Curran, M.J.
Osaka J. Math.
13 (1976), 385-398

GROUPS WITH DECOMPOSABLE INVOLUTION CENTRALIZERS

M. JOHN CURRAN

(Received June 9, 1975)

1. Introduction

Let G be a finite group with a central involution t whose centralizer in G has the structure $C(t)=\langle t\rangle\times F$, where F is a non-abelian simple group. Suppose further G has no subgroup of index 2. Then Janko [6] has shown if $F\simeq A_5$ then $G\simeq Ja$, the Janko simple group of order 175,560; and Janko and Thompson [7] have proved if $F\approx PSL(2, q)$, $q\equiv 3, 5 \pmod 8$, $q>5$, then $q=3^{2n+1}$ $(n\geq 1)$ and G is simple (these are the groups of Ree type). In this paper we prove the following result.

Theorem 1.1. *Let G be a finite group with a central involution t whose centralizer has the structure*

$$C(t)=\langle t\rangle\times F$$

where F is isomorphic to either a simple alternating group or a classical simple group of odd characteristic. Then G has a subgroup of index 2 not containing t (and so G is not simple), except when $F\approx A_5$ or $F\approx PSL$ $(2, 3^{2n+1})$ $(n\geq 1)$.

Since t is central, $C(t)$ contains an S_2-subgroup S of G of form $S=\langle t\rangle\times M$, where M is an S_2-subgroup of F. We show t is not conjugate in G to any involution in M and use the following lemma of Thompson ([8], Lemma 5.38) to obtain the result.

Lemma 1.2. *Let G be a finite group with an S_2-subgroup S. Let M be a subgroup of index 2 in S and t an involution in S-M which is not conjugate in G*

Summary. In this paper we prove the follwing result.
Theorem: Let G be a finite group with a central involution t whose centralizer has the structure

$$C(t)=\langle t\rangle\times F$$

where F is isomorphic to either a simple alternating group or a classical simple group of odd characteristic. Then G has a subgroup of index 2 not containing t (and so G is not simple), except when $F\approx A_5$ or $F\approx PSL(2, 3^{2n+1})$ $(n\geq 1)$

to any element of M. Then G has a (normal) subgroup of index 2 not containing t.

Throughout V will be the underlying n-dimensional vector space over a field K of q elements (or a field E of q^2 elements) where q is odd. If X is an involution in $GL(V)$, the invertible linear maps on V, then $V=V^+(X)\oplus V^-(X)$, where $V^+=V^+(X)=\{v\in V \mid vX=v\}$, and $V^-=V^-(X)=\{v\in V \mid vX=-v\}$. As usual (see [4]) we define the type of X to be $r(X)=\dim V^-(X)$.

We will reserve H throughout to be any one of the classical groups $SL(n, q)(n\geq 2, q>3)$, $Sp(n, q)$ (n even, $n\geq 4$), $SU(n, q)(n\geq 3)$ or $\Omega(n, q)$ ($n\geq 5$), and PH the corresponding projective simple group, so $PH=H/Z(H)$. Recall the group $\{X\in GL(n, q) \mid XAX^T=I_n\}$ is $Sp(n,q)$ when n is even and

$$A=\begin{pmatrix} \begin{array}{|cc|} 0 & 1 \\ -1 & 0 \end{array} & & \\ & \ddots & \\ & & \begin{array}{|cc} 0 & 1 \\ -1 & 0 \end{array} \end{pmatrix};$$

when $A=I_n$ the group is $0(n, q)$ (square discriminant); and if n is even and $A=\begin{bmatrix} I_{n-1} & 0 \\ 0 & \gamma \end{bmatrix}$, $\gamma\in K-K^2$, the group is $0(n, q)$ (non-square discriminant). And $U(n, q)=\{X\in GL(n, q^2) \mid \bar{X}X^T=I_n\}$ where $-$ is induced by the field automorphism $\alpha\to\alpha^q$, $\alpha\in E$.

If Z^* is any non-trivial subgroup of $Z(H)$, we denote the image of $X\in H$, by $x\in H/Z^*$. Further if $x\in H/Z^*$ is the image of an involution $X\in H$, we define the type of x to be $r(X)$ if $-1\notin Z^*$, or $\min\{r(X), r(-X)\}$ if $-1\in Z^*$. If x is an involution in PH, then $X^2\in Z(H)$ so $X^2=\lambda\cdot 1$ for some $\lambda\in\dot{K}=K-\{o\}$ (or $\dot{E}$), and X is called a semi-involution.

For $x\in PH$, $C_{PH}(x)=$ Image $C_H^*(X)$ where $C_H^*(X)=\{Y\in H \mid X^Y\equiv X \pmod{Z(H)}\}$. If X is a semi-involution and $y\in C_H^*(X)$ then $X^Y=\pm X$ so in fact $|C_H^*(X): C(X)|=1$ or 2.

We need the follow lemma on the conjugation properties of involutions and semi-involutions in H, the proof of which is effectively contained in Dickson ([3], pp. 102, 106) and Dieudonné ([4], pp. 25, 26), while a direct proof for the symplectic and orthogonal cases is given in the papers of Wong ((*IA*) in [9], section 1 in [10]).

Lemma 1.3.

