THE EXTRASPECIAL CASE OF THE $k(GV)$ PROBLEM

DAVID GLUCK AND KAY MAGAARD

Abstract. Let $E$ be an extraspecial-type group and $V$ a faithful, absolutely irreducible $k[E]$-module, where $k$ is a finite field. Let $G$ be the normalizer in $GL(V)$ of $E$. We show that, with few exceptions, there exists a $v \in V$ such that the restriction of $V$ to $C_H(v)$ is self-dual whenever $H \leq G$ and $(|H|, |V|) = 1$.

Let $G$ be a finite group and let $V$ be a faithful irreducible finite $G$-module such that $(|G|, |V|) = 1$. The $k(GV)$ problem is to show that $k(GV)$, the number of conjugacy classes in the semidirect product $GV$, is at most $|V|$. This is a special but very difficult case of Brauer’s famous conjecture that the number of ordinary irreducible characters in an $r$-block of a finite group is at most the order of its defect group. Indeed, if $r$ is the prime divisor of $|V|$, then $GV$ has a unique $r$-block, and its defect group is $|V|$. On the other hand, an affirmative solution to the $k(GV)$ problem implies Brauer’s conjecture for $r$-solvable groups.

The naive approach of directly estimating $k(GV)$ has not led to any substantial result. Recent progress on the $k(GV)$ problem is based instead on the remarkable idea of “centralizer criteria.” These criteria assert that $k(GV) \leq |V|$ if there exists $v \in V$ such that $C_G(v)$ satisfies some condition. The first such criteria were proved by Knörr [K] who showed, for example, that $k(GV) \leq |V|$ if there exists $v \in V$ such that $C_G(v)$ is abelian. Building on work of Knörr [K], Gow [Gw], and Robinson [R1], Robinson and Thompson [RT] proved the most powerful centralizer criterion to date; $k(GV) \leq |V|$ provided that there exists $v \in V$ such that $V_{C_G(v)}$ has a faithful self-dual summand. For convenience, such vectors $v$ will be called $RT$-vectors.

Unfortunately, not all modules $V$ contain $RT$-vectors. Indeed, it is not hard to see that $V$ may contain no $RT$ vector when $|V| = 5^2, 7^2$, or $13^2$ and $G/Z(G) \cong S_4$. For these modules, it is of course easy to show that $k(GV) \leq |V|$. The point, however, is that imprimitive modules which are induced from these two-dimensional modules, also, in general, do not contain $RT$-vectors. Such imprimitive modules are probably the greatest obstacle to the complete solution of the $k(GV)$ problem.

Clifford-theoretic reductions as in [R1] Sect. 4 lead to two major cases of the $k(GV)$ problem. In the quasisimple case, $F^*(G) = QZ(G)$, where $Q$ is quasisimple and $Q$ acts absolutely irreducibly on $V$. In the extraspecial case, there is a prime $p$ such that $O_p(G)$ acts absolutely irreducibly on $V$ and every characteristic abelian subgroup of $O_p(G)$ is central. Since, in the extraspecial case, one may also assume that $V$ is a primitive module, a theorem of P. Hall [Go] 5.4.9 implies that $O_p(G) = E_0Z$, where $E_0$ is extraspecial of odd prime exponent or exponent 4 and $Z$ consists...
of scalar transformations. It follows that $G$ contains a normal, absolutely irreducible subgroup $E$ of “extraspecial type”; i.e. $E$ is extraspecial of odd prime exponent or exponent 4, or $E$ is the central product of an extraspecial 2-group with $Z_4$.

By 1999, both the quasisimple and extraspecial cases were thoroughly analyzed. A corollary of this analysis is the affirmative solution of the $k(GV)$ problem when $r$ is not 3, 5, 7, 11, 13, 19, or 31.

In the quasisimple case, most of the work was done by D. Goodwin [Gd1, Gd2] who used ideas of Liebeck [L2]. Then Riese [Ri1] and Koehler and Pahlings [KP] independently completed the analysis of the quasisimple case, both building on Goodwin’s work. Riese’s work is largely computer-free, while Koehler and Pahlings make heavy use of the computer.

In the extraspecial case, $V$ contains an $RT$-vector whenever $r$ is not 3, 5, 7, or 13. A complete list of the non-$RT$ extraspecial case modules appears in our main theorem; see the paragraph following the statement of the main theorem. This classification follows from the results of this paper, the work of Riese [Ri2], and that of Koehler and Pahlings [KP]: our work and Riese’s is largely computer-free, while Koehler and Pahlings use the computer heavily.

In our approach to the extraspecial case, we relax the coprimeness requirement by letting $G = N_{GL(V)}(E)$, the full normalizer in $GL(V)$ of the extraspecial-type $p$-group $E$ mentioned above. We seek a vector $v \in V$ such that $V_{C_H(v)}$ is self-dual for all $H \leq G$ with $|H| = |V| = 1$; then the Robinson-Thompson criterion (or even an earlier result of Robinson [R1 Theorem 1]) implies that $k(HV) \leq |V|$ for all such $H$.

Let $\phi$ be the Brauer character of $G$ afforded by $V$. We show in Lemma 1.7 below that $\phi$ essentially lifts to an ordinary irreducible character $\chi$ of $G$. Thus we need only find $v \in V$ such that $\chi_{C_H(v)}$ is real-valued; we call such vectors $v$ “real vectors”. Note that every real vector is an $RT$-vector.

Now we state our main result, which is proved at the end of Section 5.

**MAIN THEOREM.** Let $E$ be an extraspecial group of odd prime exponent, an extraspecial 2-group, or the central product of an extraspecial 2-group with a cyclic group of order 4. Suppose that $E$ acts faithfully and absolutely irreducibly on a vector space $V$ over $GF(r)$, where $r$ is an odd prime power. Let $|E/Z(E)| = p^{2n}$ for a prime $p$ and a positive integer $n$. Let $\varepsilon = +$ (respectively $\varepsilon = -$) if $E$ is an extraspecial 2-group of plus (respectively minus) type. In the remaining cases, let $\varepsilon = 0$. Let $G$ be the normalizer of $E$ in $GL(V)$; thus $E$ and $G$ are determined up to conjugacy in $GL(V)$ by $p$, $n$, $r$, and $\varepsilon$.

Then there exists a vector $v \in V$ such that $V_{C_H(v)}$ is self-dual for all $H \leq G$ such that $\langle r, |H| \rangle = 1$, except possibly in the following cases:

- (a) $n = 1$, $p = 2$, and $r \in \{5, 7, 13\}$,
- (b) $n = 1$, $p = 3$, and $r \in \{7, 13\}$,
- (c) $n = 2$, $p = 2$, $\varepsilon = -$, and $r \in \{3, 7\}$,
- (d) $n = 3$, $p = 2$, $\varepsilon = -$, and $r = 7$,
- (e) $n \geq 4$, $p = 2$, $\varepsilon = -$, and $r \in \{3, 7, 11, 19\}$.

Furthermore, in the following cases, there exists $H \leq G$ such that $\langle r, |H| \rangle = 1$ and such that $V_{C_H(v)}$ is self-dual for no vector $v \in V$:

- (f) $n = 1$, $p = 2$, $r \in \{5, 7, 13\}$, with $\varepsilon$ respectively 0, $-$, 0,
- (g) $n = 1$, $p = 3$, $r \in \{7, 13\}$,
- (h) $n = 2$, $p = 2$, $r \in \{3, 7\}$, $\varepsilon = -$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
We can assume that \( r \) is odd in the Main Theorem because the \( k(GV) \) conjecture has been proved \([\text{GH}]\) when \( r \) is even; the same result was proved independently by Knörr. We remark that of the seven bad cases in (f), (g), and (h) above, \( H \) is solvable in six, and in six \( G \) has order prime to \(|V|\). We also remark that in each of the seven bad cases, \( V \) contains no \( RT \)-vector. For \( r \) odd, the work of Riese \([\text{Ri2}]\) shows that every extraspecial case module with \( r \) odd contains an \( RT \)-vector or falls under (f), (g), or (h) above. When \( r \) is even, \( RT \)-vectors always exist; see \([\text{RS}]\).

Now we give an indication of the proof of the Main Theorem. As above, we let \( G = N_{GL(V)}(E) \), and we seek a “real vector”, i.e., a vector \( v \in V \) such that \( \chi_{C_G(v)} \) is real-valued. We focus in this introduction on one of the four possibilities for \( E \) and assume that \( E \) is the central product of an extraspecial group of order \( 2^{2n+1} \) with \( Z_4 \). Thus \(|V| = r^{2n} \). We have \( F(G) = EZ(G) \). Let \( G = G/F(G) \cong Sp(2n, 2) \). Thus \( E/Z(E) \) is the natural module for \( G \).

\( \overline{G} \) contains a subgroup \( \overline{L} \cong GL(n, 2) \) such that \( (E/Z(E))_{\overline{G}} = \overline{A} \oplus \overline{A}^* \), where \( \overline{A} \) and \( \overline{A}^* \) are \( \overline{G} \)-invariant maximal totally isotropic subspaces of the symplectic space \( E/Z(E) \). We have \(|N_{\overline{G}}(\overline{L}) : \overline{L}| = 2 \) and \( N_{\overline{G}}(\overline{L}) \) induces the inverse transpose automorphism of \( L \).

Thanks to some results on cohomology, we can lift \( \overline{G} \) to a subgroup \( L \cong \overline{L} \) of \( G \), and we can lift \( \overline{A} \) and \( \overline{A}^* \) to subgroups \( A \) and \( A^* \) of \( E \), with \(|A| = |\overline{A}| = |\overline{A}^*| = |A^*| \), such that \( L \) normalizes \( A \) and \( A^* \). Now \( \text{dim} \, C_V(A) = \text{dim} \, C_V(A^*) = 1 \). Let \( W = (C_V(A), C_V(A^*)) \). Then \( \text{dim} \, W = 2 \), \( L \) centralizes \( W \), and \( N_G(L) \) acts on \( W \).

Let \( v \in W - C_V(A) - C_V(A^*) \). We show that \( C_G(v) \leq N_G(L) \) “generically”, i.e., if \( n \geq 5 \). Indeed, if this were not the case, then the image \( \overline{C}_G(v) \) of \( C_G(v) \) in \( \overline{G} \) would be an overgroup of \( \overline{L} \) which acts irreducibly on \( E/Z(E) \) with at most two orbits on the nonzero vectors of \( E/Z(E) \). Using Liebeck’s classification of the primitive rank three affine groups, we see that there are very few possibilities for \( \overline{C}_G(v) \), and none give rise to possible vector centralizers; “sporadic” possibilities for \( \overline{C}_G(v) \) arise when \( n = 3 \) or 4, but those are easy to eliminate.

Hence, provided that \( n \geq 3 \), we have \( C_G(v) \leq N_G(L) \) for all \( v \in W - C_V(A) - C_V(A^*) \). The next step is to show that \( C_G(v) \leq L \) for some such \( v \). Now \( N_G(L) \) acts on \( W \) as an abelian group \( \langle t, Z(G) \rangle \), where \( t \in N_G(L) \) induces the inverse transpose automorphism of \( L \) and \( t \) interchanges \( C_V(A) \) and \( C_V(A^*) \). It is easy to find \( v \in W - C_V(A) - C_V(A^*) \) such that \( v \) lies in a regular \( N_G(L)/L \)-orbit. Hence \( C_G(v) \leq L \).

Thus \( \chi_{C_G(v)} = \chi_L \). If \( g \in L \), then \( g \) and \( g^{-1} \) are conjugate in \( N_G(L) \), since \( t \) induces the inverse transpose automorphism of \( L \cong GL(n, 2) \). Thus \( \chi(g) = \chi(g^{-1}) \) and so \( \chi_{C_G(v)} \) is real-valued. Hence, by definition, \( v \) is a real vector, as desired.

The argument sketched above must be considerably modified when \( E \) is one of the other three extraspecial-type \( p \)-groups and when \( n \) is small. For example, when \( E \) is extraspecial of odd prime exponent, it is no longer clear that \( C_G(v) \) has at most two orbits on the nonzero vectors of \( E/Z(E) \). Hence we can’t use \([\text{LI}]\) and must rely instead on long arguments involving facts about representations of groups of Lie type and the list of maximal subgroups of \( PSp(4, p) \). In addition, the action on \( N_G(L) \) on \( W \) is more complicated than in the case discussed above.
In several cases, $G$ contains no $GL(n,p)$ subgroup $L$, and so we are forced to use ad hoc methods. This occurs when $E$ is an extraspecial 2-group of minus type, when $n = 1$ and $p$ is arbitrary, and when $n = p = 2$.

In Section 6, we discuss solvable groups and show that real vectors exist when $r > 13$. After the original version of this paper, the results of Section 6 were improved by Riese and Schmid [RS]. Since they quote from our paper, we are retaining the original Section 6 in the final version of this paper.

1. Preliminaries

Let $F$ be the field $GF(r)$, with $r$ odd, and let $p$ be a prime divisor of $r - 1$. Let $V$ be an $F$-vector space of dimension $p^n$, for some $n \geq 1$. We will be concerned with subgroups $H$ of $GL(V)$ that contain a normal extraspecial-type subgroup which acts absolutely irreducibly on $V$. When $(|H|, |V|) = 1$, we want to find vectors $v \in V$ such that $V_{CH}(v)$ is self-dual. We are led to consider the full normalizers in $GL(V)$ of certain $p$-subgroups $E \leq GL(V)$, in the following four cases:

I. $E$ is extraspecial of order $p^{2n+1}$ and exponent $p$, and $p$ is odd.
II. $E = E_0 \ast Z_4$, with $E_0$ extraspecial of order $2^{2n+1}$, and $r \equiv 1 \pmod{4}$.
III. $E$ is extraspecial of order $2^{2n+1}$ and of plus type, and $r \equiv 3 \pmod{4}$.
IV. $E$ is extraspecial of order $2^{2n+1}$ and of minus type, and $r \equiv 3 \pmod{4}$.

In each of the four cases, $E$ is determined up to conjugacy in $GL(V)$ by $n, p, r$, and a sign $\varepsilon$ to distinguish between Cases III and IV. For convenience, let $\varepsilon = 0$ in Cases I and II. We define $G = G^{\pm}(n, p, r)$ to be the normalizer in $GL(V)$ of $E$.

Now $C(E) := C_{Out(E)}Z(E)$ is $Sp(2n, p)$, $Sp(2n, 2)$, $O^+(2n, 2)$, and $O^-(2n, 2)$ in Cases I, II, III, IV, respectively. Our first goal is to determine the structure of $G$. We will show in Proposition 1.5 that $G = KZ$, where $Z = Z(GL(V))$ and $K$ is an extension of $C(E)$ by $E$.

Let $\phi$ be the Brauer character of $G$ afforded by $V$. If $v \in V, H \leq G$, and $(|H|, |V|) = 1$, then $V_{CH}(v)$ is self-dual if and only if $\phi_{CH}(v)$ is real-valued. Let $\theta \in Irr(E)$ be the restriction of $\phi$ to $E$. We will show in this section that $\theta$ extends to ordinary irreducible characters $\psi$ and $\chi$ of $K$ and $G$, respectively. We will work for the most part with $\chi$ or $\psi$, rather than with $\phi$ directly. In Definition 1.8, we define “real vectors”; these vectors are crucial in our approach to the $k(GV)$ problem. Lemma 1.11 shows that we can often use the subgroup $K$ of $G$ and the character $\psi$ of $K$ to demonstrate the existence of real vectors.

We begin with a result of Griess [Gr1], which provides much of the preliminary information we need in Cases II, III, and IV.

Lemma 1.1. (a) Suppose we are in Case III or IV. There exists a group $H$ such that $O_2(H) \cong E, H/O_2(H) \cong O^+(2n, 2), H/Z(H) \cong Aut(E)$, and $Z(H) = Z(E)$. Furthermore $H$ has a faithful irreducible complex character of degree $2^n$.

(b) Suppose we are in Case II. Then there exists a group $H$ such that $O_2(H) \cong E, Z(H) = Z(E), H/O_2(H) \cong Sp(2n, 2)$, and $H/Z(H)$ is isomorphic to the centralizer in $Aut(E)$ of $Z(E)$. Moreover, $H$ has two faithful irreducible complex characters of degree $2^n$, which are interchanged by the action of $Aut(E)$ and by complex conjugation.

Proof. This is [Gr1, Theorem 5].
Lemma 1.2. Suppose we are in Case I. Let $\theta \in \text{Irr}(E)$ be as above. There exists a split extension $H$ of $C(E) \cong \text{Sp}(2n, p)$ by $E$. Let $S \cong \text{Sp}(2n, p)$ be a fixed complement to $E$ in $H$. Then there exists $\Psi \in \text{Irr}(H)$ which extends $\theta$, and $\Psi_S$ is the sum of two irreducible characters $\psi_1$ and $\psi_2$, of degrees $(p^n - 1)/2$ and $(p^n + 1)/2$ respectively. We have $Q(\Psi) = Q(\theta) = Q_p$, the cyclotomic field of $p$th roots of unity, and $Q(\psi_1) = Q(\psi_2) = Q(\sqrt{p})$, where $\delta = (-1)^{(p-1)/2}$. If $(n, p) \neq (1, 3)$, then all complements to $E$ in $H$ are conjugate to $S$. Finally, the reductions of $\psi_1$ and $\psi_2$ in any odd characteristic different from $p$ remain irreducible.

Proof. The final statement follows from the remarks preceding [GMS] Theorem A. For the field of values of $\psi_1$ and $\psi_2$, see [III] p. 621. If $(n, p) \neq (1, 3)$, then $H = H'$. Thus $\theta$ has a unique extension to $H$ and so $Q(\Psi) = Q(\theta)$. If $(n, p) = (1, 3)$, then $Q(\Psi) = Q(\theta) = Q(\sqrt{3})$, since $\text{SL}(2, 3) \times Z_3$ has character values in $Q(\sqrt{3})$. Since $S = \{C_H(Z(S))\}^+$ when $(n, p) \neq (1, 3)$, and since all complements to $E$ in $Z(S)E$ are conjugate in $Z(S)E$, the statement about conjugacy of complements follows.

Lemma 1.3. Let $G$ be a finite group of the form $\langle x, E \rangle$, where $E$ is a normal extraspecial subgroup of $G$. Let $\chi \in \text{Irr}(G)$ with $Z(E) \nsubseteq \text{Ker} \chi$. Then $\chi(x) = 0$ or $|\chi(x)|^2 = |C_{E/Z(E)}(x)|$. Moreover, if $H$ and $\Psi$ are as in Lemma 1.2, and $x \in S$, then $|\Psi(x)|^2 = |C_{E/Z(E)}(x)|$.

Proof. All of this is well known. For the first statement, see [G12] Lemma 1.6. For the second statement, see [III] 3.5, 3.7, and 7.1.

The next result provides the detailed information we need when $n = 1$. The proof depends ultimately on Dickson's classification of the subgroups of $\text{PSL}(2, q)$.

Proposition 1.4. Let $n = 1$. There exists a subgroup $K = K^\circ(1, p, r)$ of $\text{NGL}(V)(E)$ such that $K/E \cong C_{\text{Out}(E)}(Z(E)) = C(E)$. In Case I, we can take $K$ to split over $E$. In Case II, where $K/E \cong S_3$, we can take $K$ to split over $E$ when $r \equiv 1 \pmod{8}$. In Case III, we can take $K$ to split over $E$ when $r \equiv 7 \pmod{8}$; when $r \equiv 3 \pmod{8}$, $\text{GL}(V)$ contains no split extension of $O^+(2, 2) \cong Z_2$ by $E \cong D_8$. In Case IV, we can take $K$ to split over $E$ when $r \equiv 3 \pmod{8}$; when $r \equiv 7 \pmod{8}$, $\text{GL}(V)$ contains no split extension of $O^-(2, 2) \cong S_3$ by $E \cong Q_8$.

Proof. First suppose we are in Case I. Let $H = SE$ be the split extension as in Lemma 1.2, with $S \cong \text{SL}(2, p)$. Let $\overline{F}$ be the algebraic closure of $F = GF(r)$. Lemma 1.2 implies that $H$ has a faithful irreducible representation of degree $p$ over $\overline{F}$, whose $\overline{F}$-character lies in $F_0(\omega_p)$, where $F_0$ is the prime field of $F$ and $\omega_p$ is a primitive $p$th root of 1 in $F$. Since $p$ divides $r - 1$, we have $\omega_p \in F$. Since Schur indices are trivial in positive characteristic, it follows that $\text{GL}(p, F) \cong \text{GL}(V)$ contains a subgroup isomorphic to $H$.

Next suppose we are in Case II and $r \equiv 1 \pmod{8}$. By [Hu] I.8.27, $\text{PSL}(2, r)$ contains a subgroup isomorphic to $S_3$. Since $\text{SL}(2, r)$ contains a unique involution, it follows that $\text{SL}(2, r)$ contains an extension $J$ of $S_3$ by $Q_8$. By the Frattini argument, $J = J^N = O_2(J)N$, where $N$ is a 3-Sylow normalizer of $J$. Thus $|N| = 12$ and $N \cap O_2(J) = O_2(Z(J))$. If $N$ splits over $Z(O_2(J))$, then $J$ is a split extension of $S_3$ by $Q_8$. If $N$ doesn’t split over $Z(O_2(J))$, then multiplying an element of order 4 in $N$ by an element of order 4 in $Z(GL(V))$ produces a split extension of $S_3$ by $Q_8$. Hence $\text{GL}(V)$ contains a split extension of $S_3$ by $E = Q_8 * Z_4$.
Now suppose we are in Case II and \( r \equiv 5(\text{mod} \, 8) \). By [Hu, I.8.27], \( PSL(2, r) \) contains a subgroup isomorphic to \( A_4 \). It follows that \( SL(2, r) \) contains a subgroup \( S \) such that \(|S| = 24, O_2(S) \cong Q_8, \) and \( S/Z(S) \cong A_4 \). We take \( E = O_2(S) * Z_4 \), where \( Z_4 \) denotes the unique subgroup of order 4 in \( Z(GL(V)) \). Now \( E \) has index 2 in a 2-Sylow subgroup \( T \) of \( GL(2, r) \). Hence \( \langle T, S \rangle \leq N(E) \cap G_4 \), where \( G_4 \) denotes the group of elements of \( GL(2, r) \) whose determinantal order divides 4. Since \( E \) is absolutely irreducible on \( V \), the centralizer in \( G_4 \) of \( E \) is \( Z(GL(V)) \cap G_4 = Z_4 \leq E \). Hence \( \langle T, S \rangle/Z_4 \) is isomorphic to a subgroup of \( Aut(E) \). But \( Aut(E) \) is a 2,3-group and \(|Aut(E)| = 3\). It follows that \(|\langle T, S \rangle| \) divides \( 3 \cdot |GL(2, r)|_2 = 96 \). On the other hand \( |T| = 32 \) and 3 divides \(|S| \), so \(|\langle T, S \rangle| = 96 \). Since \( \langle T, S \rangle \) normalizes \( E \) and centralizes \( Z(E) \), we have \( \langle T, S \rangle/E \cong C(E) \cong Sp(2, 2) \cong S_3 \). Hence we take \( K \) to be \( \langle T, S \rangle \).

Now we turn to Case III, in which \( E \cong D_8 \). If \( r \equiv 7(\text{mod} \, 8) \), then \( GL(2, r) \) contains a semilinear group of order \( 2(r^2 - 1) \). The norm 1 elements of \( GF(r^2) \) give rise to a dihedral subgroup of order \( 2(r + 1) \), which in turn contains a dihedral subgroup \( D \) of order 16. One checks that \( D \) splits over a normal \( D_8 \) subgroup, as desired.

On the other hand, if \( r \equiv 3(\text{mod} \, 8) \), then \(|GL(2, r)|_2 = 16 \). By [Hu, I.8.27], \( PSL(2, r) \) contains an \( A_4 \) subgroup. Hence \( SL(2, r) \) contains a \( Q_8 \) subgroup \( Q \). Let \( T \) be a 2-Sylow subgroup of \( GL(2, r) \) containing \( Q \). By absolute irreducibility of \( Q \) on \( V = GF(r^2) \), we have \( C_T(Q) = Z(Q) \). Hence \( T/Z(Q) \) is isomorphic to a \( D_8 \) subgroup of \( Aut(Q_8) \cong S_4 \), and so \( T \) has nilpotence class 3. By [G, 5.4.5], \( T \) is dihedral, semidihedral, or generalized quaternion. Now \( D_{16} \) contains no \( Q_8 \) subgroup and \( Q_{16} \) contains no noncentral involutions. Since \( T \geq Q \) and since \( GL(2, r) \) contains a noncentral involution, \( T \) must be semidihedral. Hence \( T \) has a normal \( D_8 \) subgroup \( D \). Hence we can take \( K = T \); up to conjugacy in \( GL(V) \), there are no other possibilities for \( K \). If \( \alpha \) is an involutory outer automorphism of \( D \) then the semidirect product \( \langle \alpha \rangle \cdot D \) has class 3 and contains more than five involutions. Thus \( \langle \alpha \rangle \cdot D \cong D_{16} \). It follows that \( T \) does not split over \( D \), and so \( K \) does not split over \( E \).

