Real Representations of the Finite Orthogonal and Symplectic Groups of Odd Characteristic

R. Gow

Department of Mathematics, University College Dublin, Belfield, Dublin 4, Ireland

Communicated by Walter Feit
Received March 27, 1984

Let $q$ be a power of an odd prime $p$. Let $Sp(2n, q)$ denote the symplectic group of degree $2n$ over $GF(q)$. Let $O^+(n, q)$ denote the split orthogonal group of degree $n$ over $GF(q)$, corresponding to a symmetric form of maximal Witt index, and $O^-(n, q)$ denote the non-split orthogonal group. Unless we need to be more specific, we will simply write $O(n, q)$ for either of these two orthogonal groups. In addition, we will often abbreviate these symbols further to $O(n)$ and $Sp(2n)$ whenever $q$ is understood to be fixed.

It is known from conjugacy class considerations that all complex irreducible characters of the finite orthogonal groups $O(n)$ are real-valued. The same is true of the symplectic groups $Sp(2n, q)$ provided that $q \equiv 1 \pmod{4}$. When $q \equiv 3 \pmod{4}$, not all characters of $Sp(2n, q)$ are real-valued. However, as the total number of irreducible characters is a monic polynomial in $q$ of degree $n$ and this is true of the number of real-valued irreducible characters, we can assert that the majority of characters is real-valued in this case. It is of interest to know whether or not the real-valued characters of these families of groups are the characters of representations that are defined over the real numbers. This paper gives a solution to this problem by proving the following theorem.

**Theorem 1.** Let $q$ be a power of an odd prime. Each complex irreducible character of $O(n, q)$ is the character of a real representation. Each non-faithful real-valued irreducible character of $Sp(2n, q)$ is the character of a real representation, whereas each faithful real-valued irreducible character of the group has Schur index 2 over the real numbers.

The fact that all characters of the finite orthogonal groups are real-valued is a consequence of a general theorem of Wonenburger [10]. If $G$ denotes the orthogonal group of an arbitrary non-degenerate symmetric form over a field of characteristic not equal to 2, each element of $G$ is a
product of two involutions in $G$ and hence is conjugate to its inverse. A closer analysis of Wonenburger's proof shows that if $n = 4m$, each element of $O(n)$ is inverted by an involution of determinant 1. It is clear that this also holds when $n$ is odd. Consequently, all characters of the special orthogonal groups $SO(4m)$ and $SO(2m + 1)$ are real-valued. However, it can be shown that not all characters of $SO(4m + 2)$ are real-valued. A straightforward argument, whose details we omit, extends Theorem 1 to the special orthogonal groups.

**Theorem 2.** Let $q$ be a power of an odd prime. Each real-valued irreducible complex character of $SO(n, q)$ is the character of a real representation. If $n = 4m$ or $2m + 1$, all characters of $SO(n, q)$ are real-valued.

Wonenburger also showed that if $G$ denotes the symplectic group of a non-degenerate alternating form over a field $k$ of characteristic not equal to 2, each element of $G$ is inverted by a skew-symplectic involution. In this context, a skew-symplectic transformation carries the alternating form into its negative. Now if there exists an element $\lambda$ in $k$ with $\lambda^2 = -1$, which happens in $GF(q)$ if $q \equiv 1 \pmod{4}$, multiplication of a skew-symplectic involution by the scalar $\lambda$ produces a symplectic transformation of order 4. We see then that each element of $G$ is inverted by some element of order 4 in $G$. If $-1$ is not a square in $k$, it is shown in [3, Lemma 5.3] that certain unipotent elements of $G$ are not conjugate to their inverses. In particular, if $q \equiv 3 \pmod{4}$, it can be proved that an element of $Sp(2n, q)$ is real if and only if each of its elementary divisors of the form $(X \pm 1)^{2r}$, $r \geq 1$, occurs with even multiplicity. The methods of Wall [9] can then be invoked to show that the number of real classes in $Sp(2n, q)$, $q \equiv 3 \pmod{4}$, is the coefficient of $t^{2n}$ in the infinite product

$$\prod \frac{(1 + t^{4i})^2}{\prod (1 - qt^{2i})}$$

whereas the generating function for the total number of classes is [9, p. 36]

$$\prod \frac{(1 + t^{2i})^4}{\prod (1 - qt^{2i})}.$$ 

Thus, for example, when $q \equiv 3 \pmod{4}$, $Sp(4, q)$ contains $q^2 + 5q + 10$ classes, of which $q^2 + q + 2$ are real.

The Brauer–Speiser theorem and Theorem 1 imply that all real-valued faithful irreducible characters of $Sp(2n)$ have Schur index 2 over the rational numbers. On the other hand, when $q \equiv 3 \pmod{4}$, it seems probable that those irreducible characters of $Sp(2n, q)$ that are not real-valued, both faithful and non-faithful, have Schur index 1 over the
rational. A paper of Przygocki [11] shows that this is true for \( n \leq 2 \). It is perhaps worthwhile to mention that when \( q \) is a power of 2, all characters of \( O(n, q) \) and \( Sp(2n, q) \) are also real-valued [5]. It appears possible that there are underlying real representations for these characters, but the method we use to prove Theorem 1 is not suitable for dealing with groups of characteristic 2.

We mention here a numerical corollary of Theorem 1 which can be obtained from the Frobenius–Schur involution formula [2, p. 23].

**Theorem 3.** When \( q \equiv 1 \pmod{4} \), the sum of the degrees of the irreducible complex characters of the symplectic group \( Sp(2n, q) \) is given by

\[
q^{n(n+1)/2}(q^n + 1) \cdots (q + 1).
\]

**Proof.** Let \( G \) denote the symplectic group and \( PG \) the projective symplectic group. Given an irreducible character \( \chi \) of \( G \), we define \( v(\chi) \) by

\[
v(\chi) = (1/|G|) \sum \chi(g^2).
\]

Since all characters of \( G \) are real-valued, the theorem of Frobenius and Schur and Theorem 1 imply that \( v(\chi) = 1 \) if \( \chi \) is not faithful and \( v(\chi) = -1 \) otherwise. Let \( b \) denote the sum of the degrees of the faithful irreducible characters of \( G \) and \( c \) the sum of the degrees of the irreducible characters of \( PG \). Then the Frobenius–Schur involution formula yields that \( c - b \) equals the number of involutions in \( G \) and \( c \) the number of involutions in \( PG \).

We count now involutions in \( G \) and \( PG \). The images in \( PG \) of the \( c - b \) involutions in \( G \) give rise to \((c - b)/2\) involutions in \( PG \). A further class of involutions in \( PG \) is obtained from the images of the conjugates of the element

\[
\begin{bmatrix}
\lambda I_n & 0 \\
0 & \lambda^{-1} I_n
\end{bmatrix}
\]

where \( \lambda \) has order 4 in \( GF(q) \). Since the centralizer in \( G \) of the element above is isomorphic to \( GL(n, q) \), the number of involutions of \( PG \) that arise from the images of the conjugates of this element is \( |G : GL(n, q)|/2 \). This accounts for all involutions of \( PG \). We find then that

\[
b + c = |G : GL(n, q)|,
\]

which is equivalent to the statement of Theorem 3. This completes the proof.

We remark that Theorem 3 probably holds when \( q \equiv 3 \pmod{4} \), but our method of proof does not yield such a result.
In a previous paper [4], the author obtained a formula similar to that of Theorem 3 in the case of the general linear group $GL(n, q)$. Our proof of Theorem 1 follows very closely the method used in [4] and there are various points of overlap between the two papers. However, this paper requires a considerably more involved analysis of the conjugacy classes of the orthogonal and symplectic groups than that required for the general linear group. This is perhaps not surprising, as determination of invariants to describe the conjugacy classes in the first two groups is quite complicated.

Following the method developed in [4], we use induction on the degree of the groups and the Brauer-Witt theorem to prove Theorem 1. In principle, without using any properties of the characters, this involves investigation of all $\mathbb{R}$-elementary subgroups. However, wreath product and direct product constructions applied in conjunction with the induction hypothesis reduce the amount of explicit calculation. As far as we know, there is no a priori reason to suppose that our method of proof will be successful without knowledge of the characters or their construction. It is perhaps remarkable that the structure of the $\mathbb{R}$-elementary subgroups alone forces Theorem 1 to hold.

We will briefly describe the organization of the paper. In the first section, we explain how calculation of character invariants relevant to the Brauer-Witt theorem can be made. In the second and third sections, we investigate the real representations of certain subgroups of the orthogonal and symplectic groups. The fourth section, which is rather involved, analyses the $\mathbb{R}$-elementary subgroups and their embeddings in the orthogonal and symplectic groups. Finally, in the fifth section, we show how the proof of Theorem 1 can be reduced to checking properties of the real characters of certain specific types of $\mathbb{R}$-elementary subgroups. Theorem 1 is then proved by making the appropriate calculations for these subgroups.