(i) *Two involutions in H are conjugate (in H) iff they have the same type.*

(ii) *There is exactly one class of semi-involutions Y in $Sp(n, q)$ or $0(n, q)$ such that $Y^2=-1$.*

(iii) *Suppose X and Y are semi-involutions in $SL(n, q)$ with $X^2=\lambda\cdot 1$ and $Y^2=\mu\cdot 1$ $(\lambda, \mu\in\dot{K})$. If $\lambda\in\dot{K}^2$ there exists $\gamma\in\dot{K}$ such that $X'=\gamma X$ is an involution (in $GL(n, q)$) and if $\mu\in\dot{K}^2$ then X and Y are projectively conjugate* *(in $SL(n, q)$) iff $(r(X')=r(\pm Y')$. If $\lambda \notin \dot{K}^2$ then X and Y are projectively conjugate in $SL(n, q)$ iff $\mu \equiv \lambda \pmod{\dot{K}^2}$.*

(iv) *Suppose X and Y are semi-involutions in $SU(n, q)$ with $X^2=\lambda\cdot 1$, $\lambda=\gamma^2$, and $Y^2=\mu\cdot 1$, $\mu=\rho^2$ with $\lambda, \gamma, \mu, \rho \in \dot{E}$. If $\gamma\bar{\gamma}=1$ then $X'=\gamma^{-1}X$ is an involution in $U(n, q)$ and if $\rho\bar{\rho}=1$ then X and Y are projectively conjugate in $SU(n, q)$ iff $r(X')=r(\pm Y')$. If $\gamma\bar{\gamma}=-1$ then X and Y are projectively conjugate in $SU(n, q)$ iff $\rho\bar{\rho}=-1$.*

2. Involutions which are squares

If L is any subgroup of G denote by $\langle L^2\rangle$ the subgroup generated by the squares of elements in L. Then the following lemma is useful.

Lemma 2.1. *t is not conjugate in G to any involution $x\in\langle C_F(x)^2\rangle$. In particular t cannot be conjugate to an involution which is the square of an element of order 4 in F.*

Proof. Suppose on the contrary that t is conjugate to such an x. Then $x^a=t$ for some $a\in G$, where $x=\prod_{i=1}^{m} x_i^2$, $x_i\in C_F(x)$, and m a positive integer.

$$\text{Thus } t = \prod_{i=1}^{m} (x_i^a)^2 .$$

But $x_i\in C_F(x)\subseteq C(x)$ so $x_i^a\in C(x)^a=C(t)$.

Therefore $t\in\langle C(t)^2\rangle\subseteq F$, a contradiction. Hence t cannot be conjugate to such an x.

Theorem 1.1 has been proved by Yamaki [11] when $F\approx A_n$ $(n\geq 6)$. But it is also immediate from (1.2) and (2.1), since every involution in A_n $(n\geq 6)$ is a product of squares of elements from its centralizer. Similarly, when $F\approx PSL(2, q)$, $q\equiv\pm 1 \pmod 8$, F has only one class of involutions and every involution in this class is the square of an element of order 4 in F. For the class of involutions in $PSL(2, q)$ has

$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ as a representative in $SL(2, q)$ and

$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha & \alpha \\ -\alpha & \alpha \end{bmatrix}^2$ where $\alpha = \dfrac{1}{\sqrt{2}}$. So theorem 1.1 also

holds in this case and we assume $n\geq 3$ for the remainder.

We now determine which involutions are of the above form in the various classical groups. Throughout put $H(n, \varepsilon)=H(\varepsilon)=SL(n, q)$ when $\varepsilon=1$, and $H(n, \varepsilon)=H(\varepsilon)=SU(n, q)$ when $\varepsilon=-1$. If $d=(n, q-\varepsilon)$ then $|Z(H(\varepsilon))|=d$. The result for the special linear and special unitary cases is as follows.

Lamma 2.2. *Every involution in $F\approx PH(\varepsilon)$ is square in F except, in the following cases:*

(a) $2||n$ *and* $q\equiv 4-\varepsilon$ *(mod* 8).
(b) $2^{s+1}||n$ *and* $2^s||q-\varepsilon$ $(s\geq 2)$.
(c) $2^{s-1}||n$ *and* $2^s||q-\varepsilon$ $(s\geq 2)$.
Then there is at least one class in F with representative x such that $x\notin C_F\langle (x)^2\rangle$.

Proof. We prove the lemma for $F\approx PSL(n, q)$. The case $\varepsilon=-1$ is similar. Let y be an involution in $PSL(n, q)$. If y has a pre-image which is an involution then y is a square in F since every involution in $SL(n, q)$ is a square in $SL(n, q)$. So we may assume dim V is even and $Y^2=\lambda\cdot 1$ where $\lambda^d=1$ but $\lambda^{d/2}\neq 1$.

We distinguish three cases:

(a) Let $2^s||n$ and $2^r||q-1$ with $0\leq r\leq s$. These conditions imply $\lambda\notin\dot{K}^2$ and in a suitable basis

$$Y=\begin{pmatrix} \begin{array}{|cc|} 0 & 1 \\ \lambda & 0 \\ \hline \end{array} & & \\ & \ddots & \\ & & \begin{array}{|cc} \hline 0 & 1 \\ \lambda & 0 \end{array} \end{pmatrix} \text{ with } (-\lambda)^{n/2}=1.(*)$$

Note by (1.3) if x is any other involution in F which has no involution as a preimage then X is projectively conjugate to Y. Further we can make V into an $n/2$-dimensional vector space over $E=K(\gamma)$ (where $\gamma^2=\lambda$) by defining $(\alpha+\beta\gamma)v=\alpha v+\beta(vY)$, any $v\in V$. Then a K-linear transformation X commutes with Y iff X is E-linear.

Thus $C_{GL}(Y)\approx GL(n/2, q^2)$ with $Y\leftrightarrow\gamma I_{n/2}$. So $C(Y)=C_{SL}(Y)$ is isomorphic to a subgroup of index $q-1$ in $GL(n/2, q^2)$ and $C(Y)'\approx SL(n/2, q^2)$ with $C(Y)/C(Y)'$ cyclic of order $q+1$.