Finally, suppose we are in Case IV. If \( r \equiv 7(\text{mod} \, 8) \), then, by [Hu, I.8.27], \( PSL(2, r) \) contains an \( S_4 \) subgroup. It follows that \( SL(2, r) \) contains an extension of \( S_3 \) by \( Q_8 \), which we take to be \( K \).

If \( r \equiv 3(\text{mod} \, 8) \), we claim that \( GL(2, r) \) contains a subgroup isomorphic to \( GL(2, 3) \). To prove this, we may assume \( r \) is a prime, since the prime divisor of \( r \) is also congruent to 3 modulo 8. Now \( GL(2, 3) \) has a faithful irreducible complex character \( \chi \) such that \( \chi(1) = 2 \) and \( Q(\chi) = Q(\sqrt{-2}) \). Reduction modulo a prime divisor of \( r \) in a suitable ring of local algebraic integers leads to a faithful irreducible representation of \( GL(2, 3) \) over \( GF(r) \), whose \( GF(r) \) character \( \chi \) satisfies \( \chi(1) = 2 \) and \( (GF(r))(\chi) = (GF(r))(\sqrt{-2}) \). Since \( r \equiv 3(\text{mod} \, 8) \), \( GF(r) \) contains \( \sqrt{-2} \).

Hence \( GL(2, 3) \) has a faithful 2-dimensional representation over \( GF(r) \), and so \( GL(2, r) \) contains \( GL(2, 3) \), a split extension \( K \) of \( S_3 \) by \( Q_8 \).

Conversely, suppose that \( r \equiv 7(\text{mod} \, 8) \) and \( GL(2, r) \) contains a split extension of \( S_3 \) by \( Q_8 \). Since \( Aut(Q_8) \cong S_4 \) contains a unique conjugacy class of \( S_3 \) subgroups, every such split extension is isomorphic to \( GL(2, 3) \). Let \( \chi \) be the Brauer character of \( GL(2, 3) \) afforded by the inclusion of \( GL(2, 3) \) into \( GL(2, r) \). From the character table of \( GL(2, 3) \), we see that \( \chi(x) = \sqrt{-2} \) for an element \( x \in GL(2, 3) \) of order 8. It
follows that the eigenvalues of \( x \in GL(2, r) \) are \( \alpha \) and \( \alpha^3 \), for an element \( \alpha \in GF(r) \) of multiplicative order 8. But then \( (\alpha + \alpha^3)^2 = -2 \). Since \( r \equiv 7 \pmod{8} \), \( \sqrt{-2} \notin GF(r) \). Hence \( GL(2, r) \) contains no split extension of \( S_3 \) by \( Q_8 \).

**Proposition 1.5.** With notation as in the remarks preceding Lemma 1.1, \( GL(V) \) contains an extension \( K \cong K^e(n, p, r) \) of \( C(E) \) by \( E \). Furthermore, there exists \( \psi \in \text{Irr}(K) \) such that \( \psi_E = \theta \). In Case I, we have \( Q(\psi) = Q(\theta) = Q_p \). In case II, \( Q(\psi) \) contains \( Q(\theta) = Q(i) \). In Cases III and IV, we have \( Q(\psi) = Q(\sqrt{-2}) \) if \( r \equiv 7 \pmod{8} \), and \( Q(\psi) = Q(\sqrt{-2}) \) if \( r \equiv 3 \pmod{8} \).

**Proof.** First suppose \( n = 1 \). The existence of \( K \) was proved in Proposition 1.4. If we are in Case I, the existence of \( \psi \) and the fact that \( Q(\psi) = Q_p \) follow from Lemma 1.2. If we are in Case II, then \( \theta \) has three extensions to \( K_0 = GL(2, 3) \times Z_4 \), one of which must be invariant in \( K \) and thus (since \( K/K_0 \) is cyclic) extends to \( K \). Hence \( \theta \) extends to an irreducible character of \( K \). Of course \( Q(\psi) \supseteq Q(\theta) = Q(i) \).

If we are in Case III and \( r \equiv 7 \pmod{8} \), then, by Proposition 1.4, \( K \) splits over \( E \cong D_8 \). As in the proof of Proposition 1.4, \( K \cong D_{16} \). Hence \( \theta \) extends to \( \psi \in \text{Irr}(K) \) and \( Q(\psi) = Q(\sqrt{2}) \). If we are in Case III with \( r \equiv 3 \pmod{8} \), then, by Proposition 1.4, \( K \) does not split over \( E \cong D_8 \). Then, as in the proof of Proposition 1.4, \( K \) is semidihedral and \( \theta \) extends to \( \psi \in \text{Irr}(K) \) with \( Q(\psi) = Q(\sqrt{-2}) \). If we are in Case IV and \( r \equiv 3 \pmod{8} \), then, as in the proof of Proposition 1.4, \( K \cong GL(2, 3) \) and \( \theta \) extends to \( \psi \in \text{Irr}(K) \) with \( Q(\psi) = Q(\sqrt{-2}) \). If we are in Case IV with \( r \equiv 7 \pmod{8} \), then \( K \) does not split over \( E \) by Proposition 1.4. The argument in the final paragraph of the proof of Proposition 1.4 shows that \( K \) does not have semidihedral 2-Sylow subgroups. It follows from [Go] 5.4.5 that \( K \) has generalized quaternion 2-Sylow subgroups. Now \( \theta \) has three extensions to \( K' \cong SL(2, 3) \), one of which must be rational valued and extendible to \( K \). Let \( \psi \in \text{Irr}(K) \) extend \( \theta \). Then \( Q(\psi) : Q \leq 2 \). Restriction to a 2-Sylow subgroup of \( K \) shows that \( \sqrt{2} \in Q(\psi) \). Hence \( Q(\psi) = Q(\sqrt{2}) \), as desired.

We assume from now on that \( n \geq 2 \). If we are in Case I, then the existence of \( \psi \) and the fact that \( Q(\psi) = Q_p \) follow from Lemma 1.2.

Suppose next that \( n = 2 \) and we are in Case II. By Lemma 1.1, there is a group \( H \) with \( O_2(H) \equiv E, Z(H) = Z(E), \) and \( H/O_2(H) \equiv Sp(4, 2) \equiv S_6 \). Furthermore, Lemma 1.1 implies that \( H' \) has a faithful irreducible character \( \alpha \) of degree 4, whose restriction \( \theta \) to \( O_2(H) \equiv E \) is also faithful and irreducible. Since \( H'/E \equiv A_6 \) has no nontrivial linear characters, \( \alpha \) is the unique irreducible character of \( H' \) lying over \( \theta \). Hence \( Q(\alpha) = Q(\theta) = Q(i) \). Since \( GF(r) \) contains \( \sqrt{-1} \), it follows that \( H' \) is isomorphic to a subgroup of \( GL(4, r) \); we identify \( E \) with \( O_2(H) = O_2(H') \). Since \( H' = H'' \), we have \( H' \leq SL(4, r) \).

The restriction to \( E \) of \( V := GF(r)^4 \) is tensor decomposable. We have \( V = V_1 \otimes V_2 \) and \( E = E_1 \ast E_2 \), where \( E_1 \cong D_8 \times Z_4 \), \( E_2 \cong D_8 \), \( E_1 \leq GL(V_1) \otimes id. \) and \( E_2 \leq id. \otimes GL(V_2) \). By Case II of Proposition 1.4, there exists an overgroup \( K_1 \) of \( E_1 \) in \( GL(V_1) \otimes id. \), with \( |K_1 : E_1| = 2 \) and \( K_1 \leq K(1, 2, r) \). Write \( K_1 = E_1(t) \), where \( t^2 \in E_1 \). Let \( K = \langle K_1, H' \rangle \). Now \( t \) normalizes \( E \) and induces a transvection on \( E/Z(E) \). In particular, \( t \notin H' \). Since \( \langle t \rangle \) induces \( Sp(4, 2)' \cong A_6 \cong H'/E \) on \( E/Z(E) \), we have \( \langle t \rangle \leq H' \leq H' / Z(GL(4, r)) \). Since \( t \) normalizes \( H'/Z(GL(4, r)) \), \( t \) normalizes its derived group, \( H'' = H' \). Let \( K = \langle t \rangle H' \). Then \( |K : H'\rangle = 2 \) and \( K/E \cong Sp(4, 2) \), so \( K \) can serve as \( K(2, 2, r) \). Since \( \alpha \in \text{Irr}(H') \) is the unique
extension of \( \theta \in \text{Irr}(E) \), \( \alpha \) is invariant in \( K \). Since \( K/H' \) is cyclic, \( \alpha \) extends to \( \psi \in \text{Irr}(K) \). Of course \( Q(\psi) \supseteq Q(\theta) = Q(i) \).

Now suppose we are in Case II and \( n \geq 3 \). Lemma 1.1 shows that there exists an overgroup \( H \) of \( E \) with \( H/E \cong \text{Sp}(2n,2) \). Since \( (H/E)' = H/E \), any faithful \( \theta \in \text{Irr}(E) \) has a unique extension to \( H \), whose field of values must be \( Q(\theta) = Q(i) \).

Since \( GF(r) \) contains \( \sqrt{-1} \), we view \( E \leq H \leq \text{GL}(V) \), and there exists \( \psi \in \text{Irr}(H) \) with \( \psi_E = \theta \) and \( Q(\psi) = Q(\theta) = Q(i) \).

Next suppose \( n = 2 \) and we are in Case III. We may write \( V = V_1 \otimes V_2 \) and \( E = E_1 + E_2 \), where \( E_1 \cong E_2 \cong Q_8 \), \( E_1 \leq \text{GL}(V_1) \otimes \text{id} \), and \( E_2 \leq \text{id} \otimes \text{GL}(V_2) \). Let \( t \in \text{GL}(V_1 \otimes V_2) \) be the involution that sends \( v_1 \otimes v_2 \) to \( v_2 \otimes v_1 \) for all \( v_1 \in V_1, v_2 \in V_2 \). Since \( \text{GL}(V_1 \otimes V_2) \) contains \( \text{GL}(V_1) \otimes \text{id} \), \( K_1 \leq \text{GL}(V_1) \otimes \text{id} \), \( K_2 \leq \text{id} \otimes \text{GL}(V_2) \), and \( K_1 = K_2 \). Then \( \langle t \rangle (K_1 \ast K_2) / E \cong O^+(4,2) \), and so \( \langle t \rangle (K_1 \ast K_2) \) can serve as \( K^+(2,2,r) \).

Let \( \theta_1 \) and \( \theta_2 \) be the unique faithful irreducible characters of \( E_1 \) and \( E_2 \), respectively. Let \( \psi_2 = \psi_1 \otimes \psi_2 \) extends \( \theta_2 \), and \( Q(\psi_1) = Q(\psi_2) = Q(\sqrt{-2}) \) if \( r \equiv 3(\text{mod } 8) \), while \( Q(\psi_1) = Q(\psi_2) = Q(\sqrt{2}) \) if \( r \equiv 7(\text{mod } 8) \). By [Is2 Theorem 5.2], \( \psi_1 \times \psi_2 \), viewed as an irreducible character of \( K_1 \ast K_2 \), extends to a tensor induced irreducible character \( \psi \) of \( K = \langle t \rangle (K_1 \ast K_2) \); indeed we have \( \psi = (\psi_1 \times 1)^{\otimes \langle t \rangle (K_1 \ast K_2)} \), viewed as an irreducible character of \( K \). By the formula for tensor induced characters, \( Q(\psi) = Q(\psi_1) = Q(\psi_2) = Q(\sqrt{2}) \), as desired.

Finally suppose we are in Case III with \( n \geq 3 \) or in Case IV with \( n \geq 2 \). Let \( H \) be as in Lemma 1.1(a). Then \( H' \) has a faithful irreducible character \( \alpha \) which extends the unique faithful irreducible character \( \theta \) of \( E \). Since \( (H'/E)' = H'/E \), it follows that \( \alpha \) is rational-valued. Thus we may assume that \( E \leq H' \leq \text{GL}(V) \). Write \( V = V_1 \otimes V_2 \) with \( \dim V_1 = 2, \dim V_2 = 2^{n-1} \). Write \( E = E_1 + E_2 \), where \( E_1 \cong D_8, E_2 \) is extraspecial of order \( 2^{2n-1} \), \( E_1 \leq \text{GL}(V_1) \otimes \text{id}, \) and \( E_2 \leq \text{id} \otimes \text{GL}(V_2) \).

Let \( E_1 \leq K_1 \leq \text{GL}(V_1) \otimes \text{id} \), with \( K_1 \cong K^+(1,2,r) \). Let \( K_1 = \langle t \rangle E_1 \) with \( t^2 \in E_1 \). As in the \( S p(4,2) \) case, \( t \) normalizes \( H' = H'' \) and \( K := \langle t \rangle H' \) serves as \( K^+(n,p,r) \). Moreover \( K \) contains the subgroup \( \langle t \rangle E = \langle t \rangle E_1 + E_2 \). Since \( \langle t \rangle E : E \rangle = 2, \theta \) extends to \( \langle t \rangle E \). If \( \psi_1 \in \text{Irr} \langle t \rangle E_1 = \text{Irr}(K^+(1,2,r)) \) is as in the statement of this proposition, then \( \psi_1 \) has the same field of values as either of the two extensions of \( \theta \) to \( \langle t \rangle E \). By the \( n = 1 \) case of this proposition, this field of values is \( Q(\sqrt{2}) \) if \( r \equiv 7(\text{mod } 8) \) and \( Q(\sqrt{-2}) \) if \( r \equiv 3(\text{mod } 8) \).

Since \( (H'/E)' = H'/E \), \( \alpha \) is the unique extension of \( \theta \) to \( H' \). Hence \( \alpha \) is invariant in \( K \). Since \( K/H' \) is cyclic, \( \alpha \) extends to \( \psi \in \text{Irr}(K) \). Now \( [Q(\psi) : Q] = [Q(\psi) : Q(\alpha)] \leq [K : H'] = 2 \). Since \( K \) contains \( \langle t \rangle E \), we have \( Q(\psi) \supseteq Q(\psi_1) \).

Since \( [Q(\psi_1) : Q] = 2 \), we have \( Q(\psi) = Q(\psi_1) \). Hence \( Q(\psi) = Q(\sqrt{2}) \) if \( r \equiv 7(\text{mod } 8) \) and \( Q(\psi) = Q(\sqrt{-2}) \) if \( r \equiv 3(\text{mod } 8) \), as desired.

Corollary 1.6. With notation as above, suppose that \( n \geq 3 \) and we are in Case III, or that \( n \geq 2 \) and we are in Case IV. Then the restriction of \( \psi \) to \( K' \) is rational-valued.

Proof. Under these hypotheses, \( K'/E \cong \Omega^+(2n,2) \) is a perfect group. Thus \( \psi_{K'} \) is the unique extension of \( \theta \) to \( K' \). Since \( \theta \) is rational-valued, so is \( \psi_{K'} \).

Lemma 1.7. Let \( G = N_{\text{GL}(V)}(E) \) as at the beginning of this section. Let \( Z = Z(\text{GL}(V)) \). Let \( K \) be as in Proposition 1.5, so that \( G = KZ \). Let \( \theta = \phi_E \) as at the beginning of this section, and let \( \psi \in \text{Irr}(K) \) extend \( \theta \) as in Proposition 1.5. Then there exists a unique \( \chi \in \text{Irr}(G) \) such that \( \chi_K = \psi \) and such that \( \chi_E = \phi_E \). For
such \( \chi \), we have \( \chi(x) = \pm \phi(x) \) for all \( x \in G \) of order prime to \( r \), except possibly when \( n = 1 \) and \( p = 3 \).

**Proof.** Let \( \hat{\theta} = \phi_{\mathbb{E}Z} \). Then \( \hat{\theta} \) is an ordinary irreducible character of \( \mathbb{E}Z \) which extends \( \theta \). Let \( \lambda \) be the unique and linear irreducible constituent of \( \hat{\theta}_{\mathbb{Z}} \). Now \( G \) is the central product of \( K \) and \( Z \), with \( K \cap Z = \mathbb{Z}(E) \). Since \( \psi_{\mathbb{Z}(E)} = \theta_{\mathbb{Z}(E)} \) is a multiple of \( \lambda_{\mathbb{Z}(E)} \), there exists a unique \( \chi \in \text{Irr}(G) \) such that \( \chi_{K} = \psi \) and \( \chi_{Z} \) is a multiple of \( \lambda \). Indeed \( \chi(xz) = \psi(x)\lambda(z) \) for all \( x \in K \) and all \( z \in Z \). In particular, when \( x \in E \) and \( z \in Z \), we have \( \chi(xz) = \theta(x)\lambda(z) = \hat{\theta}(xz) \), so \( \chi_{\mathbb{E}Z} = \phi_{\mathbb{E}Z} \).

Now let \( \overline{\psi} = \overline{G}(r) \otimes V \). Let \( \rho : G \to GL(\overline{\psi}) \) be the natural inclusion and let \( \sigma : G \to GL(\overline{\psi}) \) be a representation whose Brauer character is the restriction of \( \chi \) to the \( r' \)-elements of \( G \). Since \( \chi_{\mathbb{E}Z} = \phi_{\mathbb{E}Z} \), we may, after replacing \( \sigma \) by an equivalent representation, assume that \( \rho(x) = \sigma(x) \) for all \( x \in \mathbb{E}Z \). Let \( \tau(x) = \rho(x) = \sigma(x) \) for \( x \in \mathbb{E}Z \). If \( g \in G \) and \( x \in \mathbb{E}Z \), then \( \rho(g^{-1}xg) = \sigma(g^{-1}xg) \), and so \( \rho(g)^{-1}\tau(x)\rho(g) = \sigma(g)^{-1}\tau(x)\sigma(g) \). Hence \( \sigma(g)\rho(g)^{-1} \) commutes with \( \tau(x) \) for all \( x \in \mathbb{E}Z \). Thus \( \rho(g) = \mu(g)\sigma(g) \) for a scalar \( \mu(g) \). Clearly \( \mu : G \to \overline{G}(r) \) is a homomorphism. Now \( \mathbb{E}Z \leq \text{Ker} \mu \) and \( G/\mathbb{E}Z \cong C(E) \). If \( (n,p) \neq (1,3) \), then \( C(E)/C(E)' \) is an elementary abelian 2-group. It follows that \( \mu(g) = \pm 1 \) for all \( g \in G \) and so \( \chi(g) = \pm \phi(g) \) for all \( g \in G \) of order prime to \( r \). □

**Definition 1.8.** With notation as above, we say that \( v \in V \) is a real vector if \( \chi_{\mathbb{C}G(v)} \) is real-valued.

**Lemma 1.9.** Suppose \( v \in V \) is a real vector, and \( (n,p) \neq (1,3) \). Let \( H \leq G \) with \( (r,|H|) = 1 \). Then \( V_{\mathbb{C}G(v)} \) is self-dual.

**Proof.** The Brauer character of \( \mathbb{C}H(v) \) on \( V \) is \( \phi_{\mathbb{C}H(v)} \). Since \( \phi \) agrees with \( \chi \) up to sign on the \( r' \)-elements of \( G \) by Lemma 1.7, it follows that \( \phi_{\mathbb{C}H(v)} \) is real-valued. Hence \( V_{\mathbb{C}H(v)} \) and its dual have the same Brauer character. Since \( V_{\mathbb{C}H(v)} \) is completely reducible, it must then be self-dual. □

**Definition 1.10.** Let \( H \) be a finite group. We say \( H \) is almost perfect if \( H/H' \) is an elementary abelian 2-group.

**Lemma 1.11.** Let \( V, K, \) and \( \psi \) be as above. Suppose that \( v \in V \) and \( N_{K} \langle \psi \rangle = H \times Z(E) \) for a subgroup \( H \) of \( K \). Suppose that \( \psi_{H} \) is real-valued and that \( |H : \mathbb{C}H(v)| \leq 2 \). Then \( v \) is a real vector. In particular, \( v \) is real if \( N_{K} \langle \psi \rangle = H \times Z(E) \), \( \psi_{H} \) is real-valued, and \( H \) is almost perfect.

**Proof.** By Definition 1.8, it suffices to show that \( \chi_{\mathbb{C}G(v)} \) is real-valued. Let \( Z = Z(GL(V)) \). Then \( N_{G} \langle \psi \rangle = HZ \).

If \( H \leq \mathbb{C}G(v) \), then \( \mathbb{C}G(v) = H \) and \( \chi_{\mathbb{C}G(v)} = \chi_{H} = \psi_{H} \) is real-valued. If \( |H : \mathbb{C}H(v)| = 2 \), then \( \mathbb{C}G(v) \) has index 2 in \( H \times \langle -1 \rangle \) and \( \mathbb{C}G(v) = H \). Since \( \chi \) extends \( \psi \), the restriction of \( \chi \) to \( H \times \langle -1 \rangle \) is real-valued. Thus \( v \) is a real vector. □

2. Some non-generic cases

Let \( K \) be as in Section 1. In Section 3, we will introduce a subgroup \( L \) of \( K \) such that \( L \cong GL(n,p) \). In the “generic” situation, we will be able to show that \( \mathbb{C}L' \) contains a real vector. In this section, we dispose of certain cases which must be handled by other methods.
Lemma 2.1. Suppose \( n = 1 \) and \( p = 2 \). Then \( V \) contains a real vector if \( r \notin \{5, 7, 13\} \). If \( r \) is 5 or 13, so that we are in Case II, then \((|G|, |V|) = 1 \) and there exists no \( v \in V \) such that \( V_{C_G(v)} \) is self-dual. If \( r = 7 \) and we are in Case IV, then \((|G|, |V|) = 1 \) and there exists no \( v \in V \) such that \( V_{C_G(v)} \) is self-dual. If \( r = 7 \) and we are in Case III, then \( V \) contains a real vector.

Proof. Let \( Z = Z(GL(2, r)) = Z(GL(V)) \). Either \( r \equiv 1 \pmod{4} \) and we are in Case II, or \( r \equiv 3 \pmod{4} \) and we are in Case III or IV. We have \( G = KZ \). If \( r \equiv 3 \pmod{8} \) and we are in Case III, then, by Proposition 1.4, \( K = K^+(1, 2, r) \) is semidihedral of order 16. Hence \( K^+(1, 2, r) \leq K^-(1, 2, r) \cong GL(2, 3) \). If \( r \equiv 7 \pmod{8} \) and we are in Case III, then \( K \) is dihedral of order 16 and \( G = K \times O_2(Z) \). If \( v \in V \) is a nonzero vector, then \( C_G(v) \leq O_2(G) \cong D_{16} \), and so \( v \) is real by Definition 1.8.

Thus we may assume that we are in Case II or Case IV. Hence \(|G| = 24(r - 1)\) and \( G/Z \cong S_4 \). Let \( \overline{G} = G/Z \). If \( \langle v \rangle \in P_1(V) \) lies in a regular \( \overline{G} \)-orbit, then \( N_G(v) \) has order \( r - 1 \) or \( 2(r - 1) \), and \( v \) is a real vector. Now \( \overline{G} - \{1\} \) consists of three involutions and four disjoint pairs \( \{x, x^{-1}\} \) of elements of order 3. Each involution in \( \overline{G} \) fixes at most two points in \( P_1(V) \), as does each pair of elements of order 3. Thus at most 14 points in \( P_1(V) \) are fixed by some nonidentity element of \( \overline{G} \). Hence \( \overline{G} \) has a regular orbit on \( P_1(V) \) when \( r > 13 \). If \( r = 11 \), then \( r - 1 \) is divisible by neither 3 nor 4, and so \( \overline{G} \) acts regularly on \( P_1(V) \). Hence real vectors exist when \( r > 13 \) and when \( r = 11 \).

If \( r = 3 \), then \( G = GL(2, 3) \). If \( v \) is a nonzero vector in \( V \), then \( C_G(v) \cong S_3 \). Thus every vector in \( V^\# \) is real, although \( V_{C_G(v)} \) is not self-dual. If \( r = 9 \), then \( G \) is conjugate in \( GL(2, 9) \) to \( G_0Z \), where \( G_0 \) is the image of the natural embedding of \( GL(2, 3) \) into \( GL(2, 9) \). If we take \( v \) to be a nonzero vector in \( GF(3)^2 \leq GF(9)^2 \), then \( C_G(v) \cong S_3 \) as above, so real vectors exist when \( r = 9 \).

Next suppose \( r = 5 \). Then \( |G| = 96 \) and \( G \) acts transitively on \( V^\# \); see [MW, Theorem 6.8] and the subsequent remarks on [MW, p. 101]. Thus \(|C_G(v)| = 4\) for every \( v \in V^\# \). By complete reducibility, \( V = \langle v \rangle \oplus \langle w \rangle \), where \( \langle w \rangle \) is \( C_G(v) \)-invariant. Hence \( C_G(v) \cong Z_4 \) and \( V_{C_G(v)} \) is not self-dual, as desired.