1. The Brauer-Witt Theorem and $\mathbb{R}$-Elementary Subgroups

We begin by recalling that an $\mathbb{R}$-elementary subgroup of a finite group $G$ is either a Sylow 2-subgroup of $G$ or else has the form $N = AU$, where $A$ is the cyclic subgroup generated by a non-identity real element $g$ of odd order in $G$ and $U$ is a Sylow 2-subgroup of the extended centralizer $C^*(g)$ of $g$ in $G$. We can now state the Brauer-Witt theorem in the following form.

**Theorem** (Brauer and Witt). Let $\chi$ be a real-valued irreducible character of a finite group $G$. Then there exists an $\mathbb{R}$-elementary subgroup $N$ of $G$ and a real-valued irreducible character $\phi$ of $N$ such that $(\chi_N, \phi)$ is an odd integer. When $N = AU$, it can be assumed that $A$ is not contained in the kernel of $\phi$. We have $v(\chi) = v(\phi)$. 
Throughout this paper, the notation $N = AU$ will always refer to the $\mathbb{R}$-elementary subgroups that are not Sylow 2-subgroups of $G$. Similarly, $V$ will always denote the subgroup of index 2 in $U$ that centralizes $A$. If we replace the subgroup $U$ by another Sylow 2-subgroup of $C^*(g)$, the resulting $\mathbb{R}$-elementary subgroup $M$ is conjugate to $N$ and the conclusions of the theorem above clearly apply to $M$. Similarly, if we replace $g$ by a conjugate element, the corresponding $\mathbb{R}$-elementary subgroup is conjugate to $N$. This allows us to choose $g$ and $U$ in a form preferred for calculations.

We adopt the following approach to calculating the Frobenius–Schur invariants of the characters of $N$. Given an irreducible character $\theta$ of $V$, define the number $\eta(\theta)$ by

$$\eta(\theta) = (1/|V|) \sum_{x \in V} \theta(x^2),$$

the summation extending over all elements of $U - V$. Properties of $\eta(\theta)$ are described in [4]. We note in particular that $\eta(\theta) = 1$ for all irreducible characters of $V$ if and only if the sum of the degrees of the irreducible characters of $V$ equals the number of involutions in $U - V$. If $\phi$ is an irreducible character of $N$ that does not contain $A$ in its kernel, there is an irreducible character $\theta$ of $V$ such that $\eta(\theta) = \eta(\phi)$.

As we have explained, we reduce our proof of Theorem 1 to examination of the characters of certain minimal $\mathbb{R}$-elementary subgroups. In the orthogonal case, it turns out that $\eta(\theta) = 0$ or 1 for all irreducible characters $\theta$ of the relevant subgroups $V$. Thus, since no $\theta$ with $\eta(\theta) = -1$ arises, our discussion above will prove Theorem 1 in the orthogonal case. In the symplectic case, it happens that $\eta(\theta) = 0$ or 1 for all irreducible characters $\theta$ of $V$ that are trivial on the central involution of $Sp(2n)$ and $\eta(\theta) = 0$ or $-1$ otherwise. Again, this will prove Theorem 1 in the symplectic case.

2. REAL-VALUED CHARACTERS OF SOME SUBGROUPS

We begin by investigating the characters of direct products of orthogonal groups. Let $G_1, \ldots, G_r$ be orthogonal groups of degree $n_1, \ldots, n_r$ over $GF(q)$, where $n_1 + \cdots + n_r = n$ and each $n_i$ is less than $n$. Then, subject to Witt index considerations, the direct product $G_1 \times \cdots \times G_r$ can be embedded in a suitable orthogonal group $O(n)$. The following lemma is easily proved and we omit details.

**Lemma 2.1.** Assume that Theorem 1 holds for each of the orthogonal groups $G_i$. Then $\nu(\theta) = 1$ for each irreducible character $\theta$ of the direct product.
In a similar manner, let $H_1, \ldots, H_r$ be symplectic groups of degree $2n_1, \ldots, 2n_r$ over $GF(q)$, where $n_1 + \cdots + n_r = n$ and each $n_i$ is less than $n$. We can embed the direct product $H_1 \times \cdots \times H_r$ into $H = Sp(2n)$ in an obvious orthogonal manner. Let $z_i$ be the central involution of $H_i$, $1 \leq i \leq r$. Then $z = (z_1, \ldots, z_r)$ is the central involution of $H$. The next lemma is the analogue of Lemma 2.1 for the symplectic group.

**Lemma 2.2.** Assume that Theorem 1 holds for each of the symplectic groups $H_i$. Let $\theta$ be a real-valued irreducible character of the direct product $H_1 \times \cdots \times H_r$. Then $\nu(\theta) = 1$ if and only if the central involution $z$ of $Sp(2n)$ is contained in the kernel of $\theta$.

**Proof.** The irreducible character $\theta$ can be expressed as a product $\theta = \theta_1 \times \cdots \times \theta_r$, where each $\theta_i$ is a real-valued irreducible character of $H_i$. It is straightforward to verify that $\nu(\theta) = \nu(\theta_1) \cdots \nu(\theta_r)$ and $\theta(z) = \theta_1(z_1) \cdots \theta_r(z_r)$. Assuming that Theorem 1 holds for each $H_i$, we have $\nu(\theta_i) = -1$ if and only if $\theta_i(z_i) = -\theta_i(1)$. Thus if there are exactly $t$ indices $i$ for which $\nu(\theta_i) = -1$, we see that $\nu(\theta) = (-1)^t$ and $\theta(z) = (-1)^t \theta(1)$. Clearly, $\nu(\theta) = 1$ if and only if $\theta(z) = \theta(1)$. This completes the proof.

We consider next a simple wreath product construction. Let $G$ be a group and let the elements of the direct product $G \times G$ be written as ordered pairs $(g, h)$. The wreath product $G \wreath Z_2$ of $G$ by a cyclic group of order 2 is a split extension of $G \times G$ by an involution $t$ that acts on $G \times G$ according to the rule $t(g, h) = (h, g)$. The next lemma was proved by Kerber in [8, Theorem 43].

**Lemma 2.3.** Suppose that $G$ is a finite group and that $\nu(\chi) = 1$ for all irreducible characters $\chi$ of $G$. Then each irreducible character $\theta$ of $G \wreath Z_2$ also satisfies $\nu(\theta) = 1$.

We will be particularly interested in this wreath product construction when the centre of $G$ is cyclic of order 2. In this case, let $z$ generate the centre of $G$. We can see then that the involution $(z, z)$ generates the centre of $G \wreath Z_2$. The next lemma is concerned with this situation.

**Lemma 2.4.** Let $G$ be a finite group whose centre is cyclic of order 2 and let $\chi$ be any real-valued irreducible character of $G$. Suppose that $\nu(\chi) = 1$ if and only if the central involution of $G$ is contained in the kernel of $\chi$. Let $\theta$ be a real-valued irreducible character of $H = G \wreath Z_2$. Then $\nu(\theta) = 1$ if and only if the central involution of $H$ is contained in the kernel of $\theta$.

**Proof.** We begin by recalling the construction of the irreducible representations and characters of $H$. Let $F_1, \ldots, F_r$ denote the inequivalent irreducible representations of $G$ and let the characters of these represen-
GROUPS OF ODD CHARACTERISTIC

An irreducible representation $E$ of $G \times G$ can be written as a tensor product of the form $F_i \otimes F_j$, $1 \leq i, j \leq r$. If $i \neq j$, the induced representation $E^H$ of $H$ is irreducible. Moreover, the central involution of $H$ is not contained in the kernel of $E^H$ if and only if the central involution of $G$ is not contained in the kernel of exactly one of $F_i$, $F_j$. If $i = j$, $E$ can be extended to two distinct representations of $H$, both of which are trivial on the central involution of $H$.

Suppose now that $i \neq j$. Denote the irreducible character $\chi_i \times \chi_j$ of $G \times G$ by $\psi$. The induced character $\psi^H$ is real-valued if and only if either $\chi_i$ and $\chi_j$ are both real-valued or $\chi_i = \overline{\chi}_j$, calculation of $\nu(\psi^H)$ from its definition shows that its value is 1. Since the central involution of $H$ is clearly contained in the kernel of $\psi^H$, the lemma holds here. If $\chi_i$, $\chi_j$ are both real-valued, $\psi$ is also real-valued and $\nu(\psi) = \nu(\chi_i) \nu(\chi_j)$. A standard argument shows that $\nu(\psi^H) = \nu(\psi)$. It is now routine to check that the lemma holds again in this case.

