de $G$. On a

$$G/P \simeq B/B \cap P, \qquad \text{et} \qquad |P| = (G:B)|B \cap P| = (m + 1)\,|B \cap P|.$$

Il en résulte que $m + 1$ est une puissance de $p$. D'autre part, (8.2) implique $m = q(2q + 3)$, ce qui entraîne $m + 1 = (q + 1)(2q + 1)$. Il s'ensuit que $q + 1$ et $2q + 1$ sont tous deux une puissance de $p$, ce qui est impossible. On a donc $(H:H_0) > 1$. Autrement dit,

(8.4) *Le groupe de permutations $C(h_0)/H_0$ donné dans* (8.1) *n'est pas exactement doublement transitif.*

De plus, on a

(8.5) *$C(h_0)/H_0$ ne possède pas de sous-groupe invariant d'ordre $q + 1$.*

En effet, si le contraire avait lieu, un théorème de Feit **(3**, Lemma 4.1**)**

montrerait que $q + 1$ est une puissance de 2, ce qui est impossible puisque $q$ est pair.

Les propriétés (8.1)–(8.5) montrent que $C(h_0)/H_0$ est un (ZT)-groupe selon la terminologie de Suzuki **(13**, p. 106**)**. Alors d'après un théorème de Suzuki **(14**, p. 149**)**, on a soit $C(h_0) = H_0 \times L$, où $L$ est un (ZT)-groupe, soit $C(h_0) \simeq \mathrm{SL}(2, 5)$. La dernière possibilité s'élimine aussitôt, parce que $\mathrm{SL}(2, 5)$ ne possède qu'une involution tandis que $C(h_0)$ en contient au moins deux, à savoir $h_0$ et $\omega$. On a donc

$$C(h_0) = H_0 \times L \tag{8.6}$$

avec un (ZT)-groupe $L$. Supposons que $L$ contient un élément d'ordre 4. Alors il existe un élément $x$ dans $G$ tel que $x^2 = h_0$, parce que toutes les involutions dans $G$ sont conjuguées entre elles. On a $x \in C(h_0)$. D'après (8.6) on peut écrire $x = h_0 y$ avec $y \in L$, puisque $x \notin L$. On a alors $h_0 = x^2 = y^2 \in L$, ce qui est une contradiction. Donc $L$ est un (ZT)-groupe dont les 2-sous-groupes de Sylow sont élémentaires. D'après un thèoréme fondamental de Suzuki **(13**, p. 107**)**, un tel (ZT)-groupe est isomorphe à $\mathrm{PSL}(2, 2^\alpha)$ pour un entier $\alpha > 1$. Il s'ensuit que les 2-sous-groupes de Sylow de $G$ sont abéliens élémentaires et d'ordre $\geqslant 8$. Appliquant un résultat de Thompson **(12**, Lemma 3.3**)** à $G$, on conclut que $L \simeq \mathrm{PSL}(2, 3^\beta)$ avec un entier $\beta > 1$. Cependant $\mathrm{PSL}(2, 2^\alpha)$ et $\mathrm{PSL}(2, 3^\beta)$ ne peuvent être isomorphes. Cette contradiction établit donc le

THÉORÈME 8.7. *S'il existe un groupe de permutations satisfaisant aux conditions* (0.1)–(0.3), *$m$ est impair.*

## BIBLIOGRAPHIE


1. R. Brauer, M. Suzuki, et G. E. Wall. *A characterization of the one-dimensional unimodular projective groups over finite fields*, Illinois J. Math., *2* (1958), 718–745.
2. W. Burnside, *Theory of groups of finite order* (New York, 1955).
3. W. Feit, *On a class of doubly transitive permutation groups*, Illinois J. Math., *4* (1960), 170–186.
4. D. Gorenstein et J. Walter, *On finite groups with dihedral Sylow 2-subgroups*, Illinois J. Math., *6* (1962), 553–593.
5. N. Ito, *On a class of doubly transitive permutation groups*, Illinois J. Math., *6* (1962), 341–352.
6. R. Ree, *A family of simple groups associated with the simple Lie algebra of type* ($G_2$), Amer. J. Math., *83* (1961), 432–462.
7. I. Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math., *132* (1907), 85–137.
8. H. N. Ward, *On Ree's series of simple groups*, Thesis, Harvard University (1962); voir aussi Bull. Amer. Math. Soc., *69* (1963), 113–114.
9. H. Wielandt, *Über die Existenz von Normalteilern in endlichen Gruppen*, Math. Nachr., *18* (1958), 274–280.
10. H. Zassenhaus, *Kennzeichnungen endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, *11* (1936), 17–40.

**11.** D. Gorenstein, *The classification of finite groups with dihedral Sylow 2-groups*, Symposium on group theory, Harvard University (1963), 10–15.
**12.** Chih-Han Sah, *A class of finite groups with abelian 2-Sylow subgroups*, Math. Zeitschr., *82* (1963), 335–346.
**13.** M. Suzuki, *On a class of doubly transitive permutation groups*, Ann. of Math., *75* (1962), 105–145.
**14.** ——— *Two characteristic properties of* $(ZT)$*-groups*, Osaka Math. J., *15* (1963), 143–150. 105–145.

*University of British Columbia*