If \( r = 7 \), then \(|G| = 144 \) and \( G \) acts transitively on \( V^\# \) as above. Hence \(|C_G(v)| = 3\) for all \( v \in V^\# \). Complete reducibility implies again that \( V_{C_G(v)} \) is not self-dual, as desired.

Finally suppose \( r = 13 \). Complete reducibility implies that \( N_G(v) \) is abelian for every \( v \in V^\# \). Hence the image of \( N_G(v) \) in \( \overline{G} \cong S_4 \) is also abelian. Since the inverse image in \( G \) of \( O_2(\overline{G}) \) is nonabelian, the image of \( N_G(v) \) in \( \overline{G} \) must be cyclic. Since cyclic subgroups of \( S_4 \) have index at least 6, the orbits of \( G \) on \( P_1(V) \) have size at least 6. Hence \( G \) has two orbits on \( P_1(V) \), of sizes 6 and 8. If \( \langle v \rangle \) belongs to the orbit of size 6, then \( N_G(v) = Z \times C_G(v) \) and \( C_G(v) \cong Z_4 \). If \( \langle v \rangle \) belongs to the orbit of size 8, then \( C_G(v) \cong Z_3 \). Complete reducibility implies that \( V_{C_G(v)} \) is never self-dual, as desired.

Lemma 2.2. Suppose \( n = 1 \), \( p = 3 \), and \( r \notin \{7, 13\} \). Then there exists \( v \in V \) such that \( V_{C_G(v)} \) is self-dual. If \( n = 1 \), \( p = 5 \), and \( r > 11 \), then there exists \( v \in V \) such that \( V_{C_G(v)} \) is self-dual.
Proof. Suppose \( n = 1 \) and \( p = 3 \). Let \( \omega \) be an element of order 3 in the multiplicative group of \( GF(r) \). Let
\[
c = \begin{pmatrix} 0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & \omega & \omega^2 \\
0 & 1 & 0 \\
0 & 0 & 1 \end{pmatrix}.
\]
Then \( c \) and \( d \) generate an extraspecial group \( E \) of order 27 and exponent 3; see [Go p. 207]. Without loss of generality, \( G \) is the normalizer in \( GL(3, r) \) of \( E \). Let \( \mathcal{B} \) be the set of all points in \( P_1(V) \) fixed by some noncentral subgroup of \( E \). Since \( E/Z(E) \) is generated by the images of \( c \) and \( d \), every point in \( \mathcal{B} \) is fixed by one of \( c, d, dc \), or \( d^{-1}c \). We compute the eigenvectors of these four matrices and conclude that \( \mathcal{B} \) consists of the Brauer characters of
\[
\begin{bmatrix} \[1, 0, 0, \] \[0, 1, 0, \] \[0, 0, 1, \] \[1, 1, 1, \] \[1, \omega, \omega^2, \] \[1, \omega^2, \omega, \] \[\omega, 1, \] \[1, \omega, \] \[1, 1, \omega, \] \[\omega^2, 1, 1, \] \[1, \omega^2, 1, \] \end{bmatrix}
\]
and \( 1, 1, \omega^2 \). Let
\[
t = \begin{pmatrix} 0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \end{pmatrix}.
\]
One checks that \( t \in N(E) = G \). Since \( \text{det}(t) = -1 \), we have \( t = t_0 \((-id.) \), where \( t_0 \in G \cap SL(3, r) \). Now \( G = KZ \) with \( K \) as in Proposition 1.5 and \( Z = Z(GL(V)) \); thus \( K/E \cong SL(2, 3) \). We can write \( t_0 = yz \), with \( y \in K \) and \( z \in Z \). Since \( t_0 \) is an involution and \( |KZ : K'Z| = 3 \), we have \( y \in K'Z \cap K = K'(Z \cap K) = K' \). Since \( \text{det}(t_0) = 1 \), we have \( \text{det}(z) = 1 \). It follows that \( z \in Z(E) \) and so \( t_0 \in K \). We have \( C_K(t_0) = SZ(E) \), with \( S \cong SL(2, 3) \) and \( Z(S) = \langle t_0 \rangle \).

Let \( W = [V, t_0] = C_V(t) \) and \( Y = C_V(t_0) = \langle V, t \rangle \). Then \( W \) and \( Y \) are irreducible \( S \)-modules of dimension 2 and 1, respectively, and \( V = W \oplus Y \). We claim that \( NG(\langle w \rangle) \leq SZ \) for all \( \langle w \rangle \in P_1(W) \setminus \mathcal{B} \). To see this, suppose that \( x \in NG(\langle w \rangle) \) and \( x \notin SZ \). Write \( x = se \) with \( s \in SZ \) and \( e \in E \setminus Z(E) \). Then \( [t_0, x] = [t_0, s] = [t_0, e] \in E \setminus Z(E) \). Hence a noncentral subgroup of \( E \) fixes \( \langle w \rangle \), contradicting the fact that \( \langle w \rangle \notin B \). This proves the claim.

Since \( W = C_Y(t) \), the explicit list of vectors in \( \mathcal{B} \) shows that \( |\mathcal{B} \cap P_1(W)| = 4 \). Let \( \mathcal{F} \) be the image of \( S \) in \( PGL(W) \), so that \( \mathcal{F} \cong A_4 \). As in the proof of Lemma 2.1, at most 6 points in \( P_1(W) \) are fixed by involutions in \( \mathcal{F} \) and at most 8 points in \( P_1(W) \) are fixed by elements of order 3 in \( \mathcal{F} \). Hence if \( |P_1(W)| > 4 + 6 + 8 = 18 \), there exists \( \langle w \rangle \in P_1(W) \) such that \( NG(\langle w \rangle) \leq Z(S) \cong \langle t \rangle \). It follows that \( C_G(\langle w \rangle) = \langle t \rangle \) and so \( V_{C_G(w)} \) is self-dual. Since \( r \) is odd, \( r = 1 \pmod 3 \), and \( r \) is not 7 or 13, we have \( r > 19 \). Hence \( |P_1(W)| > 18 \) and there exists \( w \in W \) such that \( V_{C_G(w)} \) is self-dual.

Now suppose \( n = 1, \ p = 5, \) and \( r > 11 \). As above, let \( \mathcal{B} \) denote the set of all points in \( P_1(V) \) fixed by some noncentral subgroup of \( E \). Since \( E/Z(E) \) contains 6 subgroups of order 5, and noncentral elements of order 5 have no repeated eigenvalues on \( V \), we have \( |\mathcal{B}| \leq 6 \cdot 5 = 30 \). Write \( K = SE \) with \( S \cong SL(2, 5) \) and let \( \langle u \rangle = Z(S) \). It follows from Lemma 1.2 that \( V = [V, u]\oplus C_V(u) \) is the decomposition of \( V \) into irreducible \( S \)-modules of dimension 2 and 3, respectively. Let \( \alpha \) and \( \beta \) be the Brauer characters of \( S \) afforded by \( [V, u] \) and \( C_V(u) \), respectively. Then \( \alpha(1) = 2 \) and \( \beta(1) = 3 \). Since \( (10, r) = 1 \), \( \beta \) may be viewed as an ordinary irreducible character of \( S/\langle u \rangle \cong A_5 \) if \( r \) is not a power of 3. If \( r \) is a power of 3, then Lemma 1.2 implies that \( \beta \) is the restriction to \( 3^r \)-elements of an ordinary irreducible character of \( A_5 \). Since \( \beta \) is real-valued, it follows that elements of order 5 in \( S \) have distinct
Proof. $K$ is a semidirect product $SE$, with $S \cong SL(2,p)$ and $E$ extraspecial of order $p^7$ and exponent $p$. Let $Z(S) = \langle t \rangle$. Let $T \leq S$ be the group of diagonal matrices in $S \cong SL(2,p)$. Then $|T| = p - 1$ and $T$ is inverted by an element $x \in S$ such that $x^2 = t$. Let $N = (T, x) = NS(T)$. Then $|N : T| = 2$ and $N/\langle t \rangle$ is dihedral of order $p - 1$. Also $N$ acts irreducibly on $E/Z(E)$.

We claim that $C_V(T) > 0$. Since $\dim C_V(T) = \dim C_{\overline{V}}(T)$, where $\overline{V} = \overline{GF}(r) \otimes V$, it suffices to show that $\dim C_{\overline{V}}(T) > 0$. Following the proof of Lemma 1.7, we let $\rho : K \to GL(V)$ be the natural inclusion, and let $\sigma K \to GL(V)$ be a representation whose Brauer character is the restriction of $\psi$ to the $r'$-elements of $K$. Since $\psi_E = \bar{\phi}_E = \theta$ we may replace $\sigma$ by an equivalent representation so that $\rho_E = \bar{\sigma}_E$. It follows as in the proof of Lemma 1.7 that $\rho(x) = \mu(x)\sigma(x)$ for a linear character $\mu : K \to GF(r')$, for all $x \in K$. Since $K = K'$ we have $\rho = \sigma$. Hence $\overline{V}$ is the reduction of a characteristic zero $K$-module which affords $\psi$. By Lemma 1.2, $\psi_S$ is the sum of two irreducible characters, of degrees $(p - 1)/2$ and $(p + 1)/2$. From the character table of $SL(2,p)$ (see e.g. [D, p.228]), we find that $(\psi_T, 1_T) = 1$. Hence $\dim C_{\overline{V}}(T) > 0$, proving the claim.

Now $N$ acts as a group of order $1$ or $2$ on $C_V(T)$. Let $v \in C_V(T)$ be a $N$-eigenvector. Then $N_\delta(v) \geq N$. Since $\overline{V}$ is the reduction of a characteristic zero module that affords $\psi$, the final assertion of Lemma 1.2 implies that $N_\delta(v)$ is a proper subgroup of $S$.

We next claim that $N_K(\langle v \rangle) = N_S(\langle v \rangle)Z(E)$. To see this, let $y \in N_K(\langle v \rangle)$. Then $t^y = t[y, t]$. If $[t, y] \neq 1$, then $[t, y] \in E\setminus Z(E)$ and $[t, y] \in N_K(\langle v \rangle)$. Since $N \leq N_K(\langle v \rangle)$ acts irreducibly on $E/Z(E)$, this would force $E \leq N_K(\langle v \rangle)$, which is false. Hence $y \in C_K(t) = SZ(E)$, and so $N_K(\langle v \rangle) = N_S(\langle v \rangle)Z(E)$, as claimed.

From the list of subgroups of $PSL(2,p)$, we see that $N$ is maximal in $S$ when $p \geq 13$. When $p = 11$, $N$ has an overgroup in $S$ isomorphic to $SL(2,5)$. When $p = 7$, $N$ has an overgroup which is an extension of $S_3$ by $Q_8$. Since the constituents of $\psi_S$ are real on $p'$-elements (see [D, p. 228]), it follows that $\psi_{N_S(\langle v \rangle)}$ is real. Since $|N_S(\langle v \rangle) : C_S(\langle v \rangle)| \leq 2$ and $N_K(\langle v \rangle) = N_S(\langle v \rangle)Z(E)$, Lemma 1.11 implies that $v$ is a real vector when $p > 5$.

If $p = 5$ and $r = 11$, then either $N_S(\langle v \rangle) = N \cong Q_8$ or $N_S(\langle v \rangle) \cong SL(2,3)$. If $N_S(\langle v \rangle) \cong SL(2,3)$, then $N_S(\langle v \rangle) = C_S(\langle v \rangle)$, since $3$ does not divide $r - 1$. As above $N_K(\langle v \rangle) = N_S(\langle v \rangle)Z(E)$, and the restriction of $\psi$ to $N_S(\langle v \rangle)$ is real-valued. Since $|N_S(\langle v \rangle) : C_S(\langle v \rangle)| \leq 2$, Lemma 1.11 implies that $v$ is a real vector when $p = 5$ and $r = 11$, as desired.

Having completed the $n = 1$ case, we proceed to find real vectors in $V$ in some nongeneric situations in which $p = 2$ and $n$ is $2$ or $3$. For the cases considered in
Lemma 2.4, we can take the real vector to be a decomposable tensor. In Lemma 2.5, we can use a counting argument. Lemma 2.6 has a local group-theoretic flavor.

**Lemma 2.4.** Suppose \( p = n = 2 \). In Case III, \( V \) contains a real vector. Also \( V \) contains a real vector in Case II when \( r \) is a power of 3. If \( p = 2, \ n = 3, \ r \) is a power of 3, and we are in Case IV, then \( V \) contains a real vector.

**Proof.** Suppose we are in Case III. View \( E \) as a central product \( E_1 * E_2 \), with \( E_1 \cong E_2 \cong Q_8 \). Then \( E \) preserves a tensor decomposition \( V = V_1 \otimes V_2 \); i.e. \( E_1 \leq GL(V_1) \otimes \text{id} \) and \( E_2 \leq \text{id} \otimes GL(V_2) \). Let \( t \in GL(V) \) be the involution that sends \( v_1 \otimes v_2 \) to \( v_2 \otimes v_1 \) for all \( v_1, v_2 \). There exist subgroups \( K_1 \) and \( K_2 \) of \( GL(V_1) \otimes \text{id} \) and \( \text{id} \otimes GL(V_2) \) respectively, such that \( K_1 \cong K_2 \cong K^{-1}(1,2,3) \) and such that \( t \) interchanges \( K_1 \) and \( K_2 \).

Let \( J = K_1 K_2 \langle t \rangle \). Then \( J \) is isomorphic to \( K^{-1}(1,2,3) \wr Z_2 \), modulo a central subgroup of order 2. Clearly \( J \leq G = N_{GL(V)}(E) \). Since \( G/EZ \cong O^+(4,2) \cong S_3 \wr Z_2 \), we have \( G = JZ = KZ \) and \( G' = J' = K' \). Since \( r \equiv 3(\text{mod} \ 4) \), we have \( K'/G' = O_2(G/G') = J/G' \). Thus \( J = K \).

Suppose first that \( r \) is not a power of 3 and \( r \neq 7 \). Arguing as in the second paragraph of the proof of Lemma 2.1, we choose \( v \) with slight abuse of notation \( v \in V_1 \) and \( v_2 = tv_1 \in V_2 \) such that \( N_{K_1} (v_1) \cong N_{K_2} (v_2) \) is a 2-group; this uses the hypothesis \( r \neq 7 \). Since \( r \equiv 3(\text{mod} \ 4) \) and \( E_1 \cong E_2 \cong Q_8 \), we have \( N_{E_1} (v_1) = Z(E_i) = Z(E) \) for \( i = 1, 2 \).

Let \( v = v_1 \otimes v_2 \). Then \( N_E (v) = Z(E) \) and \( N_K (v) \) is a 2-group. Since \( 4 \mid (r-1) \), this implies that \( N_K (v) = C_K (v) \times Z(E) \). Now \( C_K (v) \) is isomorphic to a 2-subgroup of \( K/E \cong S_3 \wr Z_2 \). Hence \( C_K (v) \) has exponent at most 4. Since \( Q(\psi) = Q(\sqrt{-2}) \) by Proposition 1.5, it follows that \( \psi \) is rational on \( C_K (v) \). Hence \( v \) is a real vector by Lemma 1.11.

Suppose next that \( r = 7 \). With the help of GAP, we find that there exists \( v \in V \) such that \( |C_G (v)| = 48 \) and \( V_{C_G (v)} \) contains an irreducible self-dual submodule of dimension 3. Thus \( V_{C_G (v)} \) is self-dual.

Now suppose \( r \) is a power of 3. With notation as in the third paragraph of this proof, we have \( K_1 \cong K_2 \cong GL(2,3) \). As in the third paragraph of the proof of Lemma 2.1, there exist vectors \( v_i \in V_i (i = 1, 2) \) such that \( C_K (v_i) \cong S_3 \) and \( v_2 = tv_1 \). Let \( v = v_1 \otimes v_2 \). As above, \( N_E (v) = Z(E) \). Hence \( C_K (v) \cong S_3 \wr Z_2 \), and \( N_K (v) = C_K (v) \times Z(E) \). Since \( S_3 \wr Z_2 \) is a real group, \( \psi \) is real on \( C_K (v) \). Thus \( v \) is a real vector by Lemma 1.11.

If we are in Case IV with \( n = 3 \) and \( r \) a power of 3, then an argument analogous to that in the preceding paragraph produces a vector \( v = v_1 \otimes v_2 \otimes v_3 \) in \( V = V_1 \otimes V_2 \otimes V_3 \) such that \( C_K (v) \) contains a \( S_3 \wr S_3 \) subgroup and such that \( N_E (v) = Z(E) \).

The image of \( C_K (v) \) in \( K/E \cong O^-(6,2) \) can’t all be of \( O^-(6,2) \), since \( \text{Aut}(E) \) doesn’t split over \( \text{Inn}(E) \) by [Gr1] Theorem 1. Since the image in \( K/E \) of our \( S_3 \wr S_3 \) subgroup is a maximal \( O^-(2,2) \wr S_3 \) subgroup of \( O^-(6,2) \), we have \( C_K (v) \cong S_3 \wr S_3 \) and \( N_K (v) = C_K (v) \times Z(E) \). It follows as in the preceding paragraph that \( \psi \) is real on \( C_K (v) \). Again \( v \) is a real vector by Lemma 1.11.

Finally, suppose we are in Case II with \( n = 2 \) and \( r \) a power of 3. Let \( Z_4 \) denote the unique subgroup of \( Z(GL(V)) \) of order 4 and write \( E = E_0 \ast Z_4 \), with \( E_0 = E_1 \ast E_2 \), where \( E_1 \cong E_2 \cong Q_8 \). As in the first two paragraphs of this proof, \( E_0 \) preserves a tensor decomposition \( V = V_1 \otimes V_2 \). Also \( G \) contains a subgroup \( J = K_1 K_2 \langle t \rangle \), with \( J/E \cong O^+(4,2) \cong S_3 \wr Z_2 \), and \( K_1 \cong K_2 \cong K^{-1}(1,2,3) \cong 

---

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
GL(2,3). For $i = 1, 2$, choose $v_i \in V_i$ such that $C_{K_i}(v_i) \cong S_3$ and $v_2 = tv_1$. Let $v = v_1 \otimes v_2$.

Then $C_J(v)$ contains a subgroup isomorphic to $S_3$ wr $Z_2$. Since $C_J(v)$ acts irreducibly on $E/Z(E)$, it follows that $N_E(v) = Z(E)$. Hence $N_J(v) = C_J(v) \times Z(E)$ and $C_J(v) \cong S_3$ wr $Z_2$. Let $Z = Z(GL(V))$. Then $C_{EZ}(v) = 1$. Hence if $C_0(v)$ properly contains $C_J(v)$, then $C_{EZ}(v)EZ/EZ$ properly contains $C_J(v)EZ/EZ$. But the last group is a maximal subgroup of $G/EZ \cong Sp(4,2) \cong S_6$. Thus if $C_G(v) > C_J(v)$, then $C_G(v) \cong S_6$. But $S_6$ contains a Frobenius group of order 20, which has no faithful representation over $GF(r)$ of degree less than 4. It follows that $C_G(v) = C_J(v)$. Hence $C_G(v)$ is the real group $S_3$ wr $Z_2$, and so $\chi_{C_G}(e)$ is real-valued. By Definition 1.8, $v$ is a real vector.

**Lemma 2.5.** Suppose $p = n = 2$ and we are in Case IV. Then $V$ contains a real vector if $r \not\in (3, 7)$. If $r = 3$, then $G$ contains a subgroup $H$ of order $2^7 \cdot 5$ such there is no $v \in V$ for which $C_{Hy}(v)$ is self-dual.

**Proof.** Suppose we can find $v \in V$ such that $3 \nmid |N_K(v)|$ whenever $3|r-1$, such that $5 \nmid |N_K(v)|$ whenever $5|r-1$, and such that $C_E(v) = 1$. Since $K$ is a $(2, 3, 5)$-group, our assumptions imply that $N_K(v)/C_K(v)$ is a 2-group. Since $Z(E) \leq N_K(v)$ and $4 \nmid r - 1$, we have $|N_K(v)/C_K(v)| = 2$ and $N_K(v) = C_K(v) \times Z(E)$. Now $C_K(v)$ is isomorphic to a subgroup of $K/E \cong O^-(4, 2) \cong S_5$. Hence the exponent of $C_K(v)$ divides 60. By Proposition 1.5, $Q(\psi) = Q\left(\sqrt{\pm 2}\right)$. Hence the restriction of $\psi$ to $C_K(v)$ has values in $Q(\psi) \cap Q_{60} = Q$. Now Lemma 1.11 implies that $v$ is a real vector.

If 3 divides $r - 1$, let $n_3$ be the number of points in $P_1(V)$ which are fixed by some element of order 3 in $K$. Define $n_5$ analogously, and let $n_2$ be the number of points in $P_1(V)$ fixed by some noncentral involution of $E$. For convenience, define $n_3 = 0$ if $3 | r - 1$ and $n_5 = 0$ if $5 | r - 1$.

We claim that $n_3 \leq 80(r + 1)$. There is a natural embedding of $K_1 * K_2$ in $K$, where $K_1 \cong K^+(1, 2, r)$ and $K_2 \cong K^-(1, 2, r)$. Let $x \in K_2$ have order 3. Then the central product $N = K_1 * N_{K_2}(x)$ has order 96. Since a 3-Sylow normalizer of $O^-(4, 2) \cong S_5$ has order 12, we see that $N$ is the full normalizer of $\langle 0 \rangle$ in $K$. We may assume that 3 divides $r - 1$, so that, in particular, $r$ is not a power of 3. To compute $\psi(x)$, we restrict $\psi$ to $K_1 * K_2$. Since this restriction is faithful and since $\psi(1) = 4, \psi$ restricts irreducibly to $K_1 * K_2$ and so $\psi_{K_2} = 2\beta$ for some $\beta \in Irr(K_2)$ with $\beta(1) = 2$. Thus the restriction of $\psi$ to $K_2^+$ equals $2\alpha$, where $\alpha \in Irr(K^+) = Irr(SL(2, 3))$, $\alpha(1) = 2$, and $\alpha$ extends to $K_2$. The character table of $SL(2, 3)$ shows that $\alpha(x) = -1$, and so $\psi_2(x) = -2$. The fixed point space of $x$ on $V$ has dimension $\langle \phi(1), 1(x) \rangle$. Since $\phi(x) = \pm \psi(x)$ by Lemma 1.7, and since 3 does not divide $4 + 2 + 2$, we have $\phi(x) = -2$ and $\langle \phi(1), 1(x) \rangle = (1/3)(4 - 2 = 0)$. It follows that $x$ has two eigenspaces on $V$, each of dimension 2. Hence $x$ fixes 2($r + 1$) points in $P_1(V)$, and so the number of points in $P_1(V)$ fixed by some subgroup of order 3 in $K$ is at most $|K:N|_2 2(r + 1) = 80(r + 1)$, as claimed.

If 5 divides $r - 1$ and $y \in K$ has order 5, then $\phi(y) = \pm \psi(y)$ by Lemma 1.7. Since $\psi(y) \in Q_5 \cap Q\left(\sqrt{\pm 2}\right) = Q$, we have $\phi(y) \in Q$, and so $y$ has four distinct eigenvalues on $V$. Hence $y$ fixes only four points in $P_1(V)$. Since $K$ has 96 5-Sylow subgroups, we have $n_5 \leq 4 \cdot 96 = 384$.

One checks that $D_8 * Q_8$ contains 10 noncentral involutions, corresponding to the 5 singular points in the orthogonal space $E/Z(E)$. Since $\psi$, or equivalently $\theta$, vanishes on each such involution, each such involution has two eigenspaces on $V$,
both of dimension 2, and therefore fixes $2(r + 1)$ points in $P_1(V)$. If $t \in E$ is a noncentral involution and $(z) = Z(E)$, then $t$ and $t z$ have the same eigenspaces. Hence $n_2 \leq 5(2(r + 1)) = 10(r + 1)$.

The first paragraph of this proof shows that $V$ contains a real vector whenever $n_2 + n_3 + n_5 < |P_1(V)| = (r^4 - 1)/(r - 1)$. The bounds $80(r + 1)$, 384, and $10(r + 1)$ derived above are sufficient to prove that $n_2 + n_3 + n_5 < |P_1(V)|$ if $r \notin \{3, 7\}$.