Finally, if $i = j$, the character $\psi$ is real-valued if and only if $\chi_i$ is real-valued and then we have $\nu(\psi) = \nu(\chi_i)^2 = 1$. Application of the Frobenius–Schur formula shows that the extensions of $\psi$ to $H$ are both real-valued and have Frobenius–Schur number equal to 1. Since we have already observed that the central involution of $H$ is contained in the kernel of these extensions of $\psi$, the lemma is now proved in all cases.

We will prepare another step in the proof of Theorem 1 by appealing to the main theorem of [4]. Let $GL(n)$ denote the general linear group $GL(n,q)$. We let $GL(n)^+$ denote the split extension of $GL(n)$ by an involution that induces the transpose-inverse automorphism on $GL(n)$. It will be seen later that $GL(n)^+$ arises naturally as a subgroup of $O^+(2n)$. Theorem 2 of [4] shows that $GL(n)^+$ has a real splitting field. In connection with the symplectic group a similar extension of $GL(n)$ occurs as a subgroup. Let $GL(n)^-$ denote the extension of $GL(n)$ by an element $w$ of order 4 that satisfies $w^2 = -I$ and $w^{-1}xw = x^*$, for all $x$ in $GL(n)$, where $x^*$ is the transpose-inverse of $x$. Clearly, the central involution $-I$ of $GL(n)$ generates the centre of $GL(n)^-$. We omit the proof of the next lemma, as it is a formal calculation of Frobenius–Schur numbers that makes use of Theorem 2 of [4].

**Lemma 2.5.** Let $\chi$ be an irreducible character of $GL(n)^-$. We have $\nu(\chi) = 1$ if the central involution of $GL(n)^-$ is contained in the kernel of $\chi$ and $\nu(\chi) = 0$ or $-1$ otherwise.
3. SYLOW 2-SUBGROUPS OF CLASSICAL GROUPS
AND THEIR CHARACTERS

As a step in the description of the structure of $\mathbb{R}$-elementary subgroups of the orthogonal and symplectic groups, we need to know the construction of the Sylow 2-subgroups of the classical groups of odd characteristic. The paper of Carter and Fong [1] shows that the Sylow 2-subgroups are essentially all constructed by direct product and wreath product techniques. The Sylow 2-subgroups of the orthogonal groups require slightly more care in their description. For the sake of brevity in this and subsequent sections, we will write $S_2$ for Sylow 2-subgroup.

We consider first an $S_2$ of $G = Sp(2n)$. Let $2n = 2^{b_1} + \cdots + 2^{b_l}$ be the 2-adic decomposition of $2n$, with $1 \leq b_1 < \cdots < b_l$. Then an $S_2$, $T(2n)$, of $G$ is isomorphic to a direct product

$$T(2^{b_1}) \times \cdots \times T(2^{b_l}),$$

where each $T(2^{b_i})$ is an $S_2$ of $Sp(2^{b_i})$. Moreover, if $b \geq 2$, $T(2^b)$ can be constructed as a wreath product $T(2^{b-1}) \wr \mathbb{Z}_2$, as described in the previous section. The group $T(2)$ is generalized quaternion. We note in particular that the centre of $T(2^n)$ is generated by the unique central involution of $Sp(2^b)$.

A similar description can be given for an $S_2$ of the unitary group $U(n, q^2)$. Only an $S_2$ of $U(2, q^2)$ requires special attention, which we defer until the final section. Finally, we consider an $S_2$ of $O(n)$. The description here is slightly more complicated because of the interplay between the two Witt types of non-degenerate symmetric forms. We present information extracted from [1] in the next lemma.

**Lemma 3.1.** Let $T^+(2n)$, $T^-(2n)$, $T(2n+1)$ denote Sylow 2-subgroups of $O^+(2n)$, $O^-(2n)$, $O(2n+1)$, respectively. Then we have the following isomorphisms.

(a) $T(4m+3) \cong T^+(4m) \times T(3)$,
(b) $T^+(3) \cong T^+(2) \times T(1)$ for $q \equiv 1 \pmod{4}$,
(c) $T^-(3) \cong T^-(2) \times T(1)$ for $q \equiv 3 \pmod{4}$,
(d) $T(4m+1) \cong T^+(4m) \times T(1)$,
(e) $T^+(4m+2) \cong T^+(4m) \times T^+(2)$,
(f) $T^-(4m+2) \cong T^+(4m) \times T^-(2)$,
(g) $T^-(4m) \cong T^+(4m-2) \times T^-(2)$ for $q \equiv 3 \pmod{4}$,
(h) $T^-(4m) \cong T^-(4m-2) \times T^+(2)$ for $q \equiv 1 \pmod{4}$.

These direct product factorizations are compatible with orthogonal decompositions of the underlying vector space into subspaces of the
appropriate Witt type. We also need to describe the structure of an $S_2$ of $O^+(4m)$.

**Lemma 3.2.** Let $4m = 2^{b_1} + \cdots + 2^{b_t}$ be the 2-adic decomposition of $4m$, with $2 \leq b_1 < \cdots < b_t$. Then
\[
T^+(4m) \cong T^+(2^{b_1}) \times \cdots \times T^+(2^{b_t}).
\]
If $b \geq 3$, $T^+(2^b) \cong T^+(2^{b-1}) \wr \mathbb{Z}_2$. If $q \equiv 1 \pmod{4}$, $T^+(4) \cong T^+(2) \wr \mathbb{Z}_2$ and if $q \equiv 3 \pmod{4}$, $T^+(4) \cong T^-(2) \wr \mathbb{Z}_2$. The groups $T^+(2)$, $T^-(2)$ are dihedral.

We can now investigate the real representations of the Sylow 2-subgroups of the orthogonal and symplectic groups.

**Lemma 3.3.** Let $T$ be a Sylow 2-subgroup of $O(n)$. Then we have $\nu(\theta) = 1$ for all irreducible characters $\theta$ of $T$.

**Proof.** It is well known that all complex irreducible representations of a finite dihedral group are realizable over the real numbers. Lemma 2.3 implies that the conclusion of our lemma holds for the repeated wreath product of a dihedral group with $\mathbb{Z}_2$. Since we know from Lemmas 3.1 and 3.2 that $T$ is a direct product of such repeated wreath products, the proof of the lemma is immediate.

**Lemma 3.4.** Let $T$ be a Sylow 2-subgroup of $Sp(2n)$ and let $\theta$ be an irreducible character of $T$. Then we have $\nu(\theta) = 1$ if the central involution of $Sp(2n)$ is contained in the kernel of $\theta$ and $\nu(\theta) = -1$ otherwise.

**Proof.** When $n = 1$, $T$ is generalized quaternion and the lemma is familiar in this case. Arguing by induction, we see from Lemma 2.4 that our lemma is true when $T$ is a repeated wreath product of a generalized quaternion group with $\mathbb{Z}_2$. Since in the general case, $T$ is a direct product of such wreath products, the argument of Lemma 2.2 shows that the lemma holds for all $T$.

4. **Conjugacy Classes and $\mathbb{R}$-Elementary Subgroups**

Let $g$ be a real element of an orthogonal or symplectic group $G$. To describe the structure of the $\mathbb{R}$-elementary subgroup $N = AU$ defined in Section 1, it is first necessary to relate the conjugacy class of $g$ in $G$ to the elementary divisors of $g$. A paper of Wall [9] gives detailed information on this problem and we will refer repeatedly to this work in the course of the next two sections. Another convenient reference for us is a paper of Hup-
which gives a good account of orthogonal decompositions of the underlying vector space into $g$-invariant subspaces.

We will briefly mention certain general principles concerning conjugacy classes and centralizers which are implicit in Wall's work. Let $x, y$ be two elements of $G$ having no eigenvalues equal to $\pm 1$. Then $x, y$ are conjugate in $G$ if and only if they are conjugate in the full linear group. (This exploits the fact that we are working over a finite field.) The situation concerning the conjugacy of those elements all of whose eigenvalues are $\pm 1$ is more complicated and will be discussed later in this section. If $C$ is the centralizer of $g$ in $G$ and $R$ is its unipotent radical, $C/R$ is a direct product of orthogonal, symplectic, general linear or unitary groups over finite extensions of $GF(q)$. Thus an $S_2$ of $C$ is isomorphic to a direct product of $S_2$'s of the classical groups and we will try to relate its structure to the elementary divisors of $g$. In this way, it will be possible to show that $N$ is generally contained in a subgroup whose real-valued characters may be assumed to have known properties.