Now select $\alpha, \beta\in\dot{K}$ such that $-\alpha^2+\beta^2\lambda=1$. Then

$$W=\begin{pmatrix} \begin{array}{|cc|} \alpha & \beta \\ -\beta\lambda & -\alpha \\ \hline \end{array} & & \\ & \ddots & \\ & & \begin{array}{|cc} \hline \alpha & \beta \\ -\beta\lambda & -\alpha \end{array} \end{pmatrix}\in SL(n, q) \text{ and } Y^W=-Y,$$

so $|C^*(Y): C(Y)|=2$. Further W is semi-linear in V over E and inverts the elements of $C(Y)/C(Y)'$. When $r=s=1$ (*i.e.* $q\equiv 3$(mod 4) and $n/2$ is odd), $\langle C^*(Y)^2\rangle$ is of index 2 in $C(Y)$ and by (*) $\lambda^{n/2}=-1$.

$$\begin{aligned} \text{So } Y\in\langle C^*(Y)^2\rangle &\text{ iff } \det(\gamma I_{n/2})^{(q+1)/2}=1 \\ &\text{ iff } q\equiv 7 \text{ (mod 8)}. \end{aligned}$$

Thus $y\in\langle C_F(y)^2\rangle$ (and in fact y is a square), except when $q\equiv 3$ (mod 8).

(b) Now consider the case when $2^s||n$ $(s\geq 2)$ and $2^r||q-1$ with $0<r\leq s$.

In fact $0<r<s$ for by (*) $\lambda^{n/2}=1$ and if $r=s$, λ is a $d/2$ root of unity contradicting an earlier assumption. Here $C^*(Y)/C(Y)'$ is dihedral so $\langle C^*(Y)^2\rangle$ is again of index 2 in $C(Y)$.

$$\text{Thus } Y\in\langle C^*(Y)^2\rangle \text{ iff } \det(\gamma I_{n/2})^{(q+1)/2}=1$$
$$\text{iff } (\lambda^{n/4})^{(q+1)/2}=1.$$

Now $\lambda^{n/4}=1$ except if $r=s-1$ when $\lambda^{n/4}=-1$. And $\frac{q+1}{2}$ is odd except when $r=1$. Thus $Y\in\langle C^*(Y)^2\rangle$ except when $r>1$ and $r=s-1$. So $y\in\langle C_F(y)^2\rangle$ (and is in fact a square in F) except when $2^{s+1}||n$ and $2^s||q-1$ ($s\geq 2$).

(c) Finally suppose $2^{s-1}||n$ and $2^{s+j}||q-1$ with $s\geq 2$ and $j\geq 0$. This implies $\lambda\in\dot{K}^2$, say $\lambda=\gamma^2$ where $\gamma^n=-1$. Thus $\gamma^{-1}Y$ is an involution of determinant -1 in $GL(n, q)$ and by (1.3) Y is conjugate to

$$\gamma\begin{bmatrix}-I_r & 0\\ 0 & I_{n-r}\end{bmatrix}, \text{ some odd } r,\ 0<r<n\,.$$

Therefore $C_{GL}(Y)\approx GL(r, q)\times GL(n-r, q)$ with $C(Y)=C_{SL}(Y)$ a subgroup of index $q-1$. So $C(Y)'\approx SL(r, q)\times SL(n-r, q)$ and $C(Y)/C(Y)'$ is cyclic of order $q-1$. Further $C^*(Y)=C(Y)$ except when $2||n$ and $r=\frac{n}{2}$. Then $W=\begin{bmatrix}0 & -I_r\\ I_r & 0\end{bmatrix}\in SL(n, q)$ is such that $Y^W=-Y$ so $|C^*(Y)\colon C(Y)|=2$, and W inverts the elements of $C(Y)/C(Y)'$. In either case $\langle C^*(Y)^2\rangle$ is of index 2 in $C(Y)$ and

$$Y\in\langle C^*(Y)^2\rangle \text{ iff } (\det(-\gamma I_r))^{(q-1)/2}=1$$
$$\text{iff } j\geq 1\,.$$

Thus $y\in\langle C_F(y)^2\rangle$ (and is a square in F) except when $j=0$, and this completes the lemma.

In the symplectic case we have:

Lamma 2.3. *Every involution in $F\approx PSp(n, q)$ is a square in F except when*
(d) $n\equiv 2\,(mod\,4)$ *and* $q\equiv 4\pm 1\ (mod\,8)$.
Then there is a class with representative x such that $x\notin\langle C_F(x)^2\rangle$.

The proof of (2.3) is similar to the orthogonal case.

Lemma 2.4. *Every involution $x\in F\approx P\Omega(n, q)$ is such that $x\in\langle C_F(x)^2\rangle$ except in the following even dimensional cases:*
(e) $n\equiv 2\,(mod\,4)$ *and* $q\equiv 8\pm 1\ (mod\,16)$.
(f) $n\equiv 4\,(mod\,8)$ *and* $q\equiv 4\pm 1\ (mod\,8)$.

Proof. First suppose the non-trivial involution $y\in F$ has a preimage $Y\in\Omega(n, q)$ which is an involution. By (1.3) we may take

$$Y=\begin{bmatrix}-I_i & 0\\ 0 & I_{n-i}\end{bmatrix},\ 0<i<n;\ i=2, 4, \cdots$$

and write $V=V^+(Y)\oplus V^-(Y)$. Then $C_{0(V)}(Y)\approx 0(V^+)\times 0(V^-)$, and $C(Y)=C_\Omega(Y)\approx\{(Y_1, Y_2)\in C_{0(V)}(Y)\,|\,\det Y_1=\det Y_2;\ \theta(Y_1)=\theta(Y_2)\}$, where θ is the spinor norm on $0(V)$ (see Artin [1]). Further $C(Y)'\approx\Omega(V^-)\times\Omega(V^+)$, and since V^- has even dimension and square discriminant $-1_{V^-}\in\Omega(V^-)$. Hence $Y\in C(Y)'\subseteq\langle C^*(Y)^2\rangle$. This proves the lemma when n is even and the discriminant is a non-square, or when n is odd, for then $P\Omega(n, q)=\Omega(n, q)$.