Now suppose $r = 3$. By [MW] p.101, $G$ contains a subgroup $H$ with $|H| = 2^7 \cdot 5$, such that $H$ is transitive on the nonzero vectors of $V$. Moreover, $H$ contains a subgroup $H_0 \geq E$ of order $2^5 \cdot 5$ such that $H_0$ is also transitive on the nonzero vectors of $V$. Let $v \in V$ be a fixed nonzero vector. Then $|C_E(v)| = 2$ and so $C_E(v) \leq Z(C_H(v))$ and $C_H(v)/C_E(v) \cong Z_3$. See [MW] Theorem 6.8(a)]. It follows that $C_H(v) \cong Z_3$ or $C_H(v) \cong Z_4 \times Z_2$. Since $4 \nmid 3^3 - 1$, $V_{C_H(v)}$ has no irreducible summand of dimension 3. It follows that $V_{C_H(v)}$ is the direct sum of irreducible submodules of dimensions 1, 1 and 2.

Now $C_E(v) = \langle t \rangle$ for a noncentral involution $t$ of $E$. The two-dimensional irreducible direct summand $V_{C_H(v)}$ is $\langle V, \langle t \rangle \rangle$, the $-1$-eigenspace of $t$. Suppose $C_H(v) = \langle x \rangle \times \langle t \rangle$, with $\langle x \rangle \cong Z_3$. Then $\langle t, x^2 \rangle$ must centralize $C_V(t)$. Hence $\langle t, x^2 \rangle$ acts faithfully on $\langle V, \langle t \rangle \rangle$, an irreducible $C_H(v)$-module. This contradicts Schur’s Lemma. It follows that $C_H(v) \cong Z_8$.

We claim that $\phi$ is not real-valued on $C_H(v)$. To see this, it suffices to show that $\eta$, the Brauer character of $C_H(v)$ afforded by $\langle V, \langle t \rangle \rangle$, is not real-valued. The faithful image of $C_H(v)$ in $GL([V, \langle t \rangle]) = GL(2, 3)$ is contained in a 2-Sylow subgroup $S$ of $GL(2, 3)$, and $S$ is semidihedral of order 16. Hence $\eta$ extends to a faithful irreducible Brauer character $\tilde{\eta}$ of $S$, such that $\tilde{\eta}(1) = 2$ and $\tilde{\eta}$ is an ordinary irreducible character of $S$. Thus $\eta$ and $\tilde{\eta}$ take values $\pm \sqrt{-2}$ on elements of order 8. Hence $\eta$ is not real-valued. This completes the proof.

**Lemma 2.6.** Suppose $p = 2, n = 3, r$ is not a power of 3, and we are in Case IV. Then $V$ contains a real vector, except possibly when $r = 7$.

**Proof.** By [A], $\Omega^-(6, 2)$ contains a maximal $U_3(2)$ subgroup, which is an extension of $SL(2, 3)$ by an extraspecial subgroup of order 27 and exponent 3. This subgroup has index 2 in a maximal subgroup $N$ of $O^- (6, 2)$. Since $N/O_3(N)$ acts faithfully on $O_3(N)/Z(O_3(N)) \cong Z_3 \times Z_3$, we have $N/O_3(N) \cong GL(2, 3)$ and $|N:C_N(Z(O_3(N)))| = 2$. Let $F \leq K$ be a subgroup of order 27 whose image in $K/E \cong O^- (6, 2)$ is $O_3(N)$. Let $\pi: K \rightarrow K/E$ be the natural homomorphism. Since $FE$ is a normal subgroup of $\pi^-(N)$, the Frattini argument implies that $\pi^-(N) = EN$, where $N$ is the normalizer in $\pi^-(N)$ of $F$. Since $Z(F)$ is fixed point free on $E/Z(E)$, we have $N \cap E = Z(F)$ and so $N/Z(E) \cong \pi^-(N)/E = N$. Hence $N/Z(E)$ is an extension of $GL(2, 3)$ by $F$.

Let $\eta = \phi_N$ be the Brauer character of $N$ afforded by $V$. Since $|N| = 2^5 \cdot 3^4$ and $r$ is not a power of 3, $\eta$ is an ordinary character of $N$. By the proof of Lemma 1.7, $\eta = \psi_N \mu$ for a linear character $\mu$ of $N$ with $\mu^2 = 1$. Since $Z(F)$ acts faithfully on $V$, $\eta F$ contains a faithful irreducible constituent $\omega$, and $\omega(1) = 3$. Since $\omega$ and $\overline{\omega}$ are conjugate under $N$, $\eta F$ also contains $\overline{\omega}$. Since $\eta(1) = 8$ and $F$ has no faithful representation over $GF(r)$ of degree less than 3, it follows that $V_{\eta F}$ has an irreducible submodule $X$ of dimension 6, and $X = [V, Z(F)]$. Let $Y = C_V(Z(F))$. Then $V_{\eta F} = X \oplus Y$. Since $N$ acts transitively on $F/Z(F)$ and on $\text{Irr}(F/Z(F))$, Clifford’s Theorem implies that $Y = C_V(F)$. Let $M = N \cap K' = C_N(Z(F))$, so
that \( M/Z(E) \) is an extension of \( SL(2,3) \) by \( F \). Since \( \omega \) and \( \overline{\omega} \) are not conjugate under \( M \), Clifford’s Theorem implies that \( X_M \) is not absolutely irreducible, and so the Brauer character of \( X_M \) is the sum of two complex conjugate irreducible characters of degree 3; note that \( \eta_M = \psi_M \mu_M = \psi_M \), which is rational-valued by Corollary 1.6. On the other hand, the Brauer character of \( X_N \) is irreducible of degree 6, and is induced from \( M \), and so vanishes on \( N \setminus M \). In particular, the Brauer character of \( X_N \) is real-valued.

Since \( Z(E) \) acts as \(-1\) on \( V \), the 3-dimensional irreducible complex representations of \( M \) in the preceding paragraph are faithful. It follows that \( M \) splits over \( Z(E) \). Indeed \( M = Z(E) \times O^3(M) \), since elements of \( O^3(M) \) correspond under either of the complex representations above to complex 3 \( \times \) 3 matrices of determinant order 1 or 3, while the central involution of \( E \) is represented by a scalar matrix of determinant \(-1\).

We next claim that \( O^3(M) \) splits over \( F \). Let \( L = O^3(M) \) and let \( u \in L \) be an involution. Since \( L \) contains \( [F:CF(u)] = 9 \) involutions, \( |CL(u)| = 72 \) and \( CL(u)/Z(F) \cong SL(2,3) \). By [\( \mathbb{A} \), \( \Omega^- \) (6, 2) contains no elements of order 18. Thus \( CL(u) \) contains no elements of order 9, and so \( CL(u)/Z(F) \) contains an element of order 3. Since \( O_2(C_L(u)) \cong Z_3 \), \( C_L(u) \) is a direct product \( S \times Z(F) \) with \( S \cong SL(2,3) \). Thus \( L = SF \) and \( M = Z(E) \times SF \).

We now claim that \( S \) acts faithfully and irreducibly on \( Y \). Let \( a \in S \) be an element of order 4. Let \( \beta \) be the Brauer character of \( M \) afforded by \( Y \). We saw above that the Brauer character of \( M \) afforded by \( X \) has the form \( \alpha + \overline{\alpha} \), where \( \alpha \in \text{Irr}(M) \) and \( \alpha(1) = 3 \). Now \( \alpha_S \) has two irreducible constituents, of degrees 1 and 2. It follows that \( \alpha(a) = 1 \). Now if \( a \) centralizes \( Y \), then \( \eta(a) = \alpha(a) + \alpha(a) + \beta(a) = 4 \).

By Lemma 1.3, this implies that \( |C_{E/Z(E)}(a)| = 16 \). Since \( a \in U_3(2) \), \( a \) preserves a GF(4)-vector space structure on \( E/Z(E) \). Since \( S \cap E = 1 \), the image \( \overline{\alpha} \) of \( a \) in \( K/E \cong O^- \) (6, 2) also has order 4. Since \( \overline{\alpha} \) is a unipotent transformation on \( E/Z(E) = GF(4)^3 \), this implies that \( \overline{\alpha} \) has two Jordan blocks, of sizes 1 and 2. But then \( \overline{\alpha}^2 = 1 \), a contradiction. We conclude that \( a \) does not centralize \( Y \). Since \( S/Z(S) \cong A_4 \) has no faithful 2-dimensional representation over GF(\( r \)), it follows that \( S \) acts faithfully and irreducibly on \( Y \), as claimed.

Thus \( S \) maps injectively into \( N/C_N(Y) \). Since \( Z(S) \) and \( Z(E) \) both induce \(-1\) on \( Y \), it follows that \( |C_N(Y):F| = 2 \) and \( N/C_N(Y) \) is an extension of \( S_3 \) by \( Q_8 \). Arguing as in the second paragraph of the proof of Lemma 2.1, we can choose (since \( r > 7 \) \( y \in Y \) such that \( N_S(y) = Z(S) \). It follows that \( |C_N(y):C_N(Y)| \leq 2 \). Moreover \( |C_N(y):F| \) equals 2 or 4 and \( C_N(y)^f = F \). We claim that \( |N_K(y)|_3 = 27 \); i.e. we claim that \( F \in Syl_3(N_K(y)) \). If not, let \( \widehat{F} \leq N_K(y) \) with \( F \leq \widehat{F} \) and \( |\widehat{F}| = 81 = |K|_3 \). Then \( \widehat{F} \leq N_K(F) \). Since \( N \) is maximal in \( O^- \) (6, 2) and since \( N_S(y) = Z(E) \), we have \( N_K(F) = N \). Hence \( \widehat{F} \leq N_K(y) \). Thus \( \widehat{F} \leq O^3(M) = SF \). Since \( F \) centralizes \( Y \), it follows that \( N_S(y) \) contains a subgroup of order 3, contradicting \( N_S(y) = Z(S) \). This proves the claim. It follows that 3 does not divide \( |N_K(y):C_K(y)| \).

Let \( \overline{H} \) be a maximal subgroup of \( K/E \cong O^- \) (6, 2) that contains the image \( N_K(y) \) of \( N_K(y) \). Since \( F \) acts irreducibly on \( E/Z(E) \), so does \( \overline{H} \). By [\( \mathbb{A} \), \( \overline{H} \) is either conjugate in \( O^- \) (6, 2) to \( \mathbb{N} \), or \( \overline{H} \cong S_3 \wr S_3 \). In particular, \( \overline{H} \) and \( N_K(y) \) are \( \{2,3\} \)-groups. Thus \( N_K(y)/C_K(y) \) is a cyclic 2-group whose order divides \( r - 1 \).
Since \( r \equiv 3(\text{mod } 4) \), we have \(|N_K(y):C_K(y)| = 2\) and \(N_K(y) = C_K(y) \times Z(E)\). Suppose that \( \overline{H} \cong S_3 \) or \( S_3 \). Since \( F \leq C_K(y) \) and \( F \) acts irreducibly on \( E/Z(E) \), we have \( C_E(y) = 1 \). Thus \( C_K(y) \) is isomorphic to a subgroup of \( \overline{H} \), and so the exponent of \( C_K(y) \) divides 36. Since \( Q(\psi) = Q(\sqrt{-2}) \), it follows that the restriction of \( \psi \) to \( C_K(y) \) is rational-valued. Since \( N_K(y) = Z(E) \times C_K(y) \), Lemma 1.11 implies that \( y \) is a real vector.

The other possibility is that \( \overline{H} \) is conjugate in \( O^-(6, 2) \) to \( \overline{N} \). Since \( F \leq N_K(y)' \), it follows that \( \overline{F} := FE/E \) is contained in \( \overline{H} \), which is an extension of \( SL(2, 3) \) by an extraspecial group of order 27 and exponent 3. Suppose that \( N_K(y)' \), like \( \overline{H} \), has \( Q_8 \) Sylow 2-subgroups. Then \( N_K(y) \) acts as \( SL(2, 3) \) or \( GL(2, 3) \) on \( O_3(\overline{H})/Z(O_3(\overline{H})) \). Since 27 is the exact power of 3 dividing \(|N_K(y)|\) and \(|N_K(y)'|\), this is impossible. Hence \( N_K(y) \) has cyclic 2-Sylow subgroups, and so \( N_K(y) \) has a normal 2-complement, which must be \( \overline{F} \). Thus \( \overline{N_K(y)} \) is contained in \( N_{K/E}(\overline{F}) = \overline{N} \). It follows that \( N_K(y) \leq NE \). Since \( N_E(y) = Z(E) \), and since \( N_K(y) \) has a normal 3-Sylow subgroup, so does \( N_K(y) \). Since \( F \in \text{Syl}_3(N_K(y)) \), we have \( N_K(y) \leq N_{K/E}(F) = N \). We conclude that \( N_K(y) = N_N(y) = Z(E) \times C_N(y) \). Since \(|C_N(y):F|\) divides 4, the exponent of \( C_N(y) \) divides 12. As above, this implies that the restriction of \( \psi \) to \( C_N(y) \) is rational-valued. By Lemma 1.11, \( y \) is a real vector, as desired.

\[ \square \]

3. A \( GL(n, p) \) Subgroup

In this section, we set up the machinery to handle Case I for \( n \geq 2 \) and Case II for \( n \geq 3 \). We also dispose of Cases III and IV and complete our treatment of the \( p = n = 2 \) case.

**Lemma 3.1.** Let \( M_n \) be the natural module for \( GL(n, 2) \). Then \( H^1(GL(n, 2), M_n) = 0 \) if \( n > 3 \) and \( H^2(GL(n, 2), M_n) = 0 \) if \( n > 5 \). The Schur multiplier of \( GL(n, 2) \) is trivial if \( n > 4 \).

**Proof.** For the first two assertions, see [Gr3, p. 195]. For the last assertion, see [Gr2, p. 280].

Now let \( K \) be as in Proposition 1.5 and let \( Z = Z(GL(V)) \). Suppose we are in Case I, II, or III, so that \( G/E \cong K/E \cong Sp(2n, p), Sp(2n, 2), 3 \) or \( O^+(2n, 2) \) respectively. Let \( \overline{K} = K/E \) and let \( \overline{F} = E/Z(E) \), so that \( \overline{F} \) is the natural module for \( \overline{K} \). Let \( E = \langle \overline{e}_1, \overline{f}_1 \rangle \oplus \ldots \oplus \langle \overline{e}_n, \overline{f}_n \rangle \) be a decomposition of \( E \) into a direct sum of mutually orthogonal hyperbolic planes. Let \( \overline{A} = \langle \overline{e}_1, \ldots, \overline{e}_n \rangle \) and \( \overline{A} = \langle \overline{f}_1, \ldots, \overline{f}_n \rangle \). Then \( K \) contains a subgroup \( \overline{L} \cong GL(n, p) \) which stabilizes the totally singular subspaces \( \overline{A} \) and \( \overline{A} \) of \( \overline{E} \). With respect to the basis \( \{ \overline{e}_1, \ldots, \overline{f}_1, \ldots, \overline{f}_n \} \) of \( E \), \( \overline{L} \) consists of all matrices of the form

\[
\begin{pmatrix}
g & \ast \\
\ast & g^{-T}
\end{pmatrix}
\]

where \( g \in GL(n, p) \). The fact that \( \overline{L} \leq \overline{K} \) is proved in [Hu, Theorem II. 9.24] in Cases I and II. In Case III, view \( O^+(2n, 2) \) as a subgroup of \( Sp(2n, 2) \) and observe that \( \overline{L} \) preserves the appropriate quadratic form on \( \overline{E} \). Thus \( \overline{L} \leq \overline{K} \) in this case, too. Moreover, \( \overline{A} \) and \( \overline{A} \) are indeed \( \overline{L} \)-modules.
Lemma 3.2. Suppose that \( n \geq 2 \) and we are in Case I, II, or III. Let \( \overline{L} \) be as above. Then \( G = N_{\Gamma_0(n)}(E) \) contains a subgroup \( L \) such that \( L \cap E = 1 \) and \( L(EZ)/EZ = \overline{L} \). Moreover, \( E \) contains \( L \)-invariant elementary abelian subgroups \( A \) and \( A^* \) such that \( AZ(E)/Z(E) = \overline{A} \), \( A^*Z(E)/Z(E) = \overline{A}^* \), and \( A \cap Z(E) = A^* \cap Z(E) = 1 \). Furthermore \( L \leq K \), except possibly when \( p = n = 2 \).

Proof. First suppose we are in Case I. Then \( K \) is a semidirect product \( SE \), with \( S \cong Sp(2n,p) \). Let \( L \) be the unique subgroup of \( S \) such that \( LE/E = \overline{L} \). Let \( B \) and \( B^* \) be the inverse images in \( E \) of \( \overline{A} \) and \( \overline{A}^* \), respectively. Then \( B \) and \( B^* \) are elementary abelian of order \( p^{n+1} \). Now \( H^1(L, \overline{A}) = 0 \); see e.g. [Hu, p. 124]. Since \( \overline{A}^* \) is the twist of \( \overline{A} \) by the inverse transpose automorphism, we have \( H^1(L, \overline{A}^*) = 0 \). It follows that \( B \) and \( B^* \) respectively contain \( L \)-invariant subgroups \( A \) and \( A^* \) with the desired properties.

Now suppose we are in Case III. Suppose first that \( n \geq 6 \). By Lemma 3.1, \( H^2(\overline{L}, \overline{A}) = 0 \), and so \( H^2(\overline{L}, \overline{A}^*) = 0 \). Since \( E = \overline{A} \oplus \overline{A}^* \), we have \( H^2(\overline{L}, E) = 0 \). Hence \( K \) contains a subgroup \( L \) such that \( LE/E = \overline{L} \) and \( \overline{L} \cap E = Z(E) \). By Lemma 3.1, the Schur multiplier of \( \overline{L}/Z(E) \) is trivial and so \( \overline{L} = \overline{L} \times Z(E) \). Hence \( L := \overline{L} \) satisfies \( L \cap E = 1 \) and \( LE/E = \overline{L} \).

As in Case I, let \( B \) and \( B^* \) be the inverse images in \( E \) of \( \overline{A} \) and \( \overline{A}^* \). By Lemma 3.1, \( H^1(L, \overline{A}) = 0 \). As in Case I, it follows that there exist \( L \)-invariant complements \( A \) and \( A^* \) to \( Z(E) \) in \( B \) and \( B^* \), respectively. For \( 1 \leq i \leq n \), choose \( e_i \in A \) so that \( e_iZ(E)/Z(E) = \overline{\ell}_i \) and choose \( f_i \in A^* \) so that \( f_iZ(E)/Z(E) = \overline{f}_i \). Then \( A = \langle e_1, ..., e_n \rangle \) and \( A^* = \langle f_1, ..., f_n \rangle \).

Next suppose that \( 2 \leq n \leq 5 \). Let \( K_6 = K^+ (6, 2, r) \) and let \( L_6, A_6, A^*_6 \) be the subgroups of \( K_6 \) defined above. Now \( E = E_6 \) is a central product \( E_n \circ E_6-n \), where \( E_n = \langle e_1, ..., e_n, f_1, ..., f_n \rangle \) and \( E_6-n = \langle e_{n+1}, ..., e_6, f_{n+1}, ..., f_6 \rangle \) are extraspecial of plus type. We may write \( V_6 = V_n \circ V_6-n \), with \( E_n \leq GL(V_n) \circ \text{id} \) and \( E_6-n \leq \text{id} \circ GL(V_6-n) \). Let \( G_n \) denote the normalizer in \( GL(V_n) \) of \( E_n \) and let \( G = G_6 = N_{GL(V_6)}(E_6) \). Then \( G_6 \circ \text{id} \) normalizes \( E_6 \) and centralizes \( E_6-n \).

We claim that \( G_n \circ \text{id} \) is the full centralizer of \( E_6-n \) in \( G \). To see this, let \( Z = Z(GL(V_n)) \). Since \( G/EZ \cong O^+(12, 2) \), the image in \( G/EZ \) of \( C_G(E_6-n) \) is contained in \( (G_n \circ \text{id})EZ/EZ \cong O^+(2n, 2) \). Thus

\[
C_G(E_6-n) = (G_n \circ \text{id})EZ(E_6-n) = (G_n \circ \text{id})E_nZ = G_n \circ \text{id}.
\]

Now let \( A_n = A_6 \cap C_G(E_6-n) = \langle e_1, ..., e_n \rangle \) and let \( A^*_n = A^*_6 \cap C_G(E_6-n) = \langle f_1, ..., f_n \rangle \). Let \( L_n = L_6 \cap C_G(E_6-n) \). Under the natural isomorphism of \( L_6 \) and \( L_n \) corresponds to the set of all matrices of the form

\[
\begin{bmatrix}
g & 0 \\
0 & I
\end{bmatrix}
\]

where \( g \in GL(n, 2) \). Hence \( L_n \cong GL(n, 2) \). Clearly \( L_n \cap E_n = 1 \) and \( L_nE_n/E_n \) is the subgroup \( \overline{L}_n \) defined as in the remarks following Lemma 3.1, with respect to the hyperbolic basis \( \{\overline{e}_1, ..., \overline{e}_n, \overline{f}_1, ..., \overline{f}_n\} \) of \( E_n/Z(E_n) \). Furthermore \( A_n \) and \( A^*_n \) are \( \overline{L}_n \)-invariant, intersect \( Z(E_n) = Z(E) \) trivially, and map isomorphically onto the subspaces \( \langle \overline{e}_1, ..., \overline{e}_n \rangle \) and \( \langle \overline{f}_1, ..., \overline{f}_n \rangle \) of \( E_n/Z(E_n) \), as desired.
Since $GL(n, 2)' = GL(n, 2)$ for $n \geq 3$, we have $L_n = L_n' \leq (G_n \otimes \text{id})' \leq K_n \otimes \text{id}$ for $n \geq 3$. From the natural isomorphism between $G_n$ and $G_n \otimes \text{id}$, we obtain the desired subgroups $L_n, A_n,$ and $A_n^*$ of $G_n$. These subgroups are contained in $K_n$ if $n \geq 3$. This completes the proof in Case III.

Finally, suppose we are in Case II, with $n \geq 2$. Write $E = E_0Z_4$, as at the beginning of Section 1, with $E_0$ extraspecial of plus type. Then $E/Z(E)$ is naturally isomorphic to $E_0/Z(E_0)$. Arguing as above, even though $r \neq 3 (\text{mod } 4)$, we can find $L = N_{GL(V)}(E_0) \leq N_{GL(V)}(E)$ such that $L \cong GL(n, 2)$ and $L \cap E = L \cap E_0 = 1$, with $LE/E \cong LE_0/E_0 \cong L(EZ)/EZ = \mathcal{L}$. Furthermore, we can find elementary abelian $L$-invariant subgroups $A$ and $A^*$ of $E_0$, which map isomorphically onto $\mathcal{A}$ and $\mathcal{A}^*$. Then $L = L' \leq N_{GL(V)}(E)' = K' \leq K$ when $n \geq 3$, and so the same subgroups $L, A,$ and $A^*$ satisfy the conclusion of Lemma 3.2 in Case II.

Having constructed $L$ in Lemma 3.2, we next describe $N_K(L)$. Define $\mathcal{T} \in GL(E)$ to be the transformation that sends $\mathcal{V}_i$ to $\mathcal{V}_i$ and $\mathcal{F}_i$ to $-\mathcal{V}_i$ for $1 \leq i \leq n$. Clearly $\mathcal{T}$ lies in $Sp(2n, p)$, $Sp(2n, 2)$ and $O^+(2n, 2)$ in Cases I, II, and III, respectively, $\mathcal{T}$ interchanges $\mathcal{A}$ and $\mathcal{A}^*$, and $\mathcal{T}$ induces the inverse transpose automorphism of $\mathcal{L} \cong GL(n, p)$.

**Lemma 3.3.** With notation as above, suppose that $n \geq 3$ or that $n = 2$ and $p$ is odd. Let $\mathcal{K} = K/E$. Then

(a) $N_{\mathcal{K}}(\mathcal{L}) = N_{\mathcal{K}}(\mathcal{L})' = \mathcal{T}(\mathcal{L})$.

(b) $\mathcal{T}$ is the direct sum of two absolutely irreducible and nonisomorphic $\mathcal{L}$-modules, namely $\mathcal{A}$ and $\mathcal{A}^*$. If $n \geq 3$, $\mathcal{A}$ and $\mathcal{A}^*$ are absolutely irreducible and nonisomorphic $\mathcal{L}$-modules. If $n = 2$ and $p$ is odd, then $\mathcal{A}$ and $\mathcal{A}^*$ are absolutely irreducible and isomorphic $\mathcal{L}$-modules; the remaining $p - 1$ irreducible $\mathcal{L}$-submodules of $\mathcal{K}$ are nondegenerate.

**Proof.** Once we establish (b), it will follow that $N_{\mathcal{K}}(\mathcal{L})$ and $N_{\mathcal{K}}(\mathcal{L})'$ permute $\mathcal{A}$ and $\mathcal{A}^*$. Since $N_{\mathcal{K}}(\mathcal{A}) \cap N_{\mathcal{K}}(\mathcal{A}^*) = \mathcal{L}$, part (a) will then follow.