Let $m(X)$ denote the minimal polynomial of $g$ and let $d$ be the degree of $m(X)$. We define the adjoint polynomial $m^*(X)$ to equal $m(0)^{-1}X^dm(X^{-1})$. This is the minimal polynomial of $g^{-1}$. Since all elements of the orthogonal and symplectic groups are real elements of the general linear group, we have $m^*(X) = m(X)$ and we say that $m(X)$ is self-adjoint. We can arrange the distinct irreducible monic factors of $m(X)$ into two types: $h_i(X), h_i^*(X), \ldots, h_i(X), h_i^*(X)$ and $f_i(X), \ldots, f_i(X)$. Here, the $f_i(X)$ are self-adjoint and the $h_i(X)$ are not. If $M$ is the vector space on which $g$ acts, there is a canonical orthogonal decomposition

$$M = M_1 \perp \cdots \perp M_{r+t}$$

of $M$ into $r+t$ $g$-invariant subspaces. This follows from the primary decomposition of $M$. Retaining this notation, we prove a sequence of embeddings for $N = AU$.

**Lemma 4.1.** $N$ is contained in a direct product $G_1 \times \cdots \times G_{r+t}$, where the $G_i$ are orthogonal groups in the orthogonal case, and symplectic groups in the symplectic case.

**Proof.** The orthogonal decomposition of $M$ just discussed shows that $g$ is conjugate in $G$ to an element of the form

$$(g_1, \ldots, g_{r+t})$$

in a direct product $G_1 \times \cdots \times G_{r+t}$ of orthogonal or symplectic groups. Since we are working up to conjugacy in $G$, we can take $g$ to be this block diagonal element. Now each element $g_i$ is a real element of $G_i$, as can easily
be shown. Since the centralizer of $g$ in $G$ is the direct product of the centralizers of the elements $g_i$ in $G_i$, we see that $N$ is certainly contained in the direct product of the $G_i$. This completes the proof.

**Lemma 4.2.** Suppose that $m(X) = h(X) h^*(X)$, where $h(X)$ is a power of an irreducible polynomial that is not self-adjoint. Then $N$ is contained in a subgroup of type $GL(n)^+$ if $G = O(2n)$ and of type $GL(n)^-$ if $G = Sp(2n)$.

**Proof.** Let $M = K \oplus L$ be the primary decomposition of $M$ into $g$-invariant subspaces corresponding to the coprime divisors of $m(X)$. Both subspaces $K$ and $L$ are totally isotropic with respect to the $g$-invariant form [6, Lemma 1.6]. We take bases of $K$ and $L$ that are dual with respect to the form. Then we can take $g$ to equal a block diagonal element of the type

$$(z, z^*),$$

where $z$ is an element of $GL(n)$ and $z^*$ is its transpose-inverse. The centralizer of $g$ in $G$ then consists of all elements of the form

$$(c, c^*),$$

where $c$ belongs to the centralizer of $z$ in $GL(n)$. We now make use of the fact that, by a theorem of Frobenius [7, Theorem 66] there is a symmetric matrix $s$ that satisfies

$$s^{-1}zs = z',$$

where $z'$ is the transpose of $z$.

Suppose firstly that the form is symmetric. The involution $t$ given by

$$t = \begin{bmatrix} 0 & s \\ s^{-1} & 0 \end{bmatrix}$$

preserves the form and inverts $g$. Since $s$ is symmetric, $t$ can be written as

$$t = \begin{bmatrix} s & 0 \\ 0 & s^* \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}.$$

We see then that $C^*(g)$ is contained in the subgroup of $G$ generated by all elements of the form

$$\begin{bmatrix} x & 0 \\ 0 & x^* \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix},$$

as $x$ ranges over $GL(n)$. Clearly, this subgroup is isomorphic to $GL(n)^+$. 
Suppose now that the form is skew-symmetric. The element $w$ of order 4 given by

$$w = \begin{bmatrix} s & 0 \\ 0 & s^* \end{bmatrix} \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} = \begin{bmatrix} 0 & s \\ -s^{-1} & 0 \end{bmatrix}$$

preserves the form and inverts $g$. Thus we can see that $C^*(g)$ is now contained in the subgroup generated by all elements of the form

$$\begin{bmatrix} x & 0 \\ 0 & x^* \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix},$$

where $x$ ranges over $GL(n)$. This subgroup is isomorphic to $GL(n)^-$, as required.

**Lemma 4.3.** Suppose that $m(X)$ is a power of an irreducible self-adjoint polynomial $f(X)$. Let the distinct elementary divisors of $g$ be

$$f(X)^{b_1}, \ldots, f(X)^{b_j},$$

where $b_1 < \cdots < b_j$. Then $N$ is contained in a direct product $G_1 \times \cdots \times G_j$ of orthogonal or symplectic groups.

**Proof.** There is a (non-canonical) orthogonal decomposition of the space $M$ into a direct sum

$$M = L_1 \perp \cdots \perp L_j$$

of $g$-invariant subspaces, such that the restriction of $g$ to $L_i$ has the single type of elementary divisor $f(X)^{b_i}$. Thus, up to conjugacy in $G$, we can assume that $g$ equals a block diagonal element $(g_1, \ldots, g_j)$, which is contained in a direct product $G_1 \times \cdots \times G_j$ of orthogonal or of symplectic groups. It can be shown that each element $g_i$ is also a real element of $G_i$.

Formulae are given in [9, pp. 36–39] for the order of $C(g)$. These formulae show that an $S_2$ of $C(g)$ can be taken to be a direct product $V_1 \times \cdots \times V_j$, where $V_i$ is an $S_2$ of the centralizer of $g_i$ in $G_i$. This decomposition is compatible with the orthogonal decomposition of $M$. It can now be seen that the subgroup $N$ is contained in the direct product $G_1 \times \cdots \times G_j$. This completes the proof.

At this point, our analysis must be broken into two distinct cases. When the polynomial $f(X)$ of Lemma 4.3 has even degree, we are led to study Sylow 2-subgroups of the unitary group. When the polynomial $f(X)$ is $X - 1$, we must study Sylow 2-subgroups of the orthogonal and symplectic groups.
LEMMA 4.4. Suppose that \( g \) has a single type of elementary divisor \( f(X)^{b_i} \), repeated \( c \) times, where \( f(X) \) is an irreducible self-adjoint polynomial of even degree \( 2d \). Let \( c = 2^n + \cdots + 2^m \) be the 2-adic decomposition of \( c \). Then \( N \) is contained in a direct product \( G_1 \times \cdots \times G_t \) of orthogonal or symplectic groups. If \( c = 2^a \) and \( a \geq 2 \), \( N \) is contained in \( H \wr Z_2 \), where \( H \) is an orthogonal or symplectic group of degree half that of \( G \).

Proof. Theorem 2.6 of [6] shows that there is an orthogonal decomposition
\[
M = M_1 \perp \cdots \perp M_c
\]
of \( M \) into \( c \) \( g \)-invariant isomorphic subspaces \( M_i \). When the underlying form is symmetric, Wall's results show that the subspaces \( M_i \) all have the same Witt type. Thus, up to conjugacy in \( G \), we see that \( g \) equals a block diagonal element
\[
(h_1, \ldots, h_c)
\]
which is contained in a direct product \( H_1 \times \cdots \times H_c \) of isomorphic orthogonal or symplectic groups. Furthermore, as we are working over a finite field and the elements \( h_i \) are conjugate in the general linear group and have no eigenvalues equal to \( \pm 1 \), Wall's results show that up to conjugacy in \( G \), we can take the \( h_i \) to be all equal. Thus, we can assume that we have
\[
g = (h, \ldots, h),
\]
where \( h \) acts indecomposably on the underlying space.

Now it can be shown that \( C(g) \) factored by its unipotent radical is isomorphic to \( U(2^n, q^{2d}) \). Thus an \( S_2 \) of \( C(g) \) is isomorphic to an \( S_2 \) of \( U(2^n, q^{2d}) \). We also know from [1] that corresponding to the 2-adic decomposition of \( c \), an \( S_2 \) of \( U(c, q^{2d}) \) is expressible as a direct product of \( S_2 's \) of \( U(2^{a_i}, q^{2d}) \), \( 1 \leq i \leq t \). Write \( g \) in the form
\[
g = (g_1, \ldots, g_t),
\]
where each \( g_i \) is a sum of \( 2^{a_i} \) copies of \( h \). An \( S_2 \) of the centralizer of \( g_i \) in the appropriate orthogonal or symplectic group is isomorphic to an \( S_2 \) of \( U(2^{a_i}, q^{2d}) \). Thus we see that an \( S_2 \) of \( C(g) \) can be taken to be a direct product of the \( S_2 's \) of the centralizers of the \( g_i \). Since each element \( g_i \) is real in the appropriate classical group, it is clear that \( N = AU \) is contained in \( G_1 \times \cdots \times G_t \), as required.