Now consider when n is even and the discriminant is a square. Let $X=\begin{pmatrix}\begin{array}{|cc|}0&1\\-1&0\end{array} & & \\ & \ddots & \\ & & \begin{array}{|cc|}0&1\\-1&0\end{array}\end{pmatrix}$, a semi-involution in $SO(n, q)$. Then $\theta(X)=2^{n/2}$. But by (1.3) any non-trivial semi-involution in $0(n, q)$ is conjugate to X. Thus there are semi-involutions in $\Omega(n, q)$ iff (i) $n\equiv 0 \pmod 4$ or (ii) $n\equiv 2 \pmod 4$ and $q\equiv\pm 1 \pmod 8$. Now let $q\equiv\delta \pmod 4$ ($\delta=\pm 1$).

(a) When $\delta=1$, $-1=\gamma^2$ some $\gamma\in\dot{K}$, and $X'=\gamma^{-1}X$ is an involution in $GL(n, q)$. If we write $V=V^+(X')\oplus V^-(X')$, then V^+ and V^- are both totally isotropic with respect to the form so $\dim V^+=\dim V^-=\frac{n}{2}$. Thus with respect to a basis of $V=$(basis of V^+)$\cup$(basis of V^-) the form has matrix $\begin{bmatrix}0 & B\\ B^T & 0\end{bmatrix}$, some $B\in GL(n/2, q)$. Therefore

$$C_{0(V)}(X)=\left\{\left[\begin{array}{c|c}Y & 0\\ \hline 0 & B^T(Y^T)^{-1}(B^T)^{-1}\end{array}\right]\middle|\, Y\in GL(n/2, q)\right\}\approx GL(n/2, q)$$

with $X\leftrightarrow\gamma I_{n/2}$.

(b) When $\delta=-1$, $-1\notin\dot{K}^2$ and as in (2.2) (a) we can make V into an $n/2$-dimensional vector space over $E=K(\gamma)$, where $\gamma^2=-1$. Further V becomes a unitary space by defining a new form $\langle\!\langle\ ,\ \rangle\!\rangle$:

$$\langle\!\langle v, w\rangle\!\rangle=\langle v, w\rangle+\gamma\langle vX, w\rangle \qquad \text{any } v, w\in V,$$

where $\langle\ ,\ \rangle$ is the non-degenerate symmetric bilinear form on V. Then $\langle\!\langle\ ,\ \rangle\!\rangle$ is a non-degenerate hermitian form with respect to the automorphism $\alpha+\beta\gamma\to\alpha-\beta\gamma$ of E. And an E-linear transformation lies in $0(n, q)$ iff it is unitary with respect to this form. So $C_{0(V)}(X)\approx U(n/2, q)$ with $X\leftrightarrow\gamma I_{n/2}$.

Note in both (a) and (b), $C_{0(V)}(X)=C_{S0(V)}(X)$. Hewever, there are elements of non-trivial spinor norm centralizing X. So $C(X)=C_\Omega(X)$ is a subgroup of index 2 in $C_{0(V)}(X)$, with $C(X)'\approx H(n/2, \varepsilon)$ (where $\varepsilon=1$ in (a), $\varepsilon=-1$ in (b)).

Let $W=\begin{pmatrix} 0 & I_{n/2} \\ I_{n/2} & 0 \end{pmatrix}$ ($\varepsilon=1$) or $W=\begin{pmatrix} \begin{smallmatrix}0&1\\1&0\end{smallmatrix} & & \\ & \ddots & \\ & & \begin{smallmatrix}0&1\\1&0\end{smallmatrix} \end{pmatrix}$ ($\varepsilon=-1$).

Then W is a coset representative of $C_{0(V)}(X)$ in $C^*_{0(V)}(X)$, which inverts the elements of $C(X)/C(X)'$. However, $W\in C^*(X)$ iff $n\equiv 0 (\mathrm{mod}\ 4)$. Therefore $C^*(X)/C(X)'$ is dihedral when $n\equiv 0 (\mathrm{mod}\ 4)$ and $C^*(X)=C(X)$ when $n\equiv 2 (\mathrm{mod}\ 4)$. In either case $\langle C^*(X)^2\rangle$ is of index 2 and if $\rho=(\det \gamma I_{n/2})^{(q-\varepsilon)/4}$, then $X\in \langle C^*(X)^2\rangle$ iff $\rho=1$. So in (i) when $n\equiv 0 (\mathrm{mod}\ 4)$, $\rho=1$ iff $n\equiv 0$ (mod 8) or $n\equiv 4 (\mathrm{mod}\ 8)$ and $q\equiv\varepsilon (\mathrm{mod}\ 8)$. And in (ii) when $n\equiv 2 (\mathrm{mod}\ 4)$ and $q\equiv\delta (\mathrm{mod}\ 8)$, $\rho=1$ iff $q\equiv\delta (\mathrm{mod}\ 16)$. This completes the lemma.

We have now show theroem 1.1 holds, but for the exceptional cases (a), $\cdots$, (f). We turn our attention to these cases.

3. The exceptional cases

To prove theorem 1.1 in the exceptional cases we need the structure of the subgroup generated by involutions in the centre of an S_2-subgroup of F. To determine this we first find $\Omega_1(Z(M))$, for an S_2-subgroup M of H.

Let the dyadic expansion of the dimension of V be

$$n = 2^{m_1}+2^{m_2}+\cdots+2^{m_k}, \quad 1\leq m_1<\cdots<m_k .$$

In fact $m_1=1$ and $k>1$ in (a), (b) and (e); $m_1=2$ and $k>1$ in (f); while if $k=1$, $m_1\geq 3$ in (b); and $m_1\geq 2$ in (c).