Thus we prove (b). Since the inverse transpose automorphism of $SL(n, p)$ belongs to the diagonal automorphism group of $SL(n, p)$ for $n = 2$, but not for $n > 2$, we may assume that $n = 2$ and $p$ is odd. Since $[-1 1_0]$ induces the inverse transpose automorphism of $SL(2, p)$, $\mathcal{A}$ and $\mathcal{A}^*$ are isomorphic modules for $\mathcal{L} \cong SL(2, p)$. It remains to show that $\mathcal{E}$ contains $p + 1$ irreducible $\mathcal{L}$-modules, $p - 1$ of which are nondegenerate. By [GG, p. 79], $\mathcal{E}$ contains exactly $p + 1$ irreducible $\mathcal{L}$-submodules.

In terms of the basis $\{\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{F}_4\}$ of $\mathcal{E}$, we have $\mathcal{A} = \langle \mathcal{F}_1, \mathcal{F}_2 \rangle$, and $\mathcal{A}^* = \langle \mathcal{F}_3, \mathcal{F}_4 \rangle$. Now let $\mathcal{F}_1$ and $\mathcal{F}_2$ be the standard generators of $\mathcal{L}$:

$$
\mathcal{F}_1 = \begin{bmatrix}
1 & 1 \\
0 & 1 \\
1 & 0 \\
-1 & 1
\end{bmatrix}, \quad \mathcal{F}_2 = \begin{bmatrix}
1 & 0 \\
1 & 1 \\
1 & -1 \\
0 & 1
\end{bmatrix}
$$

with respect to our hyperbolic basis of $\mathcal{E}$. Then $\mathcal{L} := \langle \mathcal{F}_1 + \mathcal{F}_2, \mathcal{F}_2 - \mathcal{F}_1 \rangle$ is nondegenerate and invariant under $\mathcal{F}_1$ and $\mathcal{F}_2$. Hence $\mathcal{B}$ is an irreducible $\mathcal{L}$-submodule of $\mathcal{E}$. Let $\mathcal{L}_1$ be the stabilizer in $\mathcal{L}$ of $\mathcal{B}$. One can check that $\mathcal{L}_1 \cap Z(\mathcal{L}) = \langle -1 \rangle$. Since $\mathcal{L}$ induces $SL(2, p) = Sp(2, p)$ on $\mathcal{E}$, we have $\mathcal{L} = \mathcal{L}C_{\mathcal{L}_1}(\mathcal{B})$. But $C_{\mathcal{L}_1}(\mathcal{B}) \leq \mathcal{L}.$
\[ \mathcal{L}_1 \cap Z(\mathcal{T}) = \langle -1 \rangle \] Thus \( C_{\mathcal{L}_1}(\mathcal{T}) = 1 \) and \( \mathcal{L}_1 = \mathcal{T} \). Hence \( |\mathcal{L} : \mathcal{L}_1| = p - 1 \). Thus \( \mathcal{T} \) belongs to an \( \mathcal{L} \)-orbit of size \( p - 1 \), and so \( \mathcal{E} \) contains \( p - 1 \) irreducible nondegenerate \( \mathcal{L} \)-submodules, as desired.

**Lemma 3.4.** Under the assumptions of Lemma 3.3, there exists \( t \in K \) such that \( tE/E = \mathcal{T} \) and \( N_K(L) = N_K(L') = \langle t \rangle \mathcal{L}Z(E) \). Moreover, \( t \) interchanges \( A \) and \( A^* \) (notation as in Lemma 3.2).

**Proof.** Suppose we can find \( t \in N_K(L) \) such that \( tE/E = \mathcal{T} \). Then Lemma 3.3 implies that \( N_K(L) = \langle t \rangle \mathcal{L}Z(E) \). Similarly \( N_K(L') = \langle t \rangle \mathcal{L}Z(E) \). If we let \( B \) and \( B^* \) be the preimages in \( E \) of the submodules \( \mathcal{A} \) and \( \mathcal{A} \) of \( E \), then \( t \) must interchange \( B \) and \( B^* \). But \( B = A \times Z(E) \) and \( A = [L, \Omega_1(\mathcal{B})] \). Similarly \( B^* = A^* \times Z(E) \) and \( A^* = [L, \Omega_1(\mathcal{B}^*)] \). Thus \( t \) interchanges \( A \) and \( A^* \).

It remains to find \( t \in N_K(L) \) such that \( tE/E = \mathcal{T} \). If \( t \) is odd, then \( K \) is a semidirect product \( SE \), with \( S \cong Sp(2n, p) \). We have \( L \leq S \) as in the proof of Lemma 3.2. We take \( t \in N_S(L) \) such that \( tE/E = \mathcal{T} \). Thus \( t \) has order 4.

Now we assume \( p = 2 \). Thus we are in Case II or Case III. If \( n \geq 6 \), choose \( s \in K \) so that \( sE/E = \mathcal{T} \). Then \( L \) and \( L^s \) are both complements to \( E \) in \( LE \). By Lemma 3.1, \( H^1(L, E) = H^1(L, \mathcal{A}) \oplus H^1(L, \mathcal{A}) \). Hence \( L \) and \( L^s \) are conjugate in \( LE/Z(E) \). Thus there exists \( u \in E \) such that \( L^suZ(E) = L(E) \). Hence \( L^su = (L^sZ(E))' \) and \( s = su \) satisfies \( tE/E = \mathcal{T} \) and \( t \in N_K(L) \).

Next suppose that \( 3 \leq n \leq 5 \). Let \( A_0 = \langle e_1, \ldots, e_6 \rangle \) and \( A_0^* = \langle f_1, \ldots, f_6 \rangle \) as in the proof of Lemma 3.2. Thus \( \langle e_i, f_i \rangle \cong D_8 \) for \( 1 \leq i \leq 6 \). Write \( V_6 = W_1 \otimes \ldots \otimes W_6 \) with \( \dim W_i = 2 \) and \( \langle e_i, f_i \rangle \leq id \otimes \ldots \otimes GL(W_i) \otimes \ldots \otimes id \). Thus \( H_i \) for \( 1 \leq i \leq 6 \). Let \( Z_i \leq Z(H_i) \) have order 4 if we are in Case II and let \( Z_i = 1 \) if we are in Case III. Let \( t = su \) as in the preceding paragraph, when \( n \) was equal to 6. We may take \( s = s_1 \ldots s_6 u \), where \( s_i \in H_i \) interchanges \( \mathcal{A} \) and interchanges \( \mathcal{A} \) and normalizes \( \langle e_i, f_i \rangle Z_i \leq H_i \), for \( 1 \leq i \leq 6 \), and \( w \in Z(GL(V_6)) \) is chosen so that \( s \in K \). Also we may take \( u = u_1 \ldots u_6 \), where \( u_i \in \langle e_i, f_i \rangle \leq H_i \), for \( 1 \leq i \leq 6 \).

Let \( V_n = W_1 \otimes \ldots \otimes W_n \) and \( V_{6-n} = W_{n+1} \otimes \ldots \otimes W_6 \). Let \( E_n = \langle e_1, \ldots, e_n, f_1, \ldots, f_n \rangle \) and \( E_{6-n} = \langle e_{n+1}, \ldots, e_6, f_{n+1}, \ldots, f_6 \rangle \). Then \( E_6 = E_n \ast E_{6-n} \), with \( E_n \leq GL(V_n) \otimes id \) and \( E_{6-n} \leq id \otimes GL(V_{6-n}) \).

It was shown in the proof of Lemma 3.2 that \( G_n \otimes id. = C_{G_6}(E_{6-n}) \), where \( G_6 = N_{GL(V_6)}(E_6) \) and \( G_n = N_{GL(V_n)}(E_n) \). We defined \( L_n \) by

\[ L_n = L_6 \cap C_{G_6}(E_{6-n}) = L_6 \cap (G_n \otimes id.) \]

Since \( t \) normalizes \( L_6 \), we have

\[ L_n = L_6 \cap C_{G_6}(E_{6-n}) = (L_6 \cap C_{G_6}(E_{6-n}))^{s_1 \ldots s_6 u_1 \ldots u_6} = L_n^{s_1 \ldots s_n u_1 \ldots u_n s_{n+1} \ldots s_6} \]

It follows that

\[ L_n^{s_1 \ldots s_n u_1 \ldots u_n} = (L_6 \cap (G_n \otimes id.))^{(s_{n+1} \ldots s_6)} = L_n \]

Hence \( s_1 \ldots s_n u_1 \ldots u_n \) normalizes \( L_n \) and maps to the desired involution of \( Sp(2n, 2) \) or \( O^+(2n, 2) \). Identifying \( GL(V_n) \) with \( GL(V_n) \otimes id. \), we may view \( s_1 \ldots s_n u_1 \ldots u_n \) as an element of \( G^+(n, 2) \), with \( \varepsilon \) equal to 0 or + respectively. There exists \( z \in Z(GL(V_n)) \) such that \( t_n = s_1 \ldots s_n u_1 \ldots u_n z \) lies in \( K^+(n, 2) \). Thus \( t_n \) normalizes \( L_n \) and maps to the desired involution in \( Sp(2n, 2) \) or \( O^+(2n, 2) \). This completes the proof.

\[ \square \]
Corollary 3.5. Under the assumptions of Lemma 3.2, let $x \in L$. Then $x$ and $x^{-1}$ are conjugate in $N_K(L)$.

Proof. This follows from Lemma 3.4, and the fact that $t$ induces the inverse transpose automorphism of $L \cong GL(n,p)$.

Lemma 3.6. With notation and assumptions as in Lemma 3.2, we have

(a) There exist nonzero vectors $w$ and $w^*$ in $V$ such that $\langle w \rangle = C_V(A) \neq C_V(A^*) = \langle w^* \rangle$.

(b) We have $N_K(A) = N_K(\langle w \rangle)$, $N_E(A) = AZ(E)$, and $N_K(A)E/E$ is the stabilizer in $K/E$ of $\overline{A}$.

(c) Similarly $N_K(A^*) = N_K(\langle w^* \rangle)$, $N_E(A^*) = A^*Z(E)$, and $N_K(A^*)E/E$ is the stabilizer in $K/E$ of $\overline{A}$.

Proof. Let $\phi$ be the Brauer character of $N_{GL(V)}(E)$ afforded by $V$, as in Section 1. Then

$$\dim C_V(A) = (\phi_A, 1_A) = (\theta_A, 1_A) = 1.$$ Of course $\dim C_V(A^*) = 1$ also. Since $\Omega_1(Z(E)) \leq \langle A, A^* \rangle$ and $\Omega_1(Z(E))$ is fixed point free on $V$, we have $C_V(A) \neq C_V(A^*)$. This proves (a).

Since $A \cap E' = 1$, we have $N_E(A) = C_E(A) = AZ(E)$. Hence $E$ acts transitively by conjugation on the $p^n$ complements to $\Omega_1(Z(E))$ in $A\Omega_1(Z(E))$. Thus $N_K(\overline{A}) = EN_K(A)$ and $N_K(A)E/E = N_K(E/\overline{A})$.

Now $N_K(A)$ stabilizes $C_V(A) = \langle w \rangle$, and so $N_K(A) \subseteq N_K(\langle w \rangle)$. Moreover $N_E(\langle w \rangle) = AZ(E)$, since otherwise $[E : N_E(\langle w \rangle)] < p^n$ and so $w$ would generate a proper $E$-submodule of $V$, contradicting irreducibility. In particular, $N_K(\langle w \rangle)$ normalizes $AZ(E)$. Hence $N_K(\langle w \rangle) \leq N_K(\overline{A}) = EN_K(A)$. Then

$$N_K(w) = N_K(A)N_E(\langle w \rangle) = N_K(A)(AZ(E)) = N_K(A).$$

This completes the proof of (b). The proof of (c) is similar.

Having defined $L$, we can finally complete our treatment of the $p = n = 2$ case.

Lemma 3.7. Suppose that $p = n = 2$ and we are in Case II. Suppose that $r$ is not a power of 3. Then $V$ contains a real vector.

Proof. Let $G = N_{GL(V)}(E)$ and let $Z = Z(GL(V))$. Let $L \cong S_3$ be the subgroup of $G$ constructed in Lemma 3.2. As in the proof of Lemma 3.3, $\overline{E}$ contains exactly three irreducible $\overline{L}$-modules, namely $\overline{A}_1 = \langle \overline{e}_1, \overline{e}_2 \rangle$, $\overline{A}_2 = \langle \overline{f}_1, \overline{f}_2 \rangle$, and $\overline{A}_3 = \langle \overline{e}_1 + \overline{f}_2, \overline{e}_2 + \overline{f}_1 \rangle$. Since $p = 2$, all three are totally isotropic. Let $B_i$ be the inverse image of $\overline{A}_i$ in $E$, for $1 \leq i \leq 3$. Then $B_i$ is abelian, and so

$$B_i = [B_i, L'] \times C_{B_i}(L') = [B_i, L'] \times Z(E).$$

For $1 \leq i \leq 3$, let $A_i = [B_i, L']$. Then $A_i$ is $L$-invariant, $A_i \cong Z_2 \times Z_2$, and $A_i \cap Z(E) = 1$.

Now $\dim C_V(A_i) = 1$ for $1 \leq i \leq 3$, as in the proof of Lemma 3.6. Let $C_V(A_i) = \langle w_i \rangle$. Since $C_V(A_i)$ is $L$-invariant, $L'$ centralizes each $w_i$. Fix an involution $u \in L$. Then each $w_i$ is an eigenvector for $u$. Let $\Omega_1(Z(E)) = \langle z \rangle$. If necessary, replace $u$ by $uz$ and $L$ by $\langle uz \rangle L'$, so that $L$ centralizes at least two of the $w_i$. We renumber the $w_i$ so that $L$ centralizes $w_1$ and $w_2$.

Let $W_0 = \langle w_1, w_2 \rangle = \langle w_1 \rangle - \langle w_2 \rangle - \langle w_3 \rangle$. Let $v$ be an arbitrary vector in $W_0$; thus $L$ centralizes $v$. We claim that $N_E(\langle v \rangle) = Z(E)$. Indeed, if this were not the
case, then \(N_E\langle v \rangle Z(E)/Z(E)\) would be an irreducible \(L\)-submodule of \(E\). Hence \(N_E\langle v \rangle Z(E)/Z(E) = A_i\) for some \(i \leq 3\). Since \(Z(E) \leq N_E\langle v \rangle\), this implies that \(N_E\langle v \rangle = B_i\). Hence \(LA_i \leq N_G\langle v \rangle\). Since \(L\) centralizes \(v\) and \([L, A_i] = A_i\), it follows that \(A_i\) centralizes \(v\), contradicting \(C_V(A_i) = \langle w_i \rangle\). This proves the claim. It follows that \(C_E(v) = 1\).

Let \(\overline{C}\) be the image of \(C_G(v)\) in \(G/EZ \cong S_6\). Then \(\overline{C} \cong C_G(v)\) and \(S_3 \cong \overline{L} \leq \overline{C}\). Now \(\overline{L}\) (and even \(\overline{L'}\)) is contained in a unique 3-Sylow normalizer \(\overline{M}\) of \(S_6\). We claim that if \(\overline{C} \not\leq \overline{M}\), then \(v\) is a real vector.

To see this, suppose first that \(\overline{C} \not\leq \overline{M}\) and \(C_G(v)\) is nonsolvable. Then \(\overline{C}\) is isomorphic to \(A_5, A_6, S_5\), or \(S_6\). Since \(C_G(v) \cong \overline{C}\), it follows that \(C_G(v)\) is a real group. Hence \(v\) is a real vector, as desired. Thus we may assume that \(\overline{C}\) is a solvable overgroup of \(\overline{L}\) in \(S_6\). From the list of maximal subgroups of \(S_6\), we see that \(\overline{C}\) is a subgroup of \(S_4 \times Z_2\), a solvable (and hence intransitive) subgroup of \(S_5\), or \(\overline{C}\) is contained in a 3-Sylow normalizer of \(S_6\). In the first two cases, the fact that \(\overline{C}\) contains \(\overline{L} \cong S_3\) implies that \(\overline{C}\) is a real group. Then \(C_G(v)\) is a real group, and \(v\) is a real vector. Since \(\overline{M}\) is the unique 3-Sylow normalizer of \(S_6\) containing \(\overline{L}\), the claim follows.

Thus we may assume that \(\overline{C} \leq \overline{M}\). If \(\overline{C}\) does not contain \(O_3(\overline{M})\), then either \(\overline{C} = \overline{L}\) or \(\overline{C} \cong \overline{L} \times Z_2\). Hence \(C_G(v)\) is a real group and \(v\) is a real vector.

Now we may assume that \(O_3(\overline{M}) \leq \overline{C} \leq \overline{M}\). Let \(T = O_3(C_G(v)) \cong Z_3 \times Z_3\), and let \(\overline{M}\) be the inverse image in \(G\) of \(\overline{M}\), isomorphic to \(G/EZ\). Let \(M = N_{\overline{M}}(TO_3(Z))\). Since \(TO_3(Z) \in Syl_3(\overline{M})\), the Frattini argument gives \(\overline{M} = EZM\). Since \(C_{\overline{M}}(O_3(M)) = C_{\overline{M}}(O_3^+(4, 2)) = 1\), we have \(M/E \leq C_E(O_3(M)) = Z(E)\) and \(M/E \leq E\).

We claim that \(M\) is the unique 3-Sylow normalizer of \(\overline{M}\) that contains \(L\). Indeed, \(L\) has no fixed points on \(\overline{E}\), this contradicts \(M \cap E = Z(E)\). Thus \(M\) and \(TO_3(Z) = O_3(M)\) do not depend on the choice of \(v \in W_0\).

We have \(M/EZ \cong D_8\) and so \(TO_3(Z) = S \times O_3(Z)\), where \(S = [M, TO_3(Z)] \cong Z_3 \times Z_3\) is normal in \(M\). Clearly \(S\) fixes \(\langle v \rangle\). Suppose now that \(3\) divides \(r - 1\). Since the two nontrivial \(M\)-orbits on \(\text{Irr}(S)\) have size \(4\), and since \(S\) doesn’t centralize \(V\), it follows from Clifford’s Theorem that \(V_S = (V_M)_S\) is the direct sum of four non-isomorphic \(M\)-conjugate one-dimensional \(S\)-modules. Hence \(S\) fixes only 4 points in \(P_1(V)\). These 4 points correspond to linearly independent subspaces of \(V\), and so at most two of them are contained in \(P_1(\langle w_1, w_2 \rangle)\). If \(3 \not| r - 1\), then \(3| r^2 - 1\), and so \(S\) fixes exactly 4 points in \(P_1(\langle GF(r^2) \otimes V \rangle)\), and \(C_{GF(r^2) \otimes V}(S) = 0\). Hence \(C_V(S) = 0\) and so \(S\) fixes no points in \(P_1(V)\).

We conclude that \(S\) fixes at most 2 points in \(P_1(\langle w_1, w_2 \rangle)\), whether or not \(3\) divides \(r - 1\). Since \(|P_1(\langle w_1, w_2 \rangle)| = r + 1 \geq 6\), it follows that we may choose \(v \in W_0\) so that \(S\) does not fix \(v\). Thus either \(\overline{C} \not\leq \overline{M}\) or \(\overline{C} \leq \overline{M}\) and \(O_3(\overline{M}) \not\leq \overline{C}\). Hence \(v\) is a real vector, as shown above. This completes the proof.

**Proposition 3.8.** Suppose we are in Case III with \(n \geq 3\) and \(r\) unrestricted or in Case IV with \(n \geq 4\) and \(r \notin \{3, 7, 11, 19\}\). Then \(V\) contains a real vector.

**Proof.** First suppose we are in Case III with \(n \geq 3\). Let \(L\) and \(A\) be as in Lemma 3.2 and let \(w\) be as in Lemma 3.6. We claim that \(w\) is a real vector. By Lemma 3.6, \(N_K\langle w \rangle = N_K\langle A \rangle\). Furthermore \(N_K(A)E/E\) is a maximal parabolic of \(K/E \cong O^+(2n, 2)\) with Levi complement \(\overline{T} \cong GL(n, 2)\), and we have \(N_E(A) = AZ(E)\). Let
$C = C_K(w)$. Since $(N_K(A)E/E)' = N_K(A)E/E$ and since $[L, A] = A$, we have $N_K(w) = N_K(w)^*Z(E)$. Since $C_G(w) \leq N_K(w)^*Z$, we have $C_G(w) = N_K(w)^* = K$. Let $C = C_G(w)$. By Corollary 1.6, $\psi_C$ is rational-valued. Hence $\chi_C$ is rational-valued, and so $w$ is a real vector by Definition 1.8.

Now suppose we are in Case IV with $n \geq 4$ and $r \notin \{3, 7, 11, 19\}$. Write $E = E_1 \oplus E_2$, where $E_1$ is extraspecial of plus type of order $2^{2n-1}$ and $E_2 \cong Q_8$. We have $E = E_1 \oplus E_2$ and $V = V_1 \otimes V_2$, where $\dim V_1 = 2^{n-1}$, $\dim V_2 = 2$, $E_1 \leq GL(V_1) \otimes id.$, and $E_2 \leq \text{id.} \otimes GL(V_2)$. Furthermore $K$ contains a central product $K_0 = K_1 \ast K_2$, where $K_1 = K_1(n-1, 2, r)$ and $K_2 = K_2(1, 2, r)$, with $K_1 \leq GL(V_1) \otimes id.$, and $K_2 \leq \text{id.} \otimes GL(V_2)$. Let $\mathcal{A}_1 \leq \mathcal{E}_1$ and $A_1 \leq E_1 \leq K_1$ be as in Lemma 3.2. Let $\langle w_1 \rangle = C_V(A_1)$, as in Lemma 3.6.

Let $\theta$ be as in Section 1. Since $(\theta_{A_1}, 1_{A_1}) = 2$, we have $dim C_V(A_1) = 2$. Since $A_1$ centralizes $w_1 \otimes V_2$, we have $C_V(A_1) = w_1 \otimes V_2$.

Now $Z(K_2) = Z(E_2) = Z(E)$ and $K_2/Z(K_2) \cong S_4$. We claim that $K_2/Z(K_2)$ has a regular orbit on $V_1(V_2)$ if $r > 19$. Indeed, it suffices to observe that at most $2(6 + 4) < r + 1$ points in $P_1(V_2)$ are fixed by some transposition or 3-cycle in $K_2/Z(K_2) \cong S_4$. Note that double transpositions in $S_4$ correspond to elements of order 4 in $O_2(K_2) \cong Q_8$; since $4 \nmid r - 1$, these elements have no fixed points in $P_1(V_2)$. Thus there exists $w_2 \in V_2$ such that $N_{K_2}(w_2) = Z(K_2)$. Let $w = w_1 \otimes w_2$.

Let $H = C_G(w)$. We claim that $H \leq N_G(A_1)$. Since $H \cap Z(E) = 1$, we must have $[A_1, 1_{A_1}] = 1$ for all $h \in H$. It follows that $\mathcal{A}_1^H$, the $H$-submodule of $\mathcal{E}$ generated by $\mathcal{A}_1$, must lie in $\mathcal{A}_1 \perp = \mathcal{A}_1 \perp E_2$. Since $E_2$ is anisotropic, it follows that $\mathcal{A}_1$ is the unique maximal totally singular subspace of $\mathcal{A}_1^H$. Hence $H$ normalizes $\mathcal{A}_1$ and so $H$ normalizes $A_1Z(E)$, the inverse image of $\mathcal{A}_1$ in $E$. Since $A_1 \leq H$ and $H \cap Z(E) = 1$, we have $A_1H \leq A_1Z(E) \cap H = A_1$ for all $h \in H$. Thus $H \leq N_G(A_1)$, as claimed.

Let $N = N_G(A_1)$, then $N \leq N_G(\mathcal{A}_1) = N_G(A_1Z(E))$. If $x \in N_G(\mathcal{A}_1)$, then $A_1^x$ is one of the $2^{n-1}$ complements to $Z(E)$ in $A_1Z(E)$. Thus $N_G(\mathcal{A}_1) = E_1N$ and so the image $\overline{N}$ of $N$ in $\overline{G} = G/ZE \cong O^-(2n, 2)$ is the maximal parabolic $\overline{N}_{\overline{G}}(\overline{A}_1)$ of $\overline{G}$. Also $N \cap EZ = (A_1 \times E_2)Z$.

Now $N$ acts on $C_V(A_1) = w_1 \otimes V_2$. Let $C < N$ be the kernel of this action. We claim that $N \leq C(K_2Z)$.