We consider in greater detail the case that \( c = 2^a \) is a power of 2. We know from [1] that an \( S_2 \) of \( U(2^a, q^{2d}) \) is a wreath product of an \( S_2 \) of \( U(2^{a-1}, q^{2d}) \) with \( Z_2 \), provided that \( a \geq 2 \). Write \( g \) as \( (k, k) \), where \( k \) is a
sum of $2^{n-1}$ copies of $h$, and let $H$ denote an orthogonal or symplectic group of degree half that of $G$, with $k$ contained in $H$. Since an $S_2$ of $C_t(h)$ is isomorphic to an $S_2$ of $U(2^{n-1}, q^{2d})$, and $h$ is a real element of $H$, it is clear from our knowledge of the structure of an $S_2$ of $C_g(g)$ that $N = AU$ is contained in $H \wr Z_2$. We note that this description holds good when $c = 2$ and $q^d \equiv 3 \pmod{4}$. This completes the proof.

The last part of the analysis of the subgroup $N$ is concerned with the case that $g$ is unipotent. Suppose then that $g$ has the single type of elementary divisor $(X - 1)^m$. When $m$ is odd and $G$ is $Sp(2n)$, the multiplicity of this elementary divisor must be even, $2c$, say. Similarly, when $m$ is even and $G$ is $O(n)$, the multiplicity must also be even and we will denote it again by $2c$. These two cases can be treated together. Theorem 2.4 of [6] shows that there is an orthogonal decomposition

$$M = M_1 \perp \cdots \perp M_c$$

of the space $M$ into $c$ subspaces, each of dimension $2m$, that are $g$-invariant. Each subspace $M_i$ is a direct sum of two totally isotropic subspaces invariant under $g$. It is then straightforward to see that we can take $g$ to equal a block diagonal element,

$$g = (h, \ldots, h),$$

where we have $c$ copies of $h$. By Case B(iv) and Case C(iv) of [9, pp. 36–39], we find that an $S_2$ of $C(g)$ is isomorphic to an $S_2$ of $Sp(2c)$. By making use of the description of an $S_2$ of the symplectic group given in Section 3, and imitating the proof of Lemma 4.4, we can prove the lemma which follows. We omit details of the proof, as it is virtually identical with that of the previous lemma.

**Lemma 4.5.** Suppose that $g$ has the single type of elementary divisor $(X - 1)^m$, occurring with multiplicity $2c$. Suppose that $m$ is even in the orthogonal case and odd in the symplectic case. Then if $c$ is not a power of 2, $N$ is contained in a direct product of orthogonal groups or of symplectic groups, each of degree less than that of $G$. If $c$ is a power of 2 greater than 1, $N$ is contained in $H \wr Z_2$, where $H$ is an orthogonal or symplectic group of degree half that of $G$.

There remains the case that $g$ has a single type of elementary divisor $(X - 1)^m$, with $m$ odd in the orthogonal case and $m$ even in the symplectic case. The analysis is complicated here for two reasons. The first is that in $Sp(2n)$, there are two conjugacy classes corresponding to these elementary divisors. Moreover, when $q \equiv 3 \pmod{4}$, the multiplicity of $(X - 1)^m$ as an elementary divisor must be even in order that $g$ should be a real element of
Sp\(2n\)). The second reason is that in the orthogonal case, we must distinguish between the two equivalence classes of forms of odd degree over \(GF(q)\).

We consider first the orthogonal case. Let \(m = 2k + 1\) and let \(c\) be the multiplicity of \((X - 1)^{2k+1}\) as an elementary divisor of \(g\). Our group \(G\) is now \(O(mc)\). There is then an orthogonal decomposition

\[
M = M_1 \perp \cdots \perp M_c
\]

into isomorphic \(g\)-invariant subspaces, each having odd dimension \(2k + 1\). It is easily shown that there is a single conjugacy class in \(O(2k + 1)\) that contains a regular unipotent element having the single elementary divisor \((X - 1)^{2k+1}\). It follows then that we can take \(g\) to be a block diagonal element

\[
g = (h, \ldots, h),
\]

with \(c\) copies of \(h\).

Let us say that a vector space of odd dimension over \(GF(q)\) equipped with a non-degenerate symmetric form is of type \(+1\) if the form is represented by a matrix whose determinant is a square and of type \(-1\) otherwise. It is then straightforward to show that two \(g\)-invariant subspaces of type \(-1\) in the orthogonal decomposition above can be replaced by two subspaces of type \(+1\), each having the same \(g\)-action as the original subspaces. Thus we can assume that all the subspaces \(M_i\) are of type \(+1\) or all but one are of type \(+1\).

We wish to investigate the structure of the subgroup \(N = AU\). According to Wall \([9, p. 391]\), an \(S_2, V\), of \(C(g)\) is isomorphic to an \(S_2\) of \(O(c, q), T(c)\), say, where the type of orthogonal group depends on \(q\) and the parity of the number of subspaces having type \(+1\). Consider the case \(c = 4d + 1\). Using the notation of Lemma 3.1, we have

\[
T(4d + 1) \cong T^+(4d) \times T(1).
\]

We can then see that we can take \(V\) to be contained in \(O^+(4dm) \times O(m)\), where, as before, \(m = 2k + 1\). It follows easily that \(N\) is contained in this product of orthogonal groups. Similarly, when \(c = 4d + 3\), we can show that \(N\) is contained in \(O^+(4dm) \times O(3m)\). In a like manner, if \(c = 3\), we can show that \(N\) is contained in \(O^+(2m) \times O(m)\).

Suppose next that \(c = 4d + 2\). Using parts (e) and (f) of Lemma 3.1, we can show that \(N\) is contained in \(O^+(4md) \times O^\pm(2m)\). Finally, we consider the case that \(c = 4d\). Suppose that exactly one of the subspaces \(M_i\) has type \(-1\). An \(S_2\) of \(C(g)\) is isomorphic to an \(S_2 T^-(4d)\) of \(O^-(4d)\). Since by Lemma 3.1(d), we have

\[
T^-(4d) \cong T(4d - 1) \times T(1),
\]
we can invoke previous arguments to conclude that $N$ is contained in $O((4d-1)m) \times O(m)$. Now we consider what happens when all the subspaces $M_i$ have type +1. An $S_2$ of $C(g)$ is isomorphic to an $S_2$ of $O^+(4d)$. By referring to Lemma 3.2 and using the arguments of Lemma 4.4, we can show that $N$ is contained in a direct product of orthogonal groups of degree smaller than that of $G$ or in a wreath product $H \wr Z_2$, where $H$ is an orthogonal group of degree half that of $G$. We summarize all this information in the next lemma.

**Lemma 4.6.** Suppose that $g$ is a unipotent element of the orthogonal group $G$ and that $g$ has a single elementary divisor $(X-1)^{2k+1}$, occurring $c$ times. Then, unless $c = 1$ or 2, $N$ is contained in a direct product of orthogonal groups of degree smaller than that of $G$ or in a wreath product $H \wr Z_2$, where $H$ is an orthogonal group of degree half that of $G$.

The final part of our analysis of the subgroup $N$ concerns the case when $g$ is a unipotent element in the symplectic group $G$. Suppose that $g$ has the single elementary divisor $(X-1)^{2k}$, occurring with multiplicity $c$. The work of Wall shows that $Sp(2k)$ has two conjugacy classes of regular unipotent elements having minimal polynomial $(X-1)^{2k}$. Let $u, v$ be representatives of these classes. There is an orthogonal decomposition

$$M = M_1 \perp \cdots \perp M_c$$

of the space $M$ into $c$ $g$-invariant subspaces $M_i$, each of dimension $2k$. We see then that $g$ is conjugate to an element $(g_1, \ldots, g_c)$, where each $g_i$ is an element of $Sp(2k)$ equal to $u$ or $v$. Now it can be shown that in $Sp(4k)$, the element $(u, u)$ is conjugate to $(v, v)$. It follows that $g$ is conjugate to

$$(u, \ldots, u) \quad \text{or} \quad (u, \ldots, u, v)$$

and we can take $g$ to equal one of these two elements. We note in particular that there are exactly two classes in $G$ that correspond to the stated divisors. We also note that if $q \equiv 3 \pmod{4}$, $u$ is not a real element of $Sp(2k)$ and thus we can take $v = u^{-1}$. It can then be proved that if $q \equiv 3 \pmod{4}$, $g$ is real in $G$ if and only if $c$ is even.

Let $V$ denote an $S_2$ of $C(g)$. Wall's work shows that $V$ is isomorphic to an $S_2$ of $O(c, q)$. The type of orthogonal group here depends on $q$ and on which of the two conjugacy classes of $G$ that $g$ belongs to. Suppose first that $c$ is odd. Then we must have $q \equiv 1 \pmod{4}$ and both $u$ and $v$ are real elements of $Sp(2k)$. The element $g$ can be taken to equal either $(u, \ldots, u)$ or $(v, \ldots, v)$. The arguments used to prove Lemma 4.6 can be adapted to this situation to show that $N$ is contained in a direct product of symplectic groups of smaller degree than that of $G$, unless $c = 1$. 