Lemma 3.1. *Let M be an S_2-subgroup of $SL(n, q)$, $Sp(n, q)$, $SU(n, q)$ or $\Omega(n, q)$ (square discriminant). Then there are subspaces $V_1, \cdots, V_k$ of V of dimensions $2^{m_1}, \cdots, 2^{m_k}$ respectively, such that $V=V_1\oplus\cdots\oplus V_k$ and*

$$\Omega_1(Z(M)) = \langle -1_{V_1}\rangle\times\cdots\times\langle -1_{V_k}\rangle .$$

Proof. We consider only when $F\approx PH(n, \varepsilon)$ and M is an S_2-subgroup of $H(n, \varepsilon)$.

The proof of the other cases is similar.

(i) First let $q\equiv\varepsilon (\mathrm{mod}\ 4)$, and suppose as in (b) and (c) $2^s \| q-\varepsilon$ ($s\geq 2$). Then an S_2-subgroup W of $GL(2, q)$ or $U(2, q)$ has order 2^{2s+1}. In fact W is generated by the matrices

$$\begin{bmatrix} \eta & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & \eta \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

where n is a primitive 2^s root of unity in the field. Thus $W\approx Z_{2^s}\sim Z_2$ where

Z_n denotes the cyclic group of order n. Hence $\Omega_1(Z(W))\approx Z_2$.

Now let $T_i=Z_2\sim\cdots\sim Z_2$ be the wreath product of Z_2 i times, and put $W_1=W$, $W_m=W\sim T_{m-1}(m>1)$. Then from Carter and Fong [2] if S is an S_2-subgroup of $GL(n, q)$ or $U(n, q)$ there are subspaces $V_1, \cdots, V_k$ of V with corresponding dimensions $2^{m_1}, \cdots, 2^{m_k}$ such that $V=V_1\oplus\cdots\oplus V_k$ and $S=W_{m_1}\times\cdots\times W_{m_k}$, where W_{m_i} is an S_2-subgroup of $GL(V_i)$ or $U(V_i)$ respectively.

Therefore $\Omega_1(Z(S))=\langle -1_{V_1}\rangle\times\cdots\times\langle -1_{V_k}\rangle$.

Now let Q be an S_2-subgroup of $H(2, \varepsilon)$. Then Q is (generalized) quaternian of order 2^{s+1} and is generated by

$$\begin{bmatrix}\eta & 0\\ 0 & \eta^{-1}\end{bmatrix}, \quad \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},$$

so $Z(Q)\approx Z_2$. Put $Q_1=Q$ and $Q_m=Q\sim T_{m-1}(m>1)$ and let $T=Q_{m_1}\times\cdots\times Q_{m_k}$, where $Q_{m_i}\subseteq W_{m_i}$. Then T is a 2-subgroup of $H(n, \varepsilon)$. Now let M be an S_2-subgroup of $H(n, \varepsilon)$ such that $T\subseteq M\subseteq S$.

Then $\Omega_1(Z(S))=Z(T)\subseteq M$ so $\Omega_1(Z(S))=\Omega_1(Z(S))\cap M\subseteq\Omega_1(Z(M))$. Conversely if $Y\in Z(M)$,

$$Y\in C_s(T)=\prod_{i=1}^{k} C_{W_{m_i}}(Q_{m_i})=\prod_{i=1}^{k}\langle \eta 1_{V_i}\rangle \text{ by induction},$$

i.e., if $Y\in\Omega_1(Z(M))$, $Y\in\langle -1_{V_1}\rangle\times\cdots\times\langle -1_{V_k}\rangle$ so

$$\Omega_1(Z(M))\subseteq\Omega_1(Z(S)).$$

(ii) When $q\equiv -\varepsilon(\bmod 4)$ as in case (a), an S_2-subgroup W of $GL(2, q)$ or $U(2, q)$ has order 2^{s+2}, where $2^s\|q+\varepsilon$ $(s\geq 2)$. Further W is semi-dihedral (see [2]) so $Z(W)\approx Z_2$. If Q is an S_2-subgroup of $H(2, \varepsilon)$ then Q is a (generalized) quaternion group of order 2^{s+1}, so $Z(Q)\approx Z_2$. The argument now follows as in (i) above.

Lemma 3.2.

I. *The classes of involutions in $F\approx PH$ have the following representatives in H:*

(i) *In (a), (b), (d) and (e) they are:*

$$Y_i=\begin{pmatrix}-I_i & 0\\ 0 & I_{n-i}\end{pmatrix}, \quad X=X_1=\begin{pmatrix}\begin{array}{|cc|}0 & 1\\ \lambda & 0\end{array} & & 0\\ & \ddots & \\ 0 & & \begin{array}{|cc}0 & 1\\ \lambda & 0\end{array}\end{pmatrix}$$

for $i=2, 4, \cdots, 2[\frac{n}{4}]$; and in (a) and (b) λ is a primitive d-th root of unity in the field with $(-\lambda)^{n/2}=1$, while in (d) and (e) $\lambda=-1$.

(ii) *In (f) they are as above with the further representative*

$$X_2=\begin{pmatrix} \begin{matrix}0&-1\\1&0\end{matrix} & & & \\ & \begin{matrix}0&1\\-1&0\end{matrix} & & \\ & & \ddots & \\ & & & \begin{matrix}0&1\\-1&0\end{matrix}\end{pmatrix}.$$

(iii) *In (c) they are:*

$$Y_i=\begin{pmatrix}-I_i & 0\\ 0 & I_{n-i}\end{pmatrix},\quad X_j=\gamma\begin{pmatrix}-I_j & 0\\ 0 & I_{n-j}\end{pmatrix}$$

where $i=2, 4, \cdots, 2\left[\frac{n}{4}\right]$, *and* $j=1, 3, \cdots, 2\left[\frac{n-2}{4}\right]+1$; *and* γ *is a primitive* 2 *d-th root of unity in the field so* $\gamma^n=-1$.

II. *The involutions* x_j *(any* j*) and for* $k>1$ *the involution* $y_{n/2}$ *(when* $n\equiv 0$ *(mod 4)) are not central in* F.

Proof. I. (i) and (iii) follow from (1.3).