To see this, let $L_1 \leq K_1$ be as in Lemma 3.2. Then $\mathcal{L}_1 \times \mathcal{K}_2 \cong SL(n-1, 2) \times SL(2, 2)$ is a Levi complement of $\overline{N} = \overline{N}_{\overline{G}}(\overline{A}_1)$. Thus $\overline{N} = \mathcal{L}_1O_2(\mathcal{N}) \mathcal{K}_2(\mathcal{N})$. We have $\mathcal{L}_1O_2(\mathcal{N}) = O_2(\mathcal{N})$, e.g. by [GM] p. 553, and so $\overline{N} = \overline{N} = \mathcal{L}_1O_2(\mathcal{N})$. Since $n - 1 > 2$, the simple group $SL(n - 1, 2)$ has no nontrivial 2-dimensional representation over GF(r). Thus $L_1 \leq C$ and so the image $\overline{C}$ of $C$ in $\overline{G}$ contains $\mathcal{L}_1O_2(\mathcal{N})$. Since $A_1 \subseteq C$ and $N \cap EZ = (A_1 \times E_2)Z \leq A_1(K_2Z)$, we have $N \leq C(K_2Z)$, as claimed.

Thus $C \leq H \leq C(K_2Z)$. Since $N_{K_2}(w_2) = Z(E)$, the centralizer in $K_2Z$ of $w_1 \otimes w_2$ is trivial, and so $H = C$. Now

$\mathcal{T}_1O_2(\mathcal{N}) \leq \mathcal{C} \leq (\mathcal{T}_1O_2(\mathcal{N})) (\mathcal{C} \cap \mathcal{K}_2) = \mathcal{T}_1O_2(\mathcal{N})$.

Thus $\overline{C} = \mathcal{T}_1O_2(\mathcal{N})$. Since $C \cap EZ = C \cap (N \cap EZ) = C \cap (A_1 \times E_2)Z = A_1$, and $[L_1, A_1] = A_1$, it follows that $H = C = C'. \leq K'$. By Corollary 1.6, $\psi_H$ is rational-valued. Thus $\chi_H = \psi_H$ is rational-valued and so $w$ is a real vector by Definition 1.8.

**Definition 3.9.** Under the hypotheses of Lemma 3.6, let $w = \langle w, w^* \rangle$. Thus $L$ stabilizes $W$ and $L'$ centralizes $W$. Let $W_0 = W - \langle w \rangle - \langle w^* \rangle$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Remark. Our goal in Cases I and II is to show that $C_G(v) \leq N_G(L)$ for all or most $v \in W_0$. Once we have established this in Propositions 5.2 and 5.3 below, it will be easy to show that $C_G(v) \leq L \times \langle -1 \rangle$ for at least one vector $v \in W_0$; see Theorem 5.4. Then Corollary 3.5 will imply that $v$ is a real vector.

Lemma 3.10. Suppose that $n \geq 3$ or that $n = 2$ and $p > 2$. Suppose we are in Case I or Case II. Let $v \in W_0$ and let $L' \leq H \leq C_G(v)$. Then $H \cap EZ = 1$. If $p$ is odd, then $H$ centralizes the central involution of $L$. If $H$ normalizes $\overline{A}$ or $\overline{A}$, then $H \leq N_G(L)$, except possibly when $p = 2, n = 3, H = LO_2(H)$, and $O_2(H)$ is an irreducible $L$-module of cardinality 8. If $H$ interchanges $\overline{A}$ and $\overline{A}$, then $H \leq N_G(L)$.

Proof. Suppose $H \cap EZ \neq 1$. Since $H \cap Z \leq C_Z(v) = 1$, the image $(H \cap EZ)Z/Z$ of $H \cap EZ$ in $\overline{P}$ must be nonzero and totally isotropic. By Lemma 3.3, this image must be $\overline{A}$ or $\overline{A}$. Now $H$ contains $[L', H \cap EZ] = [L', (H \cap EZ)Z]$, and the latter subgroup equals $[L', A[Z]] = A$ or $[L', A^Z] = A^*$, if $A$ or $A^*$ centralizes $v$, contradicting $C_V(A) = \langle w \rangle$ or $C_V(A^*) = \langle w^* \rangle$. It follows that $H \cap EZ = H \cap Z = 1$.

If $p$ is odd, let $u$ be the central involution of $L$, and let $h \in H$. Since $L \leq K$, we have $[h, u] \in K \cap EZ = E$. Now $u \in L$ normalizes $\langle w \rangle$ and $\langle w^* \rangle$, while $t \in \langle L, w \rangle$ centralizes $u$ and interchanges $\langle w \rangle$ and $\langle w^* \rangle$. Thus $u$ acts as 1 or $-1$ on $W$ and so $u \in N_G(v)$. Thus $[h, u] \in C_G(v)$ and so $[h, u] \in C_G(v) \cap E$. By the last paragraph, $C_E(v) = 1$. Thus $H$ centralizes $u$, as desired.

Now suppose $H$ normalizes $\overline{A}$; a similar argument works if $H$ normalizes $\overline{A}$. First suppose that $H$ normalizes $A$. Now $H' \leq N_G(A)' = N_K(A)'$. By Lemma 3.6, $H'$ centralizes $w$, and so $H'$ centralizes $\langle v, w \rangle = W$. In particular, $H'$ centralizes $w^*$. By Lemma 3.6, $H'$ normalizes $A^*$. Since $H' \leq K$, we have

$$H' \leq N_K(A) \cap N_K(A^*) = L(N_E(A) \cap N_E(A^*)) = L \times Z(E).$$

Since $H' \cap EZ = 1$, $H'$ is isomorphic to a subgroup of $L \cong GL(n, p)$.

If $(n, p) \neq (2, 3)$ then $L' = L''$. Since $L' \leq H$, we have $L' = L'' \leq H''$. By the preceding paragraph, $H'' \leq L$, and so $L' = H''$. Thus $H \leq N_G(L')$. By Lemma 3.4, $H \leq N_G(L)$, as desired. If $(n, p) = (2, 3)$, then $L'' \leq H' \leq L \times Z(E)$. Since the $L''$-submodules of $\overline{E}$ coincide with $L'$-submodules of $\overline{E}$, Lemma 3.3 implies that $\overline{A}$ and $\overline{A}$ are the only two totally isotropic $H'$-submodules of $\overline{E}$. Hence $H$ permutes $\overline{A}$ and $\overline{A}$. Since $H$ normalizes $\overline{A}$, it follows that $H$ also normalizes $\overline{A}$. Since $H \cap EZ = 1$, $\overline{P}$ is isomorphic to a subgroup of $N_{G/EZ}(\overline{A}) \cap N_{G/EZ}(\overline{A}) = \overline{P}$. As $L' \leq H$ and $H \cap EZ = 1$, it follows that either $H = L'$ or $|H| = 48$ and $H \cong L \cong GL(2, 3)$. In the latter case, $H' = L'$. Thus, if $(n, p) = (2, 3)$, we have $H \leq N_G(L') = N_G(L)$.

We conclude that $H \leq N_G(L)$ whenever $H$ normalizes $A$.

Next assume that $H$ normalizes $\overline{A}$ but not $A$. Let $\overline{P}$ be the stabilizer of $\overline{A}$ in the symplectic group $G/EZ \cong K/E$. Write $\overline{P} = \overline{P} \overline{P}$, where $\overline{P} = O_p(\overline{P})$.

Since $H \cap EZ = 1$, $H$ is isomorphic to a subgroup of $\overline{P}$. Suppose now that $O_p(H) \leq N_G(A)$. Let $H_1 = L'O_p(H)$. Then $L' \leq H_1 \leq N_G(A) \cap C_G(v)$. By the preceding paragraph, $H_1 \leq N_G(L)$. Thus Lemma 3.4 implies that $H_1 \leq \langle t \rangle L$. Hence $O_p(H) = O_p(H_1) \leq H_1 \cap O_p(Z) = 1$. Thus $L' = H_1 \leq H$. Since $H$ is isomorphic to a subgroup of $\overline{P}$ and $O_p(H) = 1$, $H$ is isomorphic to a subgroup of $L$. It follows that $H' \leq L' \leq H$ and so $H \leq N_G(L') = N_G(L)$, as desired.

Thus we assume that $H$ normalizes $\overline{A}$ but not $A$, and that $O_p(H) \not\leq N_G(A)$. Since $L'$ normalizes $A, O_p(H)$ and $O_p(H) \cap N_G(A)$ are $L'$-invariant. Since $H$ normalizes $\overline{A}$,
we have $|O_p(H) : O_p(H) \cap N_G(A)| \leq p^n$, the number of complements to $\Omega_1(Z(E))$ in $A (\Omega_1(Z(E)))$.

If $p$ is odd then $\overline{U}$ is an irreducible $\overline{L}$-module of dimension $n^2 - \left(\frac{n}{2}\right)$. If $p = 2$, then $\overline{T}$ is an indecomposable module for $\overline{\mathcal{T}} = \overline{U}$ of composition length 2, with socle of dimension $n^2 - \left(\frac{n}{2}\right) - n$ and head of dimension $n$. For proofs of these statements, see e.g. [GM, Proposition 1.1.4]. Now $\log_p|O_p(H) ; O_p(H) \cap N_G(A)|$ is the dimension of an $\overline{L}$-composition factor of $\overline{U}$. Since this dimension is at most $n$ as shown above, we have $n^2 - \left(\frac{n}{2}\right) \leq n$ in Case I. Since $n \geq 2$, this can’t occur.

Suppose now that we are in Case II. If $\log_2|O_2(H)| = n^2 - \left(\frac{n}{2}\right) - n$, then $O_2(H) \cap N_G(A) = 1$ and we must have $n = 3$, $|O_2(H)| = 8$, and $H = LO_2(H)$ as in the statement of Lemma 3.10. We can’t have $\log_2|O_2(H)| = n^2 - \left(\frac{n}{2}\right)$ and $O_2(H) \cap N_G(A) = 1$, since that would imply that $n^2 - \left(\frac{n}{2}\right) \leq n$, which is false. The remaining possibility is that $\log_2|O_2(H)| = n^2 - \left(\frac{n}{2}\right)$ and $O_2(H) \cap N_G(A) = n^2 - \left(\frac{n}{2}\right) - n$. If this occurs, let $H_1 = L(O_2(H) \cap N_G(A))$. Then $L = L' \leq H_1 \leq C_G(v)$ and $H_1 \leq N_G(A)$. As above, this implies that $H_1 \leq \langle t \rangle \subset L$ and so $O_2(H_1) \leq H_1 \cap Z = 1$, a contradiction.

This completes the proof of Lemma 3.10 in the case that $H$ normalizes $\overline{A}$. Entirely similar arguments work when $H$ normalizes $\overline{A}$.

Finally, suppose $H$ permutes $\overline{A}$ and $\overline{\mathcal{T}}$ nontrivially. Let $H_0 = H \cap N_G(\overline{A}) \cap N_G(\overline{\mathcal{T}})$. Then $|H : H_0| = 2$. Since $L' \leq H_0 \leq C_G(v)$, the arguments above show that $H_0 \leq N_G(L)$, except possibly when $p = 2$ and $n = 3$. When $p = 2$ and $n = 3$, however, we can’t have $H_0 = L(O_2(H_0))$ with $|O_2(H_0)| = 8$, because $H_0 \cap Z = 1$ and the image in $G/EZ$ of $N_G(\overline{A}) \cap N_G(\overline{\mathcal{T}})$ is $\overline{U}$. Thus $H_0 \leq N_G(L)$ even when $p = 2$ and $n = 3$.

By Lemma 3.4, $N_G(L) = \langle t \rangle \subset L$, and so $H_0 \leq L$. Since $L' \leq H_0$, we have $L'' \leq H_0' \leq L'$. If $(n, p) \neq (2, 3)$, then $L' = L''$ and so $L'$ char $H_0$, which yields $H \leq N_G(L') = N_G(L)$, as desired. Even if $(n, p) = (2, 3)$, $H_0$ is isomorphic to its image in $G/EZ$, and the containments $\overline{P_0} \leq \overline{P}$ and $\overline{P} \leq H_0'$ imply that $L' = O^3(H_0)$. Again $L'$ char $H_0$ and $H \leq N_G(L') = N_G(L)$, as desired.

4. OVERGROUPS OF $L'$

Let $L' \leq H \leq C_G(v)$ as in the statement of Lemma 3.10. Our goal, as we remarked after Definition 3.9, is to show that $H \leq N_G(L)$ in most circumstances. Let $\overline{P}$ be the image of $H$ in the symplectic group $G := G/EZ \cong K/E$. In this section we use the classification of finite simple groups to show that $\overline{L}$ has few overgroups in $\overline{P}$, and therefore $\overline{P} \leq N_G(\overline{L})$ and $H \leq N_G(L)$, apart from some easily understood exceptional cases.

**Lemma 4.0.** Let $q$ be a prime. Let $Q \neq 1$ be a $q$-group with every characteristic abelian subgroup cyclic. Let $Y \leq Z(Q)$ with $|Y| = q$. Then there exist $D, T \leq Q$ such that:

(i) $Q = DT$, $D \cap T = Y$, and $T = C_Q(D)$.

(ii) $D$ is extraspecial or $D = Y$.

(iii) $\exp(D) = q$ or $q = 2$.

(iv) $T$ is cyclic or $q = 2$ and $T$ is dihedral, semidihedral, or quaternion of order at least 16.

(v) There exists $U$ char $Q$ such that $U \leq T$, $|T : U| \leq 2$, $U = C_T(U)$, and $U$ is cyclic.
(vi) $DU = C_Q(U)$ is characteristic in $Q$.

Proof. This is [MW] Theorem I.1.2. \hfill $\Box$

Proposition 4.1. Suppose that $n \geq 3$ and we are in Case I. Let $W_0$ be as in Definition 3.9. Let $v \in W_0$ and let $L' \leq H \leq C_G(v)$. Let $G$ be the symplectic group $G/EZ$ and let $\Pi$ be the image of $H$ in $\bar{G}$. Then $H \cong \Pi$ and $H \leq N_G(L)$.

Proof. By Lemma 3.10, $H \cap EZ = 1$ and so $H \cong \bar{H}$. Suppose $H \not\leq N_G(L)$. Since $\bar{A}$ and $\bar{A}'$ are the unique nonzero proper $\bar{L}'$-submodules of $\bar{E}$, Lemma 3.10 implies that $\Pi \not\leq N_{\bar{G}}(\bar{L})$ and that $\Pi$ acts irreducibly on $\bar{E}$. We claim that $\Pi$ acts primitively on $\bar{E}$. To see this, suppose that $\bar{E} = \bar{E}_1 \oplus \ldots \oplus \bar{E}_k$ is an imprimitivity decomposition for $\bar{H}$. We claim that $\bar{L}$ has exactly $p + 2$ orbits on the nonzero vectors of $\bar{E}$. Two of these orbits are $\bar{A} - \{0\}$ and $\bar{A}' - \{0\}$. Let $\Omega = \bar{E} - \bar{A} - \bar{A}'$. Then $\Omega$ is the direct product, as $\bar{L}$-sets, of $\bar{A} - \{0\}$ and $\bar{A}' - \{0\}$. Let $\pi$ be the permutation character of $\bar{L}$ on $\bar{A} - \{0\}$. Then the permutation character of $\bar{L}$ on $\bar{A}' - \{0\}$ is $\pi^\alpha$, where $\alpha$ is the inverse transpose automorphism of $\bar{L}$. Since $g^{-1}$ is conjugate to $g^\alpha$ for all $g \in \bar{L}$, we have $\pi^\alpha = \pi$. Hence the number of orbits of $\bar{L}$ on $\Omega$ is the inner product $(\pi \pi^\alpha, 1) = (\pi^2, 1)$. The last inner product equals $(\pi, \pi)$, the rank of the transitive permutation group $\bar{L}$ on $\bar{A} - \{0\}$. Matrix computation shows that the stabilizer in $\bar{L}'$ of $[100 \cdots 0]^T$ has $p$ orbits on $\bar{A} - \{0\}$. Indeed, each of the $p - 1$ scalar multiples of $[100 \cdots 0]^T$ constitutes an orbit of size one, and the remaining vectors in $\bar{A} - \{0\}$ form a single $\bar{L}'$-orbit. This proves the claim. It follows that $k \leq p + 2$, since any two elements of $\bar{E} = \bar{E}_1 \oplus \ldots \oplus \bar{E}_k$ that lie in the same $\bar{L}$-orbit have the same number of nonzero components. By [C], however, the minimal degree of a nontrivial permutation representation of $\bar{L}' \cong SL(n, p)$ is $(p^n - 1)/(p - 1)$. Since $k \leq p + 2 < (p^n - 1)/(p - 1)$, it follows that $\bar{L}$ acts trivially on $\{\bar{E}_1, \ldots, \bar{E}_k\}$. Since $\bar{A}$ and $\bar{A}'$ are the unique nonzero proper $\bar{L}'$-submodules of $\bar{E}$, it follows that $k = 2$ and $\{\bar{E}_1, \bar{E}_2\} = \{\bar{A}, \bar{A}'\}$. Hence $\bar{H}$ permutes $\bar{A}$ and $\bar{A}'$. By Lemma 3.10, $H \leq N_G(L)$, a contradiction.

We next show that $F(\Pi) = Z(F^*(\Pi))$. To see this, suppose that $\bar{Q}$ is a nonabelian Sylow subgroup of $F(\Pi)$. Since $\Pi$ is primitive on $\bar{E}$, every characteristic abelian subgroup of $\bar{Q}$ is cyclic. We use the notation of Lemma 4.0. Thus $\bar{Q} = \bar{D} \bar{T}$. If $\bar{D} = \bar{Y}$ and $\bar{Q} = \bar{T}$, then $\bar{L}$ would centralize $\bar{T}$ contradicting End$_{\bar{L}}(\bar{E}) \cong GF(p) \oplus GF(p)$. Hence $\bar{D}$ is extraspecial. Now $\bar{L}$ acts nontrivially on $\bar{D}/\bar{U} \cong \bar{D}/Z(\bar{D})$. Let $|\bar{D}/Z(\bar{D})| = q^{2a}$ for a prime $q$ and $a \geq 1$. Since $\bar{L}$ acts faithfully on $\bar{E}$, we have $q^a \leq \dim \bar{E} = 2n$. Since $H$ is irreducible on $\bar{E}$, we know that $q \neq p$. On the other hand, $2a$ is equal to or greater that the degree of a nontrivial irreducible cross-characteristic representation of $\bar{L} \cong SL(n, p)$. By [LS], $p^{n-1} - 1 \leq 2a$. Since $p$ is odd, we have $3^{a-1} \leq 2a + 1 \leq 2 \log_2(2n) + 1$, contradicting $n \geq 3$. Thus $F(\Pi)$ is abelian and so $F(\Pi) = Z(F^*(\Pi))$. Moreover $F(\Pi)$ is cyclic, since $\Pi$ is primitive on $\bar{E}$.

Since End$_{\bar{L}}(\bar{E}) \cong GF(p) \oplus GF(p)$, it follows that $\bar{L}$ centralizes no component of $\Pi$. Suppose that $\{S_1, \ldots, S_k\}$ is an $\bar{L}'$-orbit of components of $\bar{H}$, with $k > 1$. Since $(p^n - 1)/(p - 1)$ is the minimal degree of a nontrivial permutation representation of $\bar{L}'$, by [C], we have $k \geq (p^n - 1)/(p - 1)$. For some integer $m \geq k$, there exists components $S_{k+1}, \ldots, S_m$ of $\Pi$ such that $N := S_1 \ldots S_m$ is a normal subgroup of $\Pi$. By
Clifford’s Theorem, $E_{N}$ is completely reducible. Let $X$ be an irreducible summand of $E_{N}$. Since $E$ is a primitive $H$-module, $X$ is a faithful $N$-module. Now $X$ may be viewed as an irreducible module for $S_{1} \times \ldots \times S_{m}$, on which no $S_{i}$ acts trivially. It follows from [AS 27.15] that $\dim X \geq 2^{m} \geq 2^{k} \geq 2^{(p^{n}-1)/(p-1)} > 2n = \dim E$, a contradiction.

Hence $\mathcal{L}$ normalizes every component of $H$ and centralizes no component of $H$. If $S$ is a component of $H$, then $\mathcal{L}$ induces inner automorphisms of $S$ and so $\mathcal{L}/C_{\mathcal{L}}(S)$ is isomorphic to a subgroup of $Inn(S)$. Thus $S/Z(S)$ and $S$ contain central extensions of $PSL(n, p)$. Zsigmondy’s Theorem implies that $|S/Z(S)|$ does not divide $|GL(k, p)|$ for any $k < n$. It follows that every nontrivial irreducible $GF(p)[S]$-module has dimension at least $n$. Let $\mathcal{M} \subset \mathcal{H}$ be the product of all components of $\mathcal{H}$. Let $\mathcal{Y}$ be an irreducible summand of $E_{\mathcal{M}}$. Since $H$ acts primitively on $E$, Clifford’s Theorem implies that $\mathcal{Y}$ is a faithful $\mathcal{M}$-module. Arguing as in the preceding paragraph, we see that, since $n^{2} > 2n$, $H$ has only one component.

Let $S$ be the unique component of $\mathcal{H}$. Since $\mathcal{L}$ induces inner automorphisms of $S$, we have $\mathcal{L} \leq S/C_{\mathcal{L}}(S)$. Since $\mathcal{L}$ also centralizes $Z(F^{*}(H))$, we have $\mathcal{L} \leq S/C_{\mathcal{L}}(F^{*}(H)) = S/F^{*}(H) = F^{*}(H)$. It follows that $\mathcal{L} \leq S$ and $S$ is normal in $\mathcal{H}$. Since we are assuming that $H \not\leq N_{\mathcal{H}}(\mathcal{L}) = N_{\mathcal{L}}(\mathcal{L})$, it follows that $S > \mathcal{L}$, $S$ acts irreducibly on $E$, and $End_{\mathcal{H}}(E) \cong GF(p)$. Moreover $Z(F^{*}(H)) \leq End_{\mathcal{H}}(E)$. Thus $Z(F^{*}(H)) \subseteq Z(G)$. Finally $F^{*}(H) = S/Z(H)$ and so $H/Z(H) \leq Aut(S)$.

Suppose $S/Z(S)$ is an alternating group $A_{m}$. Since $n \geq 3$ and $p$ odd, the inclusion $L \leq S$ implies that $m \geq 13$; this follows because $(p^{n}-1)/(p-1)$ is the minimal degree of a nontrivial permutation representation of $PSL(n, p)$, by [C]. If $S \cong A_{m}$, then the minimal degree of a nontrivial representation of $S$ in characteristic $p$ is at least $m - 2$; see [J]. If $S \cong S_{m}$, then, by [W], the minimal degree of a nontrivial representation of $S$ in characteristic $p$ is at least $2^{(m-s-1)/2}$, where $s$ is the number of ones in the binary expansion of $m$. Since $m \geq 13$, the minimal degree of $S$ is at least $m - 2$, whether $S \cong A_{m}$ or $S \cong \tilde{A}_{m}$. Thus $m - 2 \leq 2n$.

On the other hand, the inclusion of a central extension of $PSL(n, p)$ in $A_{m}$ implies that $PSL(n, p)$ has a nontrivial permutation representation of degree at most $m$. Thus $(p^{n}-1)/(p-1) \leq m \leq 2n+2$. Since $p \geq 3$, we have $3^{n}-1 \leq 2(2n+2)$, which is false for $n \geq 3$. Thus $S/Z(S)$ can’t be an alternating group.

Suppose next that $S/Z(S)$ is a sporadic simple group. Now $|L|$ divides $|S|$ and $|S|$ divides $|Sp(2n, p)|$. If $S/Z(S)$ is not the Monster group, then these two divisibility relations easily eliminate $S$ as a possible overgroup of $L$. Indeed we first note that the $p$-part of $|SL(n, p)|$ must divide $|S/Z(S)|$; this severely limits the possibilities for $n$ and $p$. If $S/Z(S)$ is the Monster group, then $Z(S)$ is trivial. By Lemma 3.10, $H \cap EZ = 1$, so that $H' \cong S$. Lemma 3.10 also implies that $H$ centralizes the central involution of $n$ of $L$, so that $H' \leq C_{G}(u) \cong Sp(2n, p)$. Hence $\psi_{H'}$ has an irreducible constituent of degree at most $(p^{n}-1)/2$, by Lemma 1.2. Thus $(p^{n}-1)/2 \geq 196, 883$. If $p = 3$, this implies that $n \geq 12$, and so the 3-part of $|SL(12, 3)|$ divides the order of the Monster, which is false. If $p = 5$, we obtain $n \geq 9$, which leads to a similar contradiction. If $p$ is any other odd prime divisor of the order of the Monster we also obtain a similar contradiction. Thus $S/Z(S)$ can’t be a sporadic group.
Next suppose \( \overline{S}/Z(\overline{S}) \) is a group of Lie type in characteristic \( q \) with \( q \neq p \). Let \( \ell \) be the untwisted rank of \( \overline{S}/Z(\overline{S}) \). Since \( \overline{S}/Z(\overline{S}) \) has a nontrivial cross-characteristic projective representation of degree at most \( 2n \), \cite{LS} implies that 

\[
(q^\ell - 1)/2 \leq 2n; \text{ note that the Suzuki groups and the exceptions in } \cite{LS} \text{ p.419 can't have order divisible by } |SL(n,p)|.
\]

Let \( \hat{S} \) be the universal covering group of \( \overline{S}/Z(\overline{S}) \). Thus \( \hat{S} \) is also the universal covering group of \( \overline{S} \). If \( \overline{S}/Z(\overline{S}) \) is not of type \( E_8, E_7, F_4, \) or \( \tilde{F}_4 \), then \( \hat{S} \) has a nontrivial irreducible representation in characteristic \( q \) of degree at most \( 5\ell \). Since \( \hat{S} \) contains a central extension of \( PSL(n,p) \), it follows that \( PSL(n,p) \) has a nontrivial projective representation in characteristic \( q \) of degree at most \( 5\ell \). See \cite{A} p. xvi. From \cite{LS}, we deduce that \( p^{n-1} - 1 \leq 5\ell \). Our previous inequality \((q^\ell - 1)/2 \leq 2n\) yields \( \ell \leq \log_2(4n + 1) \). Hence \( p^{n-1} - 1 \leq 5 \log_2(4n + 1) \). If \( p \geq 5 \) and \( n \geq 3 \) or if \( p = 3 \) and \( n \geq 4 \), then this inequality does not hold. If \( p = n = 3 \), one can check in \cite{A} that no cross-characteristic overgroup exists.