We consider next the case that \( c = 2d \) is even. If \( q \equiv 1 \pmod{4} \) and \( g = (u, \ldots, u) \), \( V \) is isomorphic to an \( S_2 \) of \( O^*(2d) \). Again, the arguments used to prove Lemma 4.6 can be applied to show that, unless \( c = 2 \), \( N \) is contained either in a direct product of symplectic groups each of degree less than that of \( G \) or in a wreath product \( H \wr \mathbb{Z}_2 \), where \( H \) is a symplectic group of degree half that of \( G \). Similarly, if \( q \equiv 1 \pmod{4} \) and \( g = (u, \ldots, u, v) \), \( V \) is isomorphic to an \( S_2 \) of \( O^-(2d) \). It is then routine to show that \( N \) is contained in a direct product of symplectic groups each of degree less than that of \( G \).

There remains the case that \( c \) is even and \( q \equiv 3 \pmod{4} \). The analysis is slightly complicated in that while \( u \) and \( v \) are not real elements of \( Sp(2k) \), the elements \( (u, u) \) and \( (u, v) \) are real elements of \( Sp(4k) \). If \( g = (u, \ldots, u) \) and \( c \equiv 0 \pmod{4} \), \( V \) is isomorphic to an \( S_2 \) of \( O^+(c) \). We can then show that \( N \) is contained in a direct product of symplectic groups each of degree less than that of \( G \) or in \( H \wr \mathbb{Z}_2 \), where \( H \) is a symplectic group of degree half that of \( G \). Similarly, if \( g \) has the form above and \( c \equiv 2 \pmod{4} \), \( V \) is isomorphic to an \( S_2 \) of \( O^-(c) \). Then, unless \( c = 2 \), we find that \( N \) is contained in a direct product of symplectic groups of degree smaller than that of \( G \).

If \( g = (u, \ldots, u, v) \) and \( c \equiv 0 \pmod{4} \), \( V \) is isomorphic to an \( S_2 \) of \( O^-(c) \). We can then show that \( N \) is contained in a direct product of symplectic groups each of smaller degree than that of \( G \). Finally, if \( c \equiv 2 \pmod{4} \) and \( g \) has the form above, \( V \) is isomorphic to an \( S_2 \) of \( O^+(c) \) and the same conclusion can be obtained as when \( c \equiv 0 \pmod{4} \), with the exception of the case that \( c = 2 \).

Putting this analysis together, our final lemma of this section is a symplectic version of Lemma 4.6.

**Lemma 4.7.** Suppose that \( g \) is a unipotent element of the symplectic group \( G \) and that \( g \) has a single type of elementary divisor \( (X - 1)^{2k} \), occurring \( c \) times. Then unless \( c = 1 \) or \( 2 \), \( N \) is contained in a direct product of symplectic groups each of degree less than that of \( G \), or in a wreath product \( H \wr \mathbb{Z}_2 \), where \( H \) is a symplectic group of degree half that of \( G \).

5. **Proof of Theorem 1**

We proceed by induction on \( n \). Initially, we will not need to distinguish between \( O(n) \) and \( Sp(2n) \) and we will let \( G \) denote either group. The theorem is known to be true for \( Sp(2) \), although our methods can be used to prove this, and is trivially true for \( O(1) \).

Let \( \chi \) be an irreducible real-valued character of \( G \). By the Brauer–Witt theorem, there is an \( \mathbb{R} \)-elementary subgroup \( N \) of \( G \) and a real-valued
irreducible character \( \theta \) of \( N \) such that \( (\chi_N, \theta) \) is an odd integer. Now if \( M \) is any subgroup of \( G \) that contains \( N \), it can be seen that there must be a real-valued irreducible character \( \phi \) of \( M \) with \( (\chi_M, \phi) \) also an odd integer. We have then \( v(\chi) = v(\theta) = v(\phi) \). In the case that \( G \) is \( Sp(2n) \), \( N \) and \( M \) must contain the central involution of \( G \). Thus if \( \chi \) is a faithful character, the central involution of \( G \) cannot be contained in the kernel of either \( \theta \) or \( \phi \).

We consider the various possibilities for the structure of \( N \), eventually reducing the proof to three "primitive" cases that involve explicit calculation. As a first case, suppose that \( N \) is a Sylow 2-subgroup of \( G \). Lemmas 3.3 and 3.4 immediately show that Theorem 1 must hold in this case. Thus, for the rest of the proof, we will assume that \( N = A U \), as described in Section 1. Let the real element \( g \) generate \( A \) and let \( m(X) \) denote the minimal polynomial of \( g \). Let \( f_1(X), \ldots, f_t(X) \) denote the distinct self-adjoint monic irreducible factors of \( m(X) \) and \( h_1(X), h_1^*(X), \ldots, h_r(X), h_r^*(X) \) the distinct monic irreducible factors that are not self-adjoint. Then, according to Lemma 4.1, we can assume that \( N \) is contained in a direct product \( G_1 \times \cdots \times G_r \), where the \( G_i \) are all either orthogonal groups or all symplectic groups. Thus if \( r + t > 1 \), our induction hypothesis and Lemmas 2.1, 2.2 show that Theorem 1 must hold here.

Our reasoning above allows us to assume now that \( m(X) \) is either a power of an irreducible self-adjoint polynomial \( f(X) \) or else \( m(X) = h(X) h^*(X) \), where \( h(X) \) is a power of an irreducible polynomial that is not self-adjoint. We can rapidly dispose of the second possibility in our proof of Theorem 1. For if \( m(X) \) is such a product, Lemma 4.2 shows that \( N \) is contained in a subgroup of type \( GL^+ \) in the orthogonal case or a subgroup of type \( GL^- \) in the symplectic case. Since by Theorem 2 of [4], \( GL^+ \) has a real splitting field, our theorem must be true in the orthogonal case. Similarly, Lemma 2.5 implies that the theorem holds in the symplectic case.

For the remaining pages of the proof, we can take \( m(X) \) to be a power of an irreducible self-adjoint polynomial \( f(X) \). Our induction hypothesis and Lemma 4.3 enable us to assume that the elementary divisors of \( g \) are all equal. Let \( c \) be the multiplicity of the single type of elementary divisor of \( g \). Lemmas 4.4–4.7 applied in conjunction with the induction hypothesis and Lemmas 2.1–2.4 reduce us to examining only the cases where \( c = 1 \) or \( c = 2 \). We will describe the structure of \( N \) and the nature of its irreducible characters in the exceptional cases that arise in Lemmas 4.4–4.7.

Case Corresponding to 4.4

In this case, the minimal polynomial \( m(X) \) of \( g \) is a power of an irreducible self-adjoint polynomial \( f(X) \) of even degree, \( 2d \), say. The elementary divisors of \( g \) are all equal to \( m(X) \) and occur with multiplicity \( c \). The exceptional cases that we have to investigate occur when \( c = 1 \) or \( c = 2 \) and \( q^d \equiv 1 \pmod{4} \).
Suppose first that \( c = 1 \). The element \( g \) then acts indecomposably on the underlying space \( M \). The centralizer \( C \) of \( g \) in the full linear group is commutative and consists of polynomials in \( g \). It is well known that the semisimple elements of \( C \) form a cyclic subgroup \( D \) isomorphic to the multiplicative group of \( GF(q^{2d}) \). Now let \( t \) be any involution that inverts \( g \). If \( b \) is a generator of \( D \) we must have \( t^{-1}bt = b^\sigma \), since \( t \) induces an involution of \( D \) that arises as an automorphism of \( GF(q^{2d}) \).

Let the \( g \)-invariant form be represented by a matrix \( F \), so that we have

\[ g' F g = F. \]

It follows then that

\[ (Ft) g(Ft)^{-1} = g'. \]

Since \( g \) is indecomposable, a corollary to the theorem of Frobenius quoted in the proof of Lemma 4.2 shows that \( Ft \) is symmetric. We see that this forces \( t \) to be orthogonal when \( F \) is symmetric and skew-symplectic when \( F \) is skew-symmetric. Now, as all elements in \( C \) are polynomials in \( g \), we must have

\[ (Ft) b(Ft)^{-1} = b'. \]

From this, we obtain the relation

\[ b' F b = F b^q + 1. \]

Consequently, the semisimple subgroup of \( C_\sigma(g) \) is generated by \( e = b^q - 1 \) and has order equal to \( q^d + 1 \). It can also be checked that we have

\[ t^{-1} et = e^{-1}. \]

Let now \( V \) denote a Sylow 2-subgroup of \( C_\sigma(g) \).