(ii) if X and Y are two non-trivial semi-involutions in $\Omega(n, q)$ then by (1.3) $X^W=Y$, some $W\in 0(n, q)$. When $n\equiv 2(\text{mod } 4)$ we may select $W'\in C^*_{0(V)}(Y)$ of the same determinant and spinor norm as W, since in this case the elements of $C^*_{0(V)}(Y)-C_{0(V)}(Y)$ have determinant -1. Then $WW'\in\Omega(n, q)$ and $X^{WW'}=\pm Y$, so $x\sim y$ in $P\Omega(n, q)$. However when $n\equiv 0(\text{mod } 4)$, $C^*_{0(V)}(Y)\subseteq SO(n, q)$, so X_1 and X_2 which are conjugate in $0(n, q)$ by an element of determinant -1 are not projectively conjugate in $\Omega(n, q)$. But any non-trivial semi-involution in $\Omega(n, q)$ is conjugate to either X_1 or X_2.

II. When $n/2$ is even, the 2-order of $|H\colon C^*_H(Y_{n/2})|$ is 2^{k-1}. So if $k>1$, $y_{n/2}$ is not central in F.

In (a) and (b) we have

$$|H(n, \varepsilon)\colon C^*_H(X)| = \frac{1}{2}q^{n^2/4}(q^{n-1}-\varepsilon)(q^{n-3}-\varepsilon)\cdots(q-\varepsilon),$$

which is even so x is not central in F.

In (c) when $j=\frac{n}{2}$ (and so $k>1$), $|H(n, \varepsilon)\colon C^*(X_{n/2})|$ has 2-order 2^{k-1}, which is even. Otherwise

$$|SL(n, q)\colon C^*(X_j)| = |GL(n, q)\colon C_{GL}(\gamma^{-1}X_j)|.$$

But the structure of $\Omega_1(Z(S))$ where S is an S_2-subgroup of $GL(n, q)$ shows $\gamma^{-1}X_j$ is not central in $GL(n, q)$ and so x_j is not central in F, any j. Similar calculations prove the result in the other cases.

Let us denote the image of a subgroup L of H by $\bar{L}$ in PH. We now give the structure of $\Omega_1(Z(\bar{M}))$, where as above M is an S_2-subgroup of H.

Lemma 3.3

(i) $|\Omega_1(Z(\bar{M})|=2$ *when* $k=1$ *and* $\Omega_1(Z(\bar{M}))=\overline{\Omega_1(Z(M))}$ *when* $k>1$.

(ii) *No involution* $z\in\Omega_1(Z(\bar{M}))$ *is conjugate to* t *in* G.

(iii) *If* $z, z'\in\overline{\Omega_1(Z(M))}$ *with* $z\neq z'$ *then type* $z\neq$*type* z'.

Proof. (i) Clearly $\Omega_1(Z(\bar{M}))\subseteq\Omega_1(Z(\bar{M}))$. Conversely if $z\in\Omega_1(Z(\bar{M}))$ then $z\sim y_i$ some i, for by (3.2) the other classes are not central in F. Thus z has a preimage Z which is an involution and this also proves (ii) since $y_i \not\sim t$.

When $k>1$, $Z\in Z(M)$ for if not $Z^m=-Z$ some $m\in M$ and so Z is of type $n/2$. This is impossible when $m_1=1$, and implies for $m_1>1$ that $Z\sim Y_{n/2}$, a contradiction since by (3.2) $y_{n/2}$ is not central.

Let W be an S_2-sungroup of $GL(n/2, q)$ or $\cup(n/2, q)$ when $k=1$ (so $n=2^{m_1}$) then M is of form

$$M=\left\{\left[\begin{array}{c|c} C & 0 \\ \hline 0 & D\end{array}\right], \left[\begin{array}{c|c} 0 & I \\ \hline I & 0\end{array}\right] \middle| C, D\in W;\ \det C=(\det D)^{-1}\right\}$$

and $\Omega_1(Z(\bar{M})=\langle z\rangle$ where $Z=\left[\begin{array}{c|c} -I & 0 \\ \hline 0 & I\end{array}\right]$.

(iii) From (3.1) $\Omega_1(Z(M))=\langle -1_{V_1}\rangle\times\cdots\times\langle -1_{V_k}\rangle$. If $z, z'\in\Omega_1(Z(\bar{M}))$ have the same type then

$$2^{n_1}+\cdots+2^{n_l}=\text{type } Z=\text{type } Z'=2^{n'_1}+\cdots+2^{n'_\rho}$$

where $\{n_1,\cdots, n_l\}$ and $\{n'_1, \cdots, n'_\rho\}$ are subsets of $\{m_1, \cdots, m_k\}$. By uniqueness $Z=\pm Z'$ and $z=z'$

We conclude the proof of the theorem by showing in the exceptional cases t cannot be fused with any involution in F. Of course t cannot be conjugate to any of the classes with representative y_i. The only possiblity is for t to be fused with an x_j, some j. We show this is not the case.

Lemma 3.4. *In (a), (b), (d), (e) and (f) t is not conjugate (in G) to x, and in (f) t is not conjugate to* x_2 *either.*

Proof. Suppose on the contrary $x^a=t$ for some $a\in G$. (In (f) either $x=x_1\sim t$ or $x_2\sim t$ and we may assume the former without loss of generality). Now choose $Y=Y_{2^{m_1}}$ if $k>1$ or $Y=Y_{2^{m_1-1}}$ if $k=1$. From (3.1) and (3.3) there is an S_2-subgroup M of F such that $y\in\Omega_1(Z(M))$. Then $S=\langle t\rangle\times M$ is an S_2-subgroup of G. Clearly $Y\in C(X)$ so $(XY)^2=\lambda\cdot 1$ and by (1.3) $xy\sim x$ in F. Conjugating this relation by a and assuming $y^a=y$ for the moment we obtain $ty\sim t$ in G.