It remains to consider the possibility that \( \overline{S}/Z(\overline{S}) \) is of type \( E_8, E_7, F_4, \) or \( \tilde{F}_4 \). Suppose first that \( \overline{S}/Z(\overline{S}) \) is of type \( E_8 \). Then \( \ell = 8 \) and the inequalities \((q^\ell - 1)/2 \leq 2n\) and \( (p^n - 1)/2 \leq 248 \) lead to \( 256 \leq 4n + 1 \) and \( 3n^2 - 1 \leq 249 \), which are contradictory. Similar easy arguments work in the remaining three cases.

Finally suppose that \( \overline{S}/Z(\overline{S}) \) is a group of Lie type in characteristic \( p \). If \( \overline{S} \cong Sp(2n,p) \), then we have \( H' \cong \overline{S} \) as in the Monster case above. Thus \( H' = C_K(u) \cong Sp(2n,p) \). By Lemma 1.2, \( \psi_{H'} \) is the Weil character of \( Sp(2n,p) \), and \( \psi_{H'} \) has two irreducible constituents, of degrees \( (p^n - 1)/2 \) and \( (p^n + 1)/2 \), which remain irreducible in characteristic \( r \). (We abuse notation by writing “characteristic \( r \)” and “\( r \)-regular” even if \( r \) is not a prime.) With notation as in the proof of Lemma 1.7, we have \( C(E) = C(E)' \) and so \( \rho = \sigma \). Hence \( \phi \) is the restriction of \( \chi \) to the \( r \)-regular elements of \( G \). Since \( \chi_K = \psi \) by Lemma 1.7, it follows that \( \phi_K = \psi \) is the restriction of \( \psi \) to the \( r \)-regular elements of \( K \). Thus \( \phi_K = \psi \) is the sum of two nonlinear irreducible Brauer characters, contradicting our assumption that \( H \leq C_G(v) \).

Even if \( \overline{S} \cong Sp(2n,p) \), \( H \) has a normal subgroup \( H_0 \) such that \( H_0 \leq C_K(u)' \) and \( H_0 \cong \overline{S} \). Now \( \psi_{H_0} \) has a nontrivial irreducible constituent \( \alpha \) with \( \alpha(1) \leq (p^n - 1)/2 \). Let \( \ell \) be the untwisted rank of \( \overline{S}/Z(\overline{S}) \). If \( \ell \geq n \), then \cite{LS} p. 419 implies that \( \alpha(1) \geq (p^n - 1)/2 \), with equality if and only if \( \overline{S}/Z(\overline{S}) \cong PSp(2n,p) \); the \( PSU(4,3) \) exception on \cite{LS} p.419 can't arise in our situation. Since we have already eliminated the possibility that \( \overline{S} \cong Sp(2n,p) \), we conclude that \( \ell < n \).

As shown above, \( \overline{S} \) acts irreducibly on \( \overline{E} \). From \cite{Gr2} p. 280, we see that \( \overline{S} \) must be a homomorphic image of a universal group of Lie type; the containment \( SL(4,3) < 2.O_7(3) < Sp(8,3) \) is not excluded by divisibility considerations, but the minimal faithful character degree of \( 2.O_7(3) \) is 520, which is greater that \( \psi(1) = 81 \).

Suppose that \( \overline{S} \) is defined over \( GF(p^n) \), for \( a \geq 1 \). We claim that \( \overline{L} \) preserves no tensor product decomposition of \( \overline{E} \). Indeed, if this were not the case, then \( \overline{L} \) would embed into the central product of \( GL(d,p) \) and \( GL(2n/d,p) \) for a divisor \( d \) of \( 2n \). We may assume that \( 1 < d < 2n/d < 2n \). Since \( d < n \), \( \overline{L} \) would embed into \( id \otimes GL(2n/d,p) \). Hence \( d = 2 \) and \( \overline{E} \) is the direct sum of two isomorphic \( \overline{L} \)-modules, contradicting Lemma 3.3. This proves the claim. It now follows from the Steinberg Tensor Product Theorem (see \cite{KL} 5.4.6) that \( \overline{E} \) is a \( GF(p^n)[\overline{S}] \)-module which is realized over no proper subfield of \( GF(p^n) \). Since \( End_L(\overline{E}) = GF(p) \oplus GF(p) \), it follows that \( a = 1 \). Thus \( \overline{S} \) is defined over \( GF(p) \).
Now suppose that $\mathcal{S}$ is an exceptional group of Lie type, necessarily defined over $GF(p)$. Define $n(\mathcal{S})$ to be 11, 11, 7, 7, 5, or 4 for $\mathcal{S}$ of type $E_8$, $E_7$, $E_6$, $2E_6$, $F_4$, $3D_4$, or $G_2$, respectively. The order formulas show that a Zsigmondy prime divisor of $p^{n(\mathcal{S})} - 1$ does not divide $|\mathcal{S}|$. Hence $|SL(n, p)|$ does not divide $|\mathcal{S}|$ if $n \geq n(\mathcal{S})$. It follows that $n < n(\mathcal{S})$. Since $H$ has a normal subgroup $H_0 \cong \mathcal{S}$ as above, we can consider the restriction of $\psi$ to $H_0$ and conclude that $\mathcal{S}$ has a nontrivial irreducible character of degree at most $(p^{n(\mathcal{S})} - 1)/2$. In each of the seven cases, this quantity is less than the minimal degree of a cross-characteristic projective representation of $\mathcal{S}/Z(\mathcal{S})$, by [LS] or [SZ]. This contradiction shows that $\mathcal{S}/Z(\mathcal{S})$ can’t be an exceptional group.

Thus $\mathcal{S}$ is a classical group defined over $GF(p)$, and $E$ is an absolutely irreducible $GF(p)[\mathcal{S}]$-module of dimension $2n$. Moreover $\ell$, the untwisted rank of $\mathcal{S}$, is less than $n$. Following [KL], we define $d$ to be the dimension of the natural (projective) $GF(p)[\mathcal{S}/Z(\mathcal{S})]$-module (the $GF(p^2)[\mathcal{S}/Z(\mathcal{S})]$-module in the unitary case). Thus $d = \ell + 1$ if $\mathcal{S}$ is of type $A_\ell$ or $2A_\ell$; $d = 2\ell + 1$ if $\mathcal{S}$ is of type $B_\ell$, and $d = 2\ell$ in the remaining orthogonal and symplectic cases. Since $\mathcal{S}/Z(\mathcal{S})$ contains $PSL(n, p)$ as a non-normal subgroup, we have $d > n$.

The inequalities $\ell < n$ and $d = \ell + 1 > n$ show that $\mathcal{S}$ is not of type $A_\ell$. If $\mathcal{S}$ is of type $2A_\ell$, then we must have $\ell = n - 1$, since $|SL(n, p)| > |SU(n - 1, p)|$. Let $s$ be a Zsigmondy prime divisor of $p^n - 1$ if $n$ is odd; if $n$ is even let $s$ be a Zsigmondy prime divisor of $p^{n-1} - 1$. Then the order formulas show that $s$ doesn’t divide $|SU(n, p)|$. Hence $|E|$ doesn’t divide $|\mathcal{S}|$, a contradiction.

Thus $\mathcal{S}/Z(\mathcal{S})$ is a simple orthogonal or symplectic group defined over $GF(p)$. We may assume that $\mathcal{S}$ is not of type $D_2$ or $2D_2$. Since $|SL(3, p)|$ doesn’t divide $|PSp(4, p)|$, it follows that $\mathcal{S}$ is not of type $B_2 = C_2$. Hence $\ell \geq 3$ and so $d \geq 6$. Also $n \geq \ell + 1 \geq 4$. In particular, $2n \leq \left(\frac{(n + 1)^2}{2}\right) - 1 \leq \left(\frac{d^2}{2}\right) - 1$.

In [KL] 5.4.11, all absolutely irreducible $GF(p)[\mathcal{S}]$-modules of dimension less than or equal to $(d^2/2) - 1$ are determined. These modules belong to three categories. First, there are possible $GF(p)[\mathcal{S}]$-modules of dimension $d$, which are closely related to the natural module for the appropriate covering group of $\mathcal{S}/Z(\mathcal{S})$. If these occur, then

$$\dim E = 2n = d \leq 2\ell + 1 \leq 2(n - 1) + 1 = 2n - 1,$$

a contradiction.

Second, there are modules related to alternating and symmetric powers of the natural module. Such modules have dimension of least $d(d - 1)/2 - 2$. Hence they can’t arise in our situation; since $d \geq 6$, we have $\dim E = 2n < 2d < d(d - 1)/2 - 2$.

Third, spin modules of small dimension exist when $\mathcal{S}/Z(\mathcal{S})$ is a simple orthogonal group. If $\mathcal{S}$ is of type $2D_\ell$, these spin representations cannot be realized over a proper subfield of $GF(p^2)$; see [KL] 5.4.9. Hence we may assume $\mathcal{S}$ is of type $B_\ell$ or $D_\ell$. Since $p$ is odd and $\mathcal{S}$ is absolutely irreducible on $E$, $\mathcal{S}$ can’t preserve both a symplectic and a symmetric bilinear form on $E$. Hence we need only consider those spin representations which embed a spin group of type $B_\ell$ or $D_\ell$ into $Sp(2n, p)$, rather than into $\Omega^+(2n, p)$. Now [KL] 5.4.9 tells us that if $\mathcal{S}$ is of type $B_\ell$, then $\ell \equiv 1$ (mod 4) or $\ell \equiv 2$ (mod 4), and the spin module has dimension $2\ell$. If $\mathcal{S}$ is of type $D_\ell$, then $\ell \equiv 2$ (mod 4), and the spin module has dimension $2\ell - 1$. Since $\ell \geq 3$, it follows that $\ell$ is at least 5 in the $B_\ell$ case and at least 6 in the $D_\ell$ case. Thus
in the $B_\ell$ case we have $\dim \overline{E} = 2n = 2^\ell$, and so $n = 2^{\ell-1}$. Since $d = 2\ell + 1$ and $\ell \geq 5$, this contradicts $d > n$. Similarly, in the $D_\ell$ case, we have $n = 2^{\ell-2}$, $d = 2\ell$, and $\ell \geq 6$, again contradicting $d > n$.

We conclude that $\mathcal{S}$ is not a group of Lie type in characteristic $p$. Thus our assumption that $H \not\leq N_G(L)$ has led to a contradiction, as desired.

Next we establish the analog of Proposition 4.1 for $n = 2$ and $p$ odd. We recall from the proof of Lemma 3.3 that $\overline{E}$ contains exactly $p + 1$ irreducible $\overline{E}$-submodules. Two of these, namely $(\tau_1, \tau_2)$ and $(\overline{J}_1, \overline{J}_2)$, are totally isotropic. In addition, there are $(p - 1)/2$ pairs of mutually orthogonal nondegenerate irreducible $\overline{E}$-submodules; one such pair is $(\tau_1 + \overline{J}_2, \tau_2 - \overline{J}_1)$ and $(\tau_2 + \overline{J}_1, \overline{J}_2 - \tau_1)$. Now $\overline{G} = G/EZ \cong Sp(4, p)$ contains a subgroup $M \cong SL(2, p) \wr Z_2$ which permutes the two nondegenerate subspaces above. Clearly $\overline{E}$ is contained in exactly $(p - 1)/2$ distinct $\overline{G}$-conjugates of $\overline{M}$. The proof of Lemma 3.3 shows that all these $(p - 1)/2$ $\overline{G}$-conjugates of $\overline{M}$ are conjugate under $\overline{L}$.

Now let $v \in W_0$ (Definition 3.9). Suppose that $L' \leq H \leq C_G(v)$. Let $u$ be the central involution of $L \cong GL(2, p)$. Then $C_G(u) = C_G(u)^\prime Z$, where $C_G(u)^\prime \cong Sp(4, p)$ is a complement to $E$ in $K$, and thus a complement to $EZ$ in $G$. By Lemma 3.10, we have $H \leq C_G(u)$. Let $M \leq C_G(u)^\prime$ be the inverse image of $\overline{M} \leq \overline{G}$. Then $L' \leq M \cong \overline{M}$ and $L'$ is contained in exactly $(p - 1)/2 C_G(u)$-conjugates of $M$, which form a single orbit under the action of $L$.

We will show that, with few exceptions, either $H \leq N_G(L)$ or $H$ is contained in an $L$-conjugate of $MZ$. The maximal subgroups of $PSp(4, q)$, $q$ odd, were determined by Mitchell [M]. We summarize his results in the next lemma.

**Lemma 4.2.** Let $p$ be an odd prime. Then $PSp(4, p)$ contains seven families of non-parabolic maximal subgroups. For each family, the order and number of conjugacy classes are listed below.

<table>
<thead>
<tr>
<th>Order</th>
<th>Number of Classes</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p^2(p^2 - 1)^2$</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>$p^2(p^4 - 1)$</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>$p(p^2 - 1)(p - 1)$</td>
<td>1</td>
<td>$p &gt; 3$</td>
</tr>
<tr>
<td>$p(p^2 - 1)(p + 1)$</td>
<td>1</td>
<td>$p &gt; 3$</td>
</tr>
<tr>
<td>$p(p^2 - 1)/2$</td>
<td>1</td>
<td>$p &gt; 7$</td>
</tr>
<tr>
<td>$1920$</td>
<td>2</td>
<td>$p \equiv \pm 1 (\text{mod } 8)$</td>
</tr>
<tr>
<td>$960$</td>
<td>1</td>
<td>$p \equiv \pm 3 (\text{mod } 8)$</td>
</tr>
<tr>
<td>$360$</td>
<td>1</td>
<td>$p \equiv \pm 5 (\text{mod } 12)$, $p \neq 7$</td>
</tr>
<tr>
<td>$2520$</td>
<td>1</td>
<td>$p = 7$</td>
</tr>
</tbody>
</table>

**Proof.** This is Mitchell’s main theorem, specialized to the case $q = p$. Not listed here are the two families of maximal (rank 1) parabolic subgroups. If $q$ is a power of $p$ and $q > p$, then $PSp(4, q)$ contains two families of subfield groups.

With the help of this result and the Atlas, we now prove Proposition 4.3. We note the isomorphism of $PSp(4, p)$ and the orthogonal group $\Omega_6(p)$. Let $V_5(p)$ be the natural module for $\Omega_5(p)$.

**Proposition 4.3.** Suppose that $n = 2$ and $p$ is odd. Let $W_0$ be as in Definition 3.9. Let $M$ be as in the remarks preceding Lemma 4.2. Let $v \in W_0$ and let $L'$ ≤
$H \leq C_G(v)$. Let $\overline{G} = G/EZ \cong Sp(4,p)$ and let $\overline{H}$ be the image of $H$ in $\overline{G}$. Then $H \cong \overline{H}$ and either $H \leq N_G(L)$, $H$ is contained in one of the $(p - 1)/2$ distinct $L$-conjugates of $MZ$, or one of the following holds:

(a) $\overline{H} \cong SL(2,p^2)$, $|\overline{H} : \overline{H}| \leq 2$, and $\overline{H}$ preserves a $GF(p^2)$-vector space structure on $\overline{E}$.

(b) $p = 5$ and $\overline{H} \cong \hat{A}_6 \cong SL(2,9)$.

(c) $p = 5$ and $\overline{H}/Z(\overline{G})$ is a split extension of $A_5$ by an elementary abelian group of order 16.

(d) $p = 7$ and $\overline{H} \cong \hat{A}_7$.

(e) $p = 3$ and $\overline{H}$ is isomorphic to a subgroup of $\hat{S}_6$.

Proof. First note that the image of $\overline{M}$ in $PSp(4,p)$ has order $p^2(p^2 - 1)^2$, which does not divide the order of any of the maximal subgroups in classes (2) – (7) of Lemma 4.2. Since $\overline{M}$ has two components, $\overline{M}$ is not contained in any proper parabolic subgroup of $PSp(4,p)$. Hence $\overline{M}$ is a maximal subgroup of $Sp(4,p)$, corresponding to class (1) of Lemma 4.2. Under the isomorphism of $PSp(4,p)$ and $\Omega(5,p)$, $\overline{M}$ corresponds to $O^+(4, p)$, the stabilizer of a certain one-dimensional subspace of $V_5(p)$. If $\overline{H}$ is contained in a $G$-conjugate of $\overline{M}$, then the discussion preceding Lemma 4.2 shows that $H \leq C_G(u)$ and $\overline{H}$ is contained in one of the $(p - 1)/2$ distinct $L$-conjugates of $\overline{M}$. It follows that, for some $x \in L$, $H$ is contained in $M^*EZ \cap C_G(u) = M^*Z$. Thus $H$ is contained in one of the $(p - 1)/2$ distinct $L$-conjugates of $MZ$; moreover $H \cap Z = 1$.

Just as in the twelfth paragraph of the proof of Proposition 4.1, we cannot have $\overline{H} = \overline{G}$. Thus $\overline{H}$ is contained in a maximal subgroup $\overline{X}$ of $Sp(4,p)$. By Lemma 3.10, we may assume that $\overline{H}$ stabilizes neither $\overline{A}$ nor $\overline{A}'$. Since $\overline{A}$ and $\overline{A}'$ are the only totally isotropic subspaces of $\overline{E}$ stabilized by $\overline{L}$, we see that $\overline{X}$ is not a parabolic subgroup of $\overline{G}$.

First consider the possibility that $\overline{X}/Z(\overline{G})$ belongs to class (2) of Lemma 4.2. Then $|\overline{X}/Z(\overline{G})| = 2$ and, up to conjugacy in $Sp(4,p)$, $\overline{X}$ is the natural $Sp(2,p^2)$ contained in $Sp(4,p)$. Under the isomorphism of $PSp(4,p)$ and $\Omega(5,p)$, $\overline{X}/Z(\overline{G}) = O^+(4,p)$, the stabilizer of a certain one-dimensional subspace of $V_5(p)$. If $p = 3$, then conclusion (e) holds, so we assume that $p > 3$. From the list of subgroups of $PSL(2,p^2)$ in [Hu] p. 213, we see that if $\overline{L} \leq \overline{H} \leq \overline{X}$, then either $\overline{X} \leq \overline{H}$ or $\overline{L} = (\overline{H} \cap \overline{X})'$. The former possibility yields conclusion (a). The latter possibility implies that $\overline{H} \leq N_{\overline{G}}(\overline{L}) = N_{\overline{G}}(\overline{T})$. By Lemma 3.3, $H$ fixes or permutes $\overline{A}$ and $\overline{A}'$. By Lemma 3.10, $H \leq N_G(L)$.

For $p = 5$, the Atlas tells us that the maximal subgroups in classes (3) and (4) are stabilizers of decompositions $V_5(p) = V_2(p) \perp V_3(p)$, where $V_2(p)$ and $V_3(p)$ are nondegenerate subspaces of dimension 2 and 3, respectively. Since $V_2(p)$ may be of plus or minus type, we get the two classes (3) and (4). It is easy to see that classes (3) and (4) represent these same decomposition stabilizes for all $p > 3$. Indeed these decomposition stabilizers have the same orders as the maximal subgroups in classes (3) and (4), and the only other maximal subgroups of $\Omega(5,p)$ whose orders they divide are those of class (1). For $p > 3$, however, the stabilizer of the decomposition $V_5(p) = V_2(p) \perp V_3(p)$ acts irreducibly on both summands and thus stabilizes no one-dimensional subspace of $V_5(p)$. Hence the maximal subgroups in classes (3) and
(4) are the same decomposition stabilizers for $p > 5$ as they are for $p = 5$. If $\overline{X}/Z(\overline{G})$ is one of these decomposition stabilizers, then $(\overline{X}/Z(\overline{G}))'' = \overline{L}/Z(\overline{G}) \cong PSL(2, p)$. It follows that if $\overline{T} \leq \overline{H} \leq \overline{X}$, then $\overline{H} \leq N_{\overline{G}}(\overline{T})$. As in the preceding paragraph, this implies that $H \leq N_G(L)$ if $\overline{X}$ belongs to class (3) or (4). Since $\overline{L}/Z(\overline{G})$ has order $p(p^2 - 1)/2$, we need not consider the possibility that $\overline{X}/Z(\overline{G})$ belongs to class (5).

Next we consider the possibility that $\overline{X}/Z(\overline{G})$ belongs to class (6). Since $|SL(2, p)|$ divides $|\overline{X}|$, $p$ must be 3 or 5. The Atlas tells us that $\overline{X}/Z(\overline{G})$ is a split extension of $A_3$ by an elementary abelian group of order 16. There is a basis $B = \{v_1, v_2, v_3, v_4, v_5\}$ of $V_6(p)$ such that $O_2(\overline{X}/Z(\overline{G}))$ acts diagonally on $V_6(p)$ with respect to $B$, and a complement to $O_2(\overline{X}/Z(\overline{G}))$ in $\overline{X}/Z(\overline{G})$ permutes the vectors in $B$. If $p = 5$, then $\overline{L}$ is a maximal subgroup of $\overline{X}$, yielding conclusion (c).

If $p = 3$, we claim that $\overline{L}/Z(\overline{G})$ is not contained in a class (6) maximal subgroup $\overline{X}/Z(\overline{G})$ of $PSp(4, 3)$. Indeed, suppose the contrary. Since $O_2(\overline{X}/Z(\overline{G}))$ is the reduced permutation module for $\overline{X}/O_2(\overline{X}) \cong A_5$, it follows that each element of order 3 in $\overline{X}/Z(\overline{G})$ centralizes a $Z_2 \times Z_2$ subgroup of $O_2(\overline{X}/Z(\overline{G}))$. Thus if $\overline{\pi} \in \overline{X}$ has order 3, then 8 divides $|C_{\overline{G}}(\overline{\pi})|$.

To show that $\overline{L}/Z(\overline{G})$ is not contained in a class (6) maximal subgroup of $\overline{X}/Z(\overline{G})$, it therefore suffices to show that if $\overline{\pi} \in \overline{L}$ has order 3, then 8 does not divide $|C_{\overline{G}}(\overline{\pi})|$. Let $\overline{\pi}_1 \in \overline{L}$ be as in the proof of Lemma 3.3. Let $\mathcal{C}$ be the ordered basis $(\overline{v}_1, \overline{d}_1, \overline{v}_2, \overline{d}_2) := (\overline{v}_1 + \overline{v}_2 - \overline{v}_1, \overline{v}_2 - \overline{v}_1, \overline{v}_2 + \overline{v}_1)$ of $\overline{L}$. Then $\mathcal{C}$ is a hyperbolic basis; i.e. $(\overline{v}_1, \overline{d}_1) = (\overline{v}_2, \overline{d}_2) = 1$ and $(\overline{v}_1, \overline{d}_1)$ is orthogonal to $(\overline{v}_2, \overline{d}_2)$. With respect to $\mathcal{C}$, $\overline{\pi}_1$ is represented by the matrix

$$\begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{pmatrix}$$

Comparing with [St] p. 489], we see that $\overline{\pi}_1$ belongs to class $A_{31}$ of [St] and so $|C_{\overline{G}}(\overline{\pi}_1)| = 2 \cdot 3^3 \cdot (3 - 1)$, which is not divisible by 8. We remark that the image of $\pi_1$ in $\Omega_2(p)$ belongs to Atlas class 3D.