We consider the orthogonal case first. The involution \( t \) is then in the orthogonal group \( G \). As our calculations above show that \( t \) inverts all elements of the cyclic group \( AV \), we see that the subgroup \( N = AU \) is dihedral. Theorem 1 clearly holds in this case. Consider now the symplectic case. Let \( w \) be an element of \( D \) that satisfies

\[ w^{q^d + 1} = -I. \]

Then \( w \) is skew-symplectic with respect to the form. Moreover, as the involution \( t \) is also skew-symplectic, the element \( wt \) is in the symplectic group \( G \). We calculate that

\[ (wt)^2 = -I. \]
Since \( wt \) inverts all elements of the cyclic group \( AV \), the group \( N = AU \) can be seen to be generalized quaternion and its central involution coincides with that of \( G \). Theorem 1 must hold here from known properties of the generalized quaternion group.

We turn to examination of the problem when \( c = 2 \) and \( q^d \equiv 1 \) (mod 4). We can take \( g \) to equal \((h, h)\), where \( h \) is an indecomposable element belonging to an orthogonal or symplectic group whose dimension is half that of \( G \). We can apply the analysis and notation of the previous paragraphs to \( h \). Again, we let \( t \) be any involution that inverts \( h \) and let \( F \) be the matrix of the \( h \)-invariant form. In this case, we can take the matrix of the \( g \)-invariant form to be

\[
E = \begin{bmatrix} F & 0 \\ 0 & F \end{bmatrix}.
\]

The work of Wall shows that a Sylow 2-subgroup \( V \) of \( C_G(g) \) is isomorphic to a Sylow 2-subgroup of \( U(2, q^{2d}) \). We can construct an explicit form of \( V \) by following Carter and Fong [1]. We first realize \( GF(q^{2d}) \) as a subgroup of matrices centralizing \( h \), as explained previously. Let \( 2^s \) be the exact power of 2 that divides \( q^d - 1 \) and let \( \varepsilon \) have order \( 2s + 1 \) in \( GF(q^{2d}) \). Put

\[
\gamma = (\varepsilon + \varepsilon^{-1})/2, \quad \delta = (\varepsilon - \varepsilon^{-1})/2.
\]

Then we have \( \gamma^2 = 1 + \delta^2 \). Since \( \gamma^2 \) lies in \( GF(q^d) \), we can write

\[
\gamma^2 = \alpha^2 + \beta^2
\]

for suitable \( \alpha, \beta \) in \( GF(q^d) \). Now put

\[
x = \begin{bmatrix} (\alpha + \delta) I & \beta I \\ \beta I & (\delta - \alpha) I \end{bmatrix}, \quad y = \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix}
\]

where \( x, y \) are matrices of the same size as \( g \), and both centralize \( g \). We find that \( x \) has order \( 2s + 1 \), \( y \) has order 4 and we have

\[
y^{-1}xy = x^{2s - 1}.
\]

Thus \( x \) and \( y \) generate a semidihedral group \( W \) of order \( 2s + 2 \). Using the relation \( b'F = Fb^q \) previously derived for semisimple \( b \) in the centralizer of \( h \), it can be checked that both \( x \) and \( y \) preserve the form defined by \( E \). A comparison of orders then shows that \( W \) is a Sylow 2-subgroup \( V \) of \( C_G(g) \). Let \( z = (t, t) \) be an involution that inverts \( g \). We calculate that we have

\[
z^{-1}xz = x^{-1}, \quad z^{-1}yz = y.
\]
We consider first the orthogonal case. Then $z$ is an orthogonal involution and $x, y, z$ generate a Sylow 2-subgroup $U$ of the extended centralizer of $g$ in $G$. Following the method outlined in Section 1, for each irreducible character $\theta$ of $V$, we compute $\eta(\theta)$ with respect to $U$. The sum of the degrees of the irreducible characters of $V$ is easily seen to be

$$2 + 2^s + 1.$$ 

The number of involutions in $U - V$ can be shown to be given by the same formula. Thus $\eta(\theta) = 1$ for all irreducible characters $\theta$ of $V$ and then $\nu(\phi) = 1$ for each irreducible character $\phi$ of $N$ that does not contain $A$ in its kernel. We see that Theorem 1 must hold in this case.

We consider now the symplectic case. Let $u$ be the element of $G$ given by $u = (wt, wt)$, where $wt$ is defined as in the symplectic case for $c = 1$. We have $u^2 = -I$ and $u$ inverts $g$. A Sylow 2-subgroup $U$ of $C^*_x(g)$ is generated by $x, y$ and $u$, and we have

$$u^{-1}xu = x^{-1}, \quad u^{-1}yu = y.$$ 

Let $\overline{U}, \overline{V}$ denote the groups $U, V$ factored by the central subgroup generated by $-I$. $V$ is a dihedral group of order $2^{s+1}$ and the sum of the degrees of its irreducible characters is $2 + 2^s$. We check that there are $2 + 2^s$ involutions in $\overline{U} - \overline{V}$. It follows that $\eta(\theta) = 1$ for any irreducible character $\theta$ of $V$ that is trivial on the central involution. Again, we have $\nu(\phi) = 1$ for all irreducible characters $\phi$ of $N$ that are trivial on the central involution and do not contain $A$ in their kernels. This proves Theorem 1 in this case for a non-faithful character of $G$.

To complete this analysis, we consider the faithful characters of $V$. We calculate that there are just two involutions in $U - V$. Thus we have

$$\sum \eta(\theta) \theta(1) = 2,$$

the sum extending over all irreducible characters $\theta$ of $V$. Now the irreducible characters of $V$ that are not faithful make a contribution $2 + 2^s$ to the sum above. Thus

$$\sum \eta(\theta) \theta(1) = -2^s,$$

the sum now extending only over faithful characters. But the sum of the degrees of the irreducible faithful characters is easily seen to be $2^s$. Therefore we must have $\eta(\theta) = -1$ for all faithful irreducible characters of $V$. But then $\nu(\phi) = -1$ if $\phi$ is any irreducible character of $N$ that is non-trivial on $A$ and does not contain $-I$ in its kernel. This proves Theorem 1 in this case for a faithful character of $G$. 
Case Corresponding to 4.5

In the exceptional case of Lemma 4.5, \( g \) is a unipotent element. We can decompose the underlying space \( M \) into a direct sum of two totally isotropic subspaces,

\[
M = M_1 \oplus M_2,
\]

where \( M_1, M_2 \) are isomorphic indecomposable \( g \)-modules. We choose dual bases in \( M_1, M_2 \) so that with respect to these bases \( g \) can be represented by the block diagonal matrix \((u, u^*)\), where \( u \) is an indecomposable unipotent matrix. Now we can find an invertible matrix \( S \) such that \( u'Su = S \). When \( u \) has minimal polynomial \( (X - 1)^{2k} \), in which case \( G \) is an orthogonal group, we can choose \( S \) to be skew-symmetric, and when \( u \) has minimal polynomial \( (X - 1)^{2k+1} \), in which case \( G \) is a symplectic group, we can choose \( S \) to be symmetric.

We find that matrices of the kind

\[
\begin{bmatrix}
ad & bS^{-1} \\
cS & dI
\end{bmatrix}
\]

with \( ad - bc = 1 \) in \( GF(q) \), centralize \( g \) and preserve the \( g \)-invariant form. These matrices form a subgroup \( D \) isomorphic to \( Sp(2) \) that is a Levi complement to the unipotent radical of \( C(g) \). Thus we can assume that \( V \) is contained in \( D \). In particular, we see that \( V \) is generalized quaternion. By Wonenburger's theorems, we can find an involution \( t \) that inverts \( u \) and satisfies

\[
t'St = S
\]

when \( S \) is symmetric, and

\[
t'St = -S,
\]

when \( S \) is skew-symmetric. We can now take \( U \) to be generated by \( V \) and the involution \( w = (t, t^*) \).

When \( S \) is symmetric, it can be checked that \( w \) centralizes \( V \). Thus, in the symplectic case, \( U \) is a direct product of a generalized quaternion group with a cyclic group of order 2. Thus it follows that for an irreducible character \( \eta \) of \( V \), we have \( \eta(\theta) = v(\theta) \). Theorem 1 holds in this case by the arguments used in the previous case.

When \( S \) is skew-symmetric, the calculations are slightly more complicated. Suppose that \( q \equiv 1 \mod 4 \) and let \( 2' \) be the 2-part of \( q - 1 \). Let \( \varepsilon \) be an element of order \( 2' \) in \( GF(q) \). The elements

\[
x = \begin{bmatrix} \varepsilon I & 0 \\ 0 & \varepsilon^{-1}I \end{bmatrix}, \quad y = \begin{bmatrix} 0 & S^{-1} \\ -S & 0 \end{bmatrix}
\]
generate \( V \). We find that \( x \) has order \( 2^r \), \( y \) inverts \( x \) and

\[
  w^{-1}xw = x, \quad w^{-1}yw = y^{-1}.
\]

We calculate that there are \( 2 + 2^r \) involutions in \( U - V \), and this is the sum of the degrees of the irreducible characters of \( V \). Again, we see that Theorem 1 holds here.