Now t, $ty\in Z(S)$ so by the Burnside argument there is a $b\in N_G(S)$ such that $t^b=ty$. Further b normalizes $\Omega_1(Z(S))=\langle t\rangle\times\Omega_1(Z(M))$ so under conjugation permutes the elements of $\Omega_1(Z(S))-1$. This implies $(ty)^b=t$ when $k=1$, since by (3.3) $|\Omega_1(Z(M))|=2$ and $t\not\sim y$. When $k>1$ we must have $(ty')^b=t$, some $y'\in\Omega_1(Z(M))$ since again by (3.3) no element of $\Omega_1(Z(M))$ is fused with t.

Thus $C(t, y')^b=C(t, ty')^b=C(ty, t)=C(t, y)$,

$$i.e.\quad \langle t\rangle\times C_F(y')\approx\langle t\rangle\times C_F(y)\,.$$

So $|C^*(Y)|=|C^*(Y')|$ and in particular their p-orders are equal where $q=p^l$, p prime. In (a) and (b) the p-order of $|C^*(Y')|$ is $1/2\,l(j(j-1)+(n-j)(n-j-1))$ where Y' is an involution of type j. So if Y is of type i, then $i=j$ or $i+j=n$ and in either case type y=type y'. A similar calculation for (d), (e) and (f) yields the same result, so by (3.3) $y=y'$. Therefore $t\to ty\to t$ under conjugation by b.

Thus $b\in N(S)-C(t)$ and $b^2\in C(t)$. This implies $|N(S): S|$ is even which clearly contradicts S being an S_2-subgroup of G. Hence x is not conjugate to t (in G) provided we show the assumption $y^a=y$ is valid.

We are assuming $x^a=t$ with $t\in C(x)$, so $t^a\in C(t)$. Thus except in (f) t^a is conjugate to one of the following $\{y_i, ty_i, x, tx, t\,|\,i=2, 4, \cdots, 2[n/4]\}$ (a maximal set of representatives of classes in $C(t)$). In fact we may assume $x^a=t$ and $t^a=ty_i$ (some i), tx or x. However if $t^a=ty_i$ some i, then $(tx)^a=y_i$ and $C(t, x)^a=C(t, y_i)$. Therefore $C_F(x)'^a=C_F(y_i)'$. But $y_i\in C_F(y_i)'$, and $C_F(x)'\subseteq F$ contradicting $(tx)^a=y_i$. Hence $t^a=x$ or tx and in either case $C(t, x)^a=C(t, x)$.

Now in (a) and (b), from the proof of (2.2)

$$\begin{aligned}&C(t, x)' = \langle C^*(X)^2\rangle/Z(H(n, \varepsilon))\approx L/Z\\ &\text{where } Z(H(n, \varepsilon))\leftrightarrow Z \text{ in } GL(n/2, q^2)\\ &\text{and } \langle C^*(X)^2\rangle\leftrightarrow L = \{A\in GL(n/2, q^2)\,|\,(\det A)^{(q+\varepsilon)/2} = 1\}\,.\end{aligned}$$

Let $Z^*=Z\cap Z(SL(n/2, q^2))$ then $C(t, x)^{(2)}\approx SL(n/2, q^2)/Z^*$. And $y\in C(t, x)^{(2)}$ corresponds to an involution of a certain type in $SL(n/2, q^2)/Z^*$. Now a normalizes $C(t, x)^{(2)}$ so induces an automorphism on $SL(n/2, q^2)/Z^*$. But every automorphism on $SL(n/2, q^2)/Z^*$ comes from one on $SL(n/2, q^2)$ since $n\geq 6$ (Dieudonné [5]) and any automorphism on $SL(n/2, q^2)$ preserves the type of an involution. Hence y^a is of the same type as y conjugate in $C(t, x)^{(2)}$ to y, *i.e.* $y^a=y^f$, some $f\in F$. Replacing a by af^{-1} we have $x^{af^{-1}}=t$, $y^{af^{-1}}=y$ and we may assume without loss of generality that a centralizes y.

In (f) as above, we may assume $t^a=x'$ or tx' where $x'=x_i$ ($i=1$ or 2). Thus $C(t, x)^a=C(t, x')$. From the proof of (2.4) if $q\equiv\varepsilon\,(\text{mod }4)$ then

$$\langle C(t, x')^2\rangle'\approx\langle C(t, x)^2\rangle'\approx H(n/2, \varepsilon)/Z$$

where $Z=\langle -I_{n/2}\rangle$. But $y\in\langle C(t, x)^2\rangle'$ and $y\in\langle C(t, x')^2\rangle'$ both correspond to involutions of type 2 in $H(n/2, \varepsilon)/Z$. Again a induces an isomorphism from $H(n/2, \varepsilon)/Z$ onto $H(n/2, \varepsilon)/Z$. However by [5] such an isomorphism comes from one on $H(n/2, \varepsilon)$ ($n \geq 6$, $n \neq 8$), which preserves the type of an involution. And the argument above applies. The proof of (d) and (e) is similar.

Lemma 3.5. *In (c) t is not conjugate (in G) to x_j, any i.*

Proof. Let $r=2^{s-3}$ if $k=1$, and $r=2^{s-2}$ if $k>1$.

(i) First we show no x_j is conjugate to t for $i \geq r$. Suppose on the contrary $x^a=t$, some $a \in G$, for $x=x_i$ $(i \geq r)$.

$$\text{Let } Y=\left(\begin{array}{cc|cc} I_{i-r} & & & \\ & -I_r & & 0 \\ \hline & 0 & -I_r & \\ & & & I_{n-i-r} \end{array}\right) \text{ then } y \sim y_{2r} \text{ in } F,$$

and so by (3.1) and (3.3) $y \in Z(M)$ for some S_2-subgroup M of F. Let $S=\langle t \rangle \times M$, an S_2-subgroup of G.

$$\text{Now } XY=\gamma\left(\begin{array}{cc|cc} -I_{i-r} & & & \\ & I_r & & 0 \\ \hline & 0 & -I_r & \\ & & & I_{n-i-r} \end{array}\right) \text{ which by (1.3)}$$

is projectively conjugate to X; *i.e.* $xy \sim x$ in F. So provided $y^a=y$ we have $ty \sim t$ in G, where t, $ty \in Z(S)$. And the argument of (3.4) leads to a contradiction.

(ii) If $r=1$ we are done. Otherwise we procede by induction to show x_{r-j} is not conjugate to t for $j=1, 3, \cdots, r-1$. Suppose $j=1$ and $x=x_{r-1}$ is conjugate to t.

$$\text{Let } Y=\begin{pmatrix} I_{r-2} & & 0 \\ 0 & -I_2 & \\ & & -I_{n-r} \end{pmatrix} \quad \text{and} \quad Y'=\begin{pmatrix} I_{r-1} & & 0 \\ 0 & -I_2 & \\ & & I_{n-r-1} \end{pmatrix}.$$

Then $xy \sim x$ in F and $xy' \sim x_{r+1}$ in F. (*)

But $x \sim t$. So suppose we may select conjugating elements a and a' such that $x^a=t$, $y^a=y$ and $x^{a'}=t$, $y'^{a'}=y'$. Then conjugating the relations (*) by a and a' respectively we obtain $t \sim ty$ in G, and $ty' \sim x_{r+1}$ in G. But $y \sim y'$ in F and so $ty \sim ty'$. Hence $t \sim x_{r+1}$ in G, a contradiction. So our claim is true for $j=1$ and similarly for $j=3, \cdots, r-1$. To complete the proof we show the assumptions made on the choice of conjugating elements are valid.

We are supposing $x_i^a=t$ and must show a centralizes y. As in (3.4) since $y_i \in C_F(y_j)'$ each j, we may assume $t^a=x_l$ or tx_l, some l. Thus $C(t, x_i)^a=C(t, x_l)$

which implies $i=l$ as in (3.4). Therefore $C(t, x)^a=C(t, x)$ where $x=x_i$. Now except in the case when $2||n$ and $i=\frac{n}{2}$, $C^*(X)=C(X)$. Therefore $C(t, x)'=C_F(X)'=(C(X)/Z(H(n, \varepsilon)))'$ and from (2.2) $C(X)'\approx H(i, \varepsilon)\times H(n-i, \varepsilon)$, with $Z(H(n, \varepsilon))\cap C(X)'\approx Z^*=\{(\lambda I_i, \lambda I_{n-i})\,|\,\lambda^i=\lambda^d=1\}$.

$$\text{Hence } C(t, x)'\approx(H(i, \varepsilon)\times H(n-i, \varepsilon))/Z^* = L_1 \text{ say}.$$

Now a induces an automorphism φ on L_1. The Krull-Schmidt theorem and the fact that every automorphism on $PH(n, \varepsilon))$ comes from one on $H(n, \varepsilon)$ for $n\geq 3$, and $n\neq 4$ when $\varepsilon=-1$ (Dieudonné [5]), show φ is induced from a direct product $\varphi_1\times\varphi_2$ of automorphisms on $H(i, \varepsilon)$ and $H(n-i, \varepsilon)$ respectively. Since φ_i $(i=1, 2)$ preserves the type of an involution, $y^a(y'^{a'})$ is an involution in L_1 of the same type as $y(y')$, and thus conjugate to $y(y')$ in F. The result follows.

When $2||n$ and $i=\frac{n}{2}$ we have from (2.2) $C(t, x)'=C_F(x)'=\langle C^*(x)\rangle/Z(H(n, \varepsilon))$, and $C(t, x)^{(2)}\approx(H(n/2, \varepsilon)\times H(n/2, \varepsilon))/Z^*=L_2$ say, where $Z^*=\{(\lambda I_{n/2}, \lambda I_{n/2}\,|\,\lambda^d=1\}$.

In this case $y\in C(t,x)^{(2)}$ corresponds to an involution of type $\left(\frac{n}{2}-1, \frac{n}{2}-1\right)$ in L_2. Again a induces an automorphism on L_2 which comes from one on $H(n/2, \varepsilon)\times H(2, \varepsilon)$. This automorphism either preserves the factors or interchanges them. In either case y^a is of the same type as y. So as above we may assume without loss of generality that a centralizes y. This completes the proof of theorem 1.1.

The material in this paper forms part of my doctoral thesis and I wish to thank my advisor Professor Warren Wong of the University of Notre Dame, for suggesting the problem.

UNIVERSITY OF AUCKLAND

References

[1] E. Artin: Geometric Algebra, Interscience, New York, 1957.

[2] R.W. Carter and P. Fong: *The Sylow 2-subgroups of the finite classical groups*, J. Algebra **1** (1965), 139–151.

[3] L.D. Dickson: Linear Groups, Dover, New York, 1958.

[4] J. Dieudonné: La Géométrie des Groupes Classiques. 3rd Edition, Springer, Berlin, 1971.

[5] J. Dieudonné: *On the automorphisms of classical groups*, Mem. Amer. Math. Soc. 2 (1971).

[6] Z. Janko: *A new finite simple group with Abelian S_2-subgroups and its characterization*, J. Algebra **3** (1966), 147–186.

[7] Z. Janko and J.G. Thompson: *On a class of finite simple groups of Ree*, J. Algebra **4** (1966), 274–292.

[8] J.G. Thompson: *Nonsolvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968), 383–437.

[9] W.J. Wong: *Characterization of the finite simple groups* $PSp_{2n}(q)$, J. Algebra **14** (1970), 431–551.

[10] W.J. Wong: *A characterization of finite orthogonal simple groups*, J. Algebra **28** (1974), 518–540.

[11] H. Yamaki: *On Janko's simple group of order* 175, 560, Osaka J. Math. **9** (1972), 111–112.