Now suppose that \( q \equiv 3 \pmod{4} \). Let \( 2^s \) be the 2-part of \( q + 1 \) and let \( \rho \) be an element of order \( 2^s \) in \( GF(q^2) \). Let \( i \) be an element of order 4 in \( GF(q^2) \). Set

\[
a = \frac{\rho + \rho^q}{2}, \quad b = \frac{\rho - \rho^q}{2i},
\]

Finally, let \( c, d \) be elements of \( GF(q) \) that satisfy

\[
c^2 + d^2 = -1.
\]

The elements

\[
x = \begin{bmatrix} aI & -bS^{-1} \\ bS & aI \end{bmatrix}, \quad y = \begin{bmatrix} cI & dS^{-1} \\ dS & -cI \end{bmatrix}
\]

generate \( V \). We find that \( x \) has order \( 2^s \), \( y \) inverts \( x \) and has order 4, and we have

\[
w^{-1}xw = x^{-1}, \quad w^{-1}yw = \begin{bmatrix} cI & -dS^{-1} \\ -dS & -cI \end{bmatrix}.
\]

We calculate that there are \( 2^s \) involutions in \( U - V \), whereas the sum of the degrees of the irreducible characters of \( V \) equals \( 2 + 2^s \). This is only possible if \( \eta(\theta) = 1 \) for all irreducible characters \( \theta \) of \( V \) except for two linear characters. The \( \eta \)-values for these two linear characters must be 0. Thus there are no characters \( \theta \) with \( \eta(\theta) = -1 \) and Theorem 1 is proved for this configuration.

**Case Corresponding to 4.6**

In the exceptional cases of Lemma 4.6, \( g \) is a unipotent element of an orthogonal group \( G \). Following the notation of Lemma 4.6, suppose that \( c = 1 \). Then \( V \) has order 2 and is generated by \(-I\). Since \( g \) is inverted by an orthogonal involution, we see that \( AV \) is cyclic and \( N \) is dihedral. Theorem 1 clearly holds in this case.

Suppose next that \( c = 2 \). We can take \( g \) to be the block diagonal element \((u, u)\), where \( u \) is a unipotent element in \( O(2k + 1) \). We consider the case
that the underlying space has type $+1$. Then the $g$-invariant form can be represented by a matrix
\[
\begin{bmatrix}
F & 0 \\
0 & F'
\end{bmatrix},
\]
for a suitable invertible symmetric matrix $F$. Consider the subgroup $D$ of $C(g)$ generated by all elements of the form
\[
\begin{bmatrix}
\lambda I & \mu I \\
-\mu I & \lambda I
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
0 & I \\
I & 0
\end{bmatrix},
\]
where $\lambda^2 + \mu^2 = 1$ in $GF(q)$. It can be seen that the elements of $D$ preserve the $g$-invariant form. $D$ is isomorphic to $O^+(2)$ when $q \equiv 1 \mod 4$ and to $O^-(2)$ when $q \equiv 3 \mod 4$, and it can be shown that $D$ is a Levi complement to the unipotent radical of $C(g)$. Thus $D$ contains a Sylow 2-subgroup $V$ of $C(g)$. Let $t$ be an involution that inverts $u$ and preserves the form defined by $F$. The involution $(t, t)$ inverts $g$, preserves the $g$-invariant form and commutes with $D$. It follows that $N$ is a direct product of the dihedral 2-subgroup $V$ and a dihedral group whose order is twice that of $g$. Theorem 1 is an immediate consequence when $N$ has this form.

Suppose now that the underlying space has type $-1$. Since the two types of non-degenerate symmetric form on a space of odd dimension over $GF(q)$ differ only by a scalar multiple, we can take the $g$-invariant form to be represented by the matrix
\[
\begin{bmatrix}
F & 0 \\
0 & dF
\end{bmatrix},
\]
where $d$ is a non-square in $GF(q)$, and $F$ is as before. Wall's results show that in this case $V$ has order 4 and can be taken to consist of the elements $(\pm I, \pm I)$. The argument of the previous paragraph shows that $N$ has the same structure as above and again we have proved Theorem 1 in this case.

**Case Corresponding to 4.7**

In the exceptional cases of Lemma 4.7, $g$ is a unipotent element of the symplectic group. If $c = 1$, $g$ is an element of $Sp(2k)$ which acts indecompositely on the underlying space. We must have $q \equiv 1 \mod 4$ in order that $g$ is real and, as we observed in the introduction, $g$ is then inverted by an element of order 4 whose square is $-I$. Since $V$ is generated by $-I$, $N$ is a generalized quaternion group whose order is four times the order of $g$. Theorem 1 holds in a straightforward way in this case by elementary properties of generalized quaternion groups.
Now we consider the case that $c = 2$. Suppose that $g$ is the block diagonal element $(u, u)$. The $g$-invariant alternating form can be represented by the matrix

$$\begin{bmatrix} F & 0 \\ 0 & F \end{bmatrix}$$

where $F$ is a suitable invertible skew-symmetric matrix. The subgroup $D$ considered in the previous orthogonal case centralizes $g$ and can be assumed to contain $V$ by Wall's results. By Wonenburger's theorem, there exists an involution $t$ that inverts $u$ and satisfies $t'Ft = -F$. Take elements $a, b$ in $GF(q)$ with $a^2 + b^2 = -1$. The matrix

$$\begin{bmatrix} at & bt \\ bt & -at \end{bmatrix}$$

inverts $g$, preserves the $g$-invariant form and satisfies $u^2 = -I$. $U$ is then generated by $u$ and $V$.

Suppose first that $q \equiv 1 \pmod{4}$. Let $i$ be an element of order 4 in $GF(q)$. We can take $u$ to equal $(it, -it)$. Since the element $(i, -1)$ is in $D$, we can replace $u$ by $(it, it)$, which clearly centralizes $D$. It follows that $U$ is a central product of a dihedral group $V$ and a cyclic group of order 4. Thus if $\theta$ is an irreducible character of $V$, we have $\eta(\theta) = \nu(\theta)$ if $\theta$ is trivial on the central involution, and $\eta(\theta) = -\nu(\theta)$ otherwise. Since $\nu(\theta) = 1$ for all characters $\theta$ of $V$, Theorem 1 holds in this case.

Now suppose that $q \equiv 3 \pmod{4}$. We calculate that there are no $-1$-involutions in $U - V$. Let $\bar{U}, \bar{V}$ denote the images of $U, V$ modulo the central subgroup of order 2. We calculate that there are $2^{r-1}$ involutions in $U - \bar{V}$, where $2^r$ is the 2-part of $q + 1$. Now $\bar{V}$ has order $2^r$ and the sum of the degrees of the irreducible characters of $\bar{V}$ is $2 + 2^{r-1}$. Following an argument that we used in the exceptional cases of Lemma 4.5, we must have $\eta(\theta) = 1$ for all irreducible characters $\theta$ of $\bar{V}$, except for two linear characters. For the two exceptional linear characters, the $\eta$-value is 0. Thus if $\theta$ is any irreducible character of $V$ that is trivial on the central involution, we certainly do not have $\eta(\theta) = -1$. Since the sum of the degrees of the faithful irreducible characters of $V$ is $2^{r-1}$, the fact that $U - V$ contains no involutions implies that $\eta(\theta) = -1$ for all faithful irreducible characters $\theta$ of $V$. This proves Theorem 1 in this special case.

Finally, we consider what happens when $g$ is the block diagonal element $(u, v)$, where $u, v$ are non-conjugate unipotent elements of $Sp(2k)$, each having minimal polynomial $(X - 1)^{2k}$. Wall's results show that $V$ has order 4 and can be taken to consist of the elements $(\pm I, \pm I)$. If $q \equiv 1 \pmod{4}$, $u$ and $v$ are inverted by elements $x$ and $y$ satisfying $x^2 = y^2 = -I$. Then $V$ and
(x, y) generate U, which is isomorphic to $Z_2 \times Z_4$. It is straightforward to check that $\eta(\theta) = 1$ if \( \theta \) is an irreducible character of \( V \) that is trivial on the central involution and $\eta(\theta) = -1$ otherwise.

If \( q \equiv 3 \pmod{4} \), we can take $u = v^{-1}$. We see that in this case, \( g \) is inverted by the element

$$w = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}.$$ 

It follows that \( U \) is a dihedral group of order 8. We calculate that $\eta(\theta) = 1$ for an irreducible character \( \theta \) of \( V \) that is trivial on the central involution and $\eta(\theta) = 0$ otherwise. Our previous reasoning, as described in Section 1, shows that Theorem 1 holds for this situation. This completes the analysis of all exceptional cases and we conclude that Theorem 1 holds by induction.

REFERENCES