Finally, suppose $\overline{X}/Z(\overline{G})$ belongs to class (7). Since $|SL(2, p)|$ divides $|\overline{X}|$, we have $p \leq 7$. If $p = 7$, then $|\overline{X}/Z(\overline{G})| = 2520 = |A_7|$. But $PSp(4, 7)$ contains an $A_7$ subgroup; see e.g. [HL] p. 479. Since 2520 doesn’t divide the order of any maximal subgroups in classes (1)-(6), we have $\overline{X}/Z(\overline{G}) \cong A_7$. Since $A_7$ contains no subgroup isomorphic to $SL(2, 7)$, we have $\overline{X} \cong A_7$. Since $SL(2, 7)$ is a maximal subgroup of $A_7$, we obtain conclusion (d). Similarly, if $p = 5$, then $|\overline{X}/Z(\overline{G})| = 360$. The Atlas tells us that $\overline{X}/Z(\overline{G}) \cong A_6$, and so $\overline{X} \cong A_6 \cong SL(2, 9)$, giving conclusion (b).

The final result in this section is the analog of Proposition 4.1 for $p = 2$. The proof is shorter than that of Proposition 4.1, because we are able to use Liebeck’s classification of the rank 3 primitive affine groups when $p = 2$.

**Proposition 4.4.** Suppose $\nu \geq 3$ and we are in Case II. Let $W_0$ be as in Definition 3.9. Let $v \in W_0$ and let $L = L' \leq H \leq C_G(v)$. Let $\overline{G}$ be the symplectic group $G/EZ$ and let $\overline{H}$ be the image of $H$ in $\overline{G}$. Then $H \cong \overline{H}$ and either $H \leq N_G(L)$, $H \cong GL(3, 2)(Z_2^3)$ as in Lemma 3.10, or one of the following holds:

(a) $\overline{H} = \overline{G}$.

(b) $\overline{H} \cong O^+(2n, 2)$ is the stabilizer of a nondegenerate quadratic form on $\overline{E}$, or $\overline{H} \cong \Omega^+(2n, 2)$ is the commutator subgroup of such a form stabilizer.
THE EXTRASPECIAL CASE OF THE $k(GV)$ PROBLEM

(c) $\overline{H}$ is isomorphic to $Sp(6,2)$, $A_9$, or $S_9$, and $n = 4$.
(d) $\overline{H} \cong G_2(2)$ or $\overline{H} \cong G_2(2)' \cong PSU(3,3)$, and $\alpha$ and $\beta$ are $n = 3$.

Proof. First we show that $\Gamma$ has four orbits on $\overline{E}^\#$. Since $p = 2$, we identify $\overline{E}^\#$ with $P_1(\overline{E})$, the set of all one-dimensional subspaces of $\overline{E}$. Clearly $P_1(\overline{A})$ and $P_1(\overline{A}^*)$ are each $\Gamma$-orbits. Let $\Omega = P_1(\overline{E}) - P_1(\overline{A}) - P_1(\overline{A}^*)$. Then $\Omega$ is the direct product, of $\Gamma$-sets, of $P_1(\overline{A})$ and $P_1(\overline{A}^*)$. Let $\pi$ be the permutation character of $\Gamma$ on $P_1(\overline{A})$. Then the permutation character of $\Gamma$ on $P_1(\overline{A}^*)$ is $\pi^\alpha$, where $\alpha$ is the inverse transpose automorphism of $\overline{A}$. Since $g^{-1}$ is conjugate to $g^\alpha$ for all $g \in \Gamma$, we have $\pi^\alpha = \pi$. Hence the number of orbits of $\Gamma$ on $\Omega$ is the inner product $(\pi^2, 1)$. Since $\Gamma$ is doubly transitive on $P_1(\overline{A})$, we have $(\pi^2, 1) = (\pi, \pi) = 2$. Hence $\Omega$ is the union of two $\Gamma$-orbits, namely $S = \{\pi + \overline{b} : \pi \in P_1(\overline{A}), \overline{b} \in P_1(\overline{A}^*)\}$, and $(\pi, \overline{b}) = 0$ and $N = \{\pi + \overline{b} : \pi \in P_1(\overline{A}), \overline{b} \in P_1(\overline{A}^*)\}$, and $(\pi, \overline{b}) = 1$. We have $|P_1(\overline{A})| = |P_1(\overline{A}^*)| = 2^{n-1} - 1$, while $|S| = (2^n - 1)(2^{n-1} - 1)$ and $|N| = 2^{n-1} - 2^{n-2} - 1$.

By Lemma 3.10, $H \cong \overline{H}$. We may assume that $H \not\cong N_G(L)$, and that $H \not\cong GL(3,2)(Z_2^3)$ when $n = 3$. By Lemma 3.10, $\overline{H}$ does not normalize $A$ or $\overline{A}$, and $\overline{H}$ does not permute $\overline{A}$ and $\overline{A}$. Thus $\overline{H}$ has no orbit of size $2^n - 1$ on $P_1(\overline{E})$. Suppose that $P_1(\overline{A}) \cup P_1(\overline{A}^*)$ is an $\overline{H}$-orbit. Then, for each $h \in \overline{H}$, we have $\overline{A}^h \cup (\overline{A}^* \cap \overline{A})$. Since $\overline{A}^h \cap \overline{A}$ and $\overline{A}^* \cap \overline{A}$ are subspaces of $\overline{A}^*$, it follows that $\overline{A}^h = \overline{A}$ or $\overline{A}^* = \overline{A}$. This contradicts the fact that $\overline{H}$ does not permute $\overline{A}$ and $\overline{A}$. Hence $P_1(\overline{A}) \cup P_1(\overline{A}^*)$ is not an $\overline{H}$-orbit.

It follows that $\overline{H}$ has at most two orbits on $P_1(\overline{E})$. If there are two orbits, then their sizes are either $(2^n - 1)(2^{n-1} + 1)$ and $(2^n - 1)2^{n-1}$, or $(2^n - 1)(2^{n-1} + 1)$ and $(2^n - 1)2^{n-1} - 2$. Clearly $\overline{H}$ acts irreducibly on $\overline{E}$. Lemma 3.3(b) implies that $End_G(\overline{E}) \cong GF(2) \oplus GF(2)$. Thus $End(\overline{H})(\overline{E}) \cong GF(2)$ and so $\overline{H}$ is absolutely irreducible on $\overline{E}$. The semidirect product $\overline{H} \overline{E}$ is a primitive affine group with point stabilizer $\overline{H}$, and $\overline{H} \overline{E}$ is either a doubly transitive or a rank 3 affine group. Using the classification of finite simple groups, Liebeck [11] has determined all primitive rank 3 affine groups. The doubly transitive affine groups were determined earlier by Hering [10].

First suppose that $\overline{H}$ is transitive on $\overline{E}$. By Hering’s Theorem [11], p.512, there are four infinite classes of doubly transitive affine groups. If $\overline{H} \overline{E}$ belongs to one of those classes, then Hering’s Theorem and absolute irreducibility imply that either $\overline{H}$ is contained in a solvable semilinear group, $SL(2n,2) \not\cong \overline{H}$, $Sp(2n,2) \not\cong \overline{H}$, or $|E| = 2^6$ and $G_2(2)' \not\cong \overline{H}$. Obviously the first two possibilities don’t arise in our situation. The third possibility is conclusion (a) of Proposition 4.4. Since $Aut(G_2(2)) = G_2(2)$, the fourth possibility gives conclusion (d) of Proposition 4.4. If $\overline{H} \overline{E}$ is a doubly transitive affine group not belonging to one of the four infinite classes, then $|E|$ is either odd or equal to 16. Thus we need not consider such groups.

Hence we assume that $\overline{H} \overline{E}$ is a rank 3 affine group, with subdegrees as above. By the main result of [11], there are eleven infinite classes of rank 3 affine groups, denoted (A1), . . . , (A11). In class (A1), the point stabilizer is contained in a solvable semilinear group; this obviously can’t occur here. In class (A2), the point stabilizer acts imprimitively on $\overline{E}$ and permutes a pair of subspaces whose dimensions are half the dimension of $\overline{E}$. Since $\overline{E} \overline{H} = \overline{A} \oplus \overline{A}^*$, and $\overline{H}$ does not permute $\overline{A}$ and $\overline{A}^*$, our
affine group \( \overline{H} \overline{E} \) does not belong to class (A2). In class (A3), the point stabilizer stabilizes a tensor product decomposition of \( \overline{E} \). In view of absolute irreducibility, the subdegrees, given in [L1 p. 514], are \( 3(2^n - 1) \) and \( 2(2^n - 1)(2^{n-1} - 1) \). These subdegrees are consistent with the ones we determined above only when \( n = 3 \). Then \( \overline{H} \) is isomorphic to a subgroup of \( GL(2,2) \times GL(3,2) \). Since \( \overline{L} \cong GL(3,2) \), we would then have \( \overline{H} \leq N_{\overline{G}}(\overline{L}) \), and so \( \overline{H} \) would fix or permute \( \overline{A} \) and \( \overline{A}^\prime \), contrary to assumption. Similarly, in class (A4), the subdegrees are consistent with ours only for \( n = 3 \), and then the point stabilizer has a normal subgroup isomorphic to \( GL(3,2) \). As with class (A3), this is impossible. In class (A5), we again find that the subdegrees are consistent with ours only when \( n = 3 \), and then the point stabilizer has a normal \( SL(2,2) \) subgroup. Since \( \overline{L} \) centralizes no \( SL(2,2) \) subgroup of \( GL(\overline{E}) \), this class does not arise.

In class (A6), the point stabilizer normalizes a special unitary group which has \( \overline{E} \) as its natural module (see [L1 p. 483]). Thus \( \text{End}_F(\overline{H})(\overline{E}) \) is a field which properly contains \( GF(2) \). Then \( \overline{H} \leq F^*(\overline{H}) \), contradicting \( \text{End}_F(\overline{H})(\overline{E}) = GF(2) \oplus GF(2) \), and so \( \overline{H} \overline{E} \) does not belong to class (A6). In class (A7), the point stabilizer normalizes a group of the form \( \Omega^+(2a,q) \), which has \( \overline{E} \) as its natural module ([L1 p. 483]). Since \( \text{End}_F(\overline{H})(\overline{E}) = GF(2) \oplus GF(2) \), we have \( q = 2 \) and \( a = n \). The subdegrees are consistent with ours if and only if \( \varepsilon = + \). The natural \( \Omega^+(2n,2) \) has index 2 in its normalizer in \( Sp(2n,2) \); this is obvious for \( n \neq 4 \) since \( |Out(\Omega^+(2n,2))| = 2 \) when \( n = 4 \), and can be checked in the Atlas for \( n = 4 \). Thus class (A7) yields conclusion (b) of Proposition 4.4.

In class (A8), \( |\overline{E}| = q^{10} \) and the point stabilizer normalizes an absolutely irreducible \( SL(5,q) \) subgroup; \( \overline{E} \) affords the skew square of the natural representation of \( SL(5,q) \). Hence \( q = 2 \) and the subdegrees are not consistent with ours. In class (A10), \( |\overline{E}| = q^{16} \) and the point stabilizer normalizes an absolutely irreducible \( D_5(q) \) subgroup. As with class (A8), \( q = 2 \) and the subdegrees are not consistent with ours. Class (A11) arises from the embedding of \( Sz(q) \) in \( Sp(4,q) \) and is obviously inconsistent with our situation.

Finally, class (A9) arises from the absolutely irreducible action of \( Sp(6,q) \cong \Omega^+(7,q) \) on a spin module of cardinality \( q^8 \), and the point stabilizer normalizes this \( Sp(6,q) \) subgroup. As usual, absolute irreducibility implies that \( q = 2 \) in our situation. Since \( Sp(6,2) \) has no outer automorphism, this is covered under conclusion (c).

In addition to the eleven infinite classes of rank 3 affine groups, there are finite families (B) and (C). Each point stabilizer in family (B) contains a normal extraspecial subgroup. These affine groups do not arise in our situation; [L1, Table 1] implies that \( |\overline{E}| \) would be either odd or equal to \( 2^6 \), in which case \( \overline{E} \cong GL(3,2) \) does not act on an extraspecial subgroup of order \( 27 \) in \( GL(\overline{E}) \).

Family (C) consists of rank 3 affine groups whose point stabilizer \( \overline{H} \) satisfies the condition that \( \overline{H}/Z(\overline{H}) \) has a simple socle \( \overline{S} \). In our situation, \( Z(\overline{H}) = 1 \), and so \( \overline{H} \leq Aut(\overline{S}) \). Since \( |\overline{E}| \) is an even power of 2, [L1, Table 2] says that \( \overline{S} \) must be \( A_6, A_7, A_9, A_{10}, PSL(2,17), \) or \( J_2 \), with \( |\overline{E}| \) respectively equal to \( 2^6, 2^8, 2^8, 2^8, 2^8, \) or \( 2^{12} \). The fact that \( |\overline{L}| \) divides \( |\overline{S}| \) eliminates all but the third and fourth of these possibilities. The fourth possibility is not consistent with our subdegrees. The third possibility is covered under conclusion (c). \[ \square \]
5. Existence of real vectors

**Definition 5.1.** Let $W_0$ be as in Definition 3.9. We define $W_1$ to be the set of all $v \in W_0$ such that either $v$ is a real vector or $C_G(v) \leq N_G(L)$.

**Proposition 5.2.** Suppose $n \geq 3$ and we are in Case I or Case II. Let $W_1$ be as in Definition 5.1. Then either $W_0 = W_1$ or $p = 2$, $n = 3$, $|P_1(W_1)| \geq |P_1(W_0)| - 2$, and $C_G(v) \cong PSU(3,3)$ for all $v \in W_0 - W_1$.

**Proof.** If $p$ is odd, the result follows from Proposition 4.1. Suppose then that $p = 2$. Let $v \in W_0 - W_1$.

First suppose that $n = 3$ and $H := C_G(v)$ is a split extension of $GL(3,2)$ by an elementary abelian group of order 8. Let $\chi$ be as in Section 1. Since $\chi(1) = 8$ and $O_2(H) \not\leq Ker \chi$, it follows that $\chi_H = 1_H + \alpha$, where $\alpha \in Irr(H)$ and $\alpha(1) = 7$. Let $\lambda$ be a linear constituent of $\alpha_{O_2(H)}$. Then $\alpha = \omega^H$, where $\omega \in Irr(H(\lambda))$ is an extension of $\lambda$. Now $I_H(\lambda)/Ker \lambda \cong S_4 \times Z_2$, and so $\omega^2$ is the principal character of $I_H(\lambda)$. It follows from Clifford’s Theorem that $\alpha$ and $\chi_H$ are real-valued. By Definition 1.8, $v$ is a real vector. Thus $v \in W_1$, a contradiction.

Let $N = N_K(v)$. Since $L = L' \leq N \leq N_G(v) = C_G(v)Z = NZ$, Proposition 4.4 implies that the image $\overline{N}$ of $N$ in $G/EZ$ is one of the groups in (a), (b), (c), or (d) of Proposition 4.4. Moreover $\overline{N} \cong C_G(v)$.

Suppose first that $\overline{N}$ falls under conclusion (a) of Proposition 4.4. Then $\overline{N} \cong Sp(2n,2)$. Since $N_G(v) = C_G(v)Z$, Lemma 3.10 implies that $C_G(v) \cap EZ = 1$, and thus $N \cap EZ = Z(E)$, and so $N \cap E = Z(E)$. Thus $N/Z(E)$ is a complement to $E/Z(E)$ in $K/Z(E) = C_{Aut(E)}(Z(E))$. Since $n \geq 3$, however, $C_{Aut(E)}(Z(E))$ does not split over $E/Z(E)$ by [Gr1], Corollary 2], a contradiction.

Suppose next that $\overline{N}$ falls under conclusion (b) of Proposition 4.4. Write $E = E_0Z$, as at the beginning of Section 1, with $E_0$ of plus type. Then $N_{GL(v)}(E_0) = K_0Z$, with $K_0 \cong K^+(2n,2)$. Thus $K_0/E_0 \cong O^+(2n,2)$. Clearly $K_0 \leq G$. Up to conjugacy in $G/EZ$, we have $\overline{N} = K_0$ or $\overline{N} = K_0$, so we assume without loss of generality that $\overline{N} = K_0$ or $\overline{N} = K_0$. As in the preceding paragraph, $N \cap E = Z(E)$, and so $N \cap E_0 = Z(E_0)$. Since $N$ normalizes $E_0$, we have $N = (N \cap K_0)Z(E)$. and so $(N \cap E_0)E_0 = K_0$ or $(N \cap K_0)E_0 = K_0$. Thus $(N \cap K_0)Z(E_0)$ is a complement to $E_0/Z(E_0)$ in $K_0/Z(E_0)$ or $K_0/Z(E_0)$. By [Gr1] Theorem 1], however, $Aut(E_0) \cong K_0/Z(E_0)$ and $Aut(E_0)^n \cong K_0/Z(E_0)$ don’t split over $E_0/Z(E_0) = Inn(E_0)$ for $n \geq 3$, a contradiction.

If $\overline{N}$ falls under conclusion (c) of Proposition 4.4, then $n = 4$ and $\overline{N} = A_9, S_9$, or $Sp(6,2)$. We saw above that $\overline{N} = C_G(v)$, and Proposition 4.4 implies that $C_G(v) \cong C_G(v)$. Thus $C_G(v)$ is a real group, and so $v$ is a real vector by Definition 1.8. This contradicts our assumption that $v \notin W_1$.

Next suppose that $\overline{N}$ falls under conclusion (d) of Proposition 4.4. If $\overline{N} \cong G_2(2)$, then, as in the preceding paragraph, $C_G(v) \cong G_2(2)$. Let $H = C_G(v)$ and let $\chi$ be as in Section 1. From the character table of $G_2(2)$, we see that either $\chi_H = \lambda + \alpha$, with $\lambda(1) = 1$ and $\alpha$ irreducible of degree 7, or $\chi_H = \lambda + \mu + \beta$, with $\lambda(1) = \mu(1) = 1$ and $\beta$ irreducible of degree 6. We claim that the latter possibility can’t occur. Indeed, if we had $\chi_H = \lambda + \mu + \beta$ as above, then by [A] p. 14], $\chi(x) = 3$ for certain elements $x \in H'$. Since $\chi$ restricts irreducibly to $\langle x \rangle E$, this contradicts Lemma 1.3. Hence $\chi_H = \lambda + \alpha$ as above. Since $G_2(2)$ has a unique irreducible character of degree 7, we see that $\chi_H$ is real-valued. Hence $v$ is a real vector by Definition 1.8, contradicting our assumption that $v \notin W_1$. 

It follows that $C_G(v) \cong \overline{N} \cong G_2(2)' = PSU(3,3)$. From the Atlas, we see that $G \cong Sp(6,2)$ contains a unique conjugacy class of $PSU(3,3)$ subgroups, and a unique conjugacy class of $G_2(2)$ subgroups. Let $\overline{T} \leq \overline{M} \leq \overline{N}$, with $\overline{M} \cong G_2(2)$. By the Atlas, $\overline{M}$ contains a unique conjugacy class of $GL(3,2)$ subgroups, and each such subgroup has index 2 in its normalizer in $\overline{M}$. By Lemma 3.3, we have $|N_{G_2(2)}(T):(T)| = 2$. Thus $N_{G_2(2)}(L) \leq \overline{M}$. If $\overline{T} \leq (\overline{M})^x$ for some $x \in G$, then the $\overline{M}$-conjugacy of $\overline{T}$ and $(\overline{T})^{x^{-1}}$ implies that $x^{-1}y \in N_{G_2(2)}(T)$ for some $y \in \overline{M}$. Thus $x^{-1}y \in \overline{M}$ and so $x \in \overline{M}$. Hence $\overline{M}$ is the unique $PSU(3,3)$ subgroup of $G$ containing $T$.

Let $\widetilde{M}$ be the inverse image of $\overline{M}$ in $K$. The preceding paragraph implies that $N \leq \widetilde{M}$. By Lemma 3.10, $N \cap E = Z(E)$ and so $\overline{N} \cong N/Z(E)$. Thus $N/Z(E)$ is a complement to $E/Z(E)$ in $\overline{M}/Z(E)$. Let $k$ be an algebraically closed field of characteristic 2. Then $k \otimes \overline{E}$ is the unique 6-dimensional simple $k\overline{M}$-module. By [Si, p. 4517], $Ext^1_{\overline{M}}(k \otimes \overline{E}, k)$ has dimension 1 over $k$. It follows that $Ext^1_{GF(2)\overline{M}}(\overline{E}, GF(2))$ has cardinality 2. Thus $|H^1(\overline{M}, \overline{E})| = 2$ and there are exactly two conjugacy classes of complements to $E/Z(E)$ in $\overline{M}/Z(E)$; see [As] p. 64.

We have $L \leq N \leq NE = \widetilde{M} \leq K$, with $N/Z(E) \cong PSU(3,3)$. Suppose that $L$ is contained in two distinct $NE$-conjugates of $N$. Then $L^e \leq N$ for some $e \in E\setminus Z(E)$, but $L^e = \{x|x,e|x \in L\}$. It follows that $N$ contains $[L,e]$, contradicting $N \cap E = Z(E)$.

Thus each of the two conjugacy classes of complements to $E/Z(E)$ in $\overline{M}/Z(E)$ yields at most one overgroup of $L$ in $\overline{M}$ which can equal $N_K \langle v \rangle$, for some $v \in W_0 - W_1$. Since $L$ uniquely determines $\overline{M}, \overline{M}$, and $\overline{M}$, it follows that $L$ has at most two overgroups in $K$ which can equal $N_K \langle v \rangle$, for some $v \in W_0 - W_1$. Denote these two overgroups, if they exist, by $N_1$ and $N_2$. Thus if $v \in W_0 - W_1$, then $\langle v \rangle$ must be stabilized by $N_1$ or $N_2$. Since $PSU(3,3)$ has trivial Schur multiplier, $N_i = N_i' \times Z(E)$ for $i = 1, 2$. Hence if either $N_i$ stabilizes more than one point in $P(1)$, then $N_i'$ must centralize $W$. Thus $N_i'$ centralizes the vector $w$ of Lemma 3.6. By Lemma 3.6, $A$ also centralizes $w$. Thus $\langle N_i', A \rangle = \overline{M}$ centralizes $w$, contradicting Lemma 3.6 (b). We conclude that each $N_i$ fixes at most one point in $P(1)$. Thus $|P_1(W_0)| - |P_1(W_1)| \leq 2$, as desired.

**Proposition 5.3.** Suppose we are in Case I with $n = 2$. Let $W_1$ be as in Definition 5.1. Then either $W_0 = W_1$ or $p = 3$ and $W_0 - W_1$ is contained in the union of three one-dimensional subspaces of $W$.

**Proof.** First suppose $p \geq 5$. Let $v \in W_0 - W_1$. Let $H = C_G(v)$. By Proposition 4.3, $H \cong \overline{T}$ and either $H$ is contained in one of the $(p-1)/2$ distinct $L$-conjugates of $MZ$, or $\overline{T}$ falls under conclusion (a), (b), (c), or (d) of Proposition 4.3.

Suppose first that $H$ is contained in one of the $L$-conjugates of $MZ$. We will show that supposing $H \leq MZ$ leads to a contradiction; the same argument will work if $H$ is contained in one of the other $L$-conjugates of $MZ$. Suppose then that $H \leq MZ$. Then $\overline{T} \leq H \leq \overline{M} \cong SL(2,p) wr Z_2$. By Lemma 3.10, $\overline{H} \not\leq N_{\overline{M}}(\overline{T})$. Since $p \geq 5$, $\overline{E}/Z(\overline{E})$ is a maximal subgroup of $\overline{M}/Z(\overline{M}) \cong PSL(2,p) \times PSL(2,p)$. Since
By Lemma 1.2, the restriction of $E_i$ lying over $\lambda_i$ and let $\psi_i \in \text{Irr}(K_i)$ be the unique extension of $\theta_i$ to $K_i$. Now $\psi_1 \times \psi_2$, viewed as an irreducible character of $K_1 * K_2 = M'E$, lies over $\lambda$. Since $K_1 * K_2$ has no nontrivial linear character, $\psi_1 \times \psi_2$ is the unique irreducible character of $K_1 * K_2$ of degree $p^2$ lying over $\lambda$. But if $\psi \in \text{Irr}(K)$ is as in Section 1, then $\psi_{M'E}$ is irreducible of degree $p^2$ and also lies over $\lambda$. Hence $\psi_1 \times \psi_2 = \psi_{M'E}$.

By Lemma 1.2, $\psi_{M'} = (\psi_1)_{S_1} \times (\psi_2)_{S_2}$ is the sum of four irreducible characters, of degrees $(p - 1)^2/4, (p^2 - 1)/4, (p^2 - 1)/4$ and $(p + 1)^2/4$.

Let $\phi$ be the Brauer character of $G$ afforded by $V$, as in Section 1. The proof of Lemma 1.7 shows that there exists a linear character $\mu$ of $G$ with $EZ \leq \text{Ker}\mu$ such that $\chi(g) = \mu(\phi(g))$ for all $g \in G$ of order prime to $r$. Since $\chi_K = \phi$ and $M' = M'',$ it follows that the Brauer character of $M'$ afforded by $V$ coincides with the restriction of $\psi$ to the $r^i$-elements of $M'$. By Lemma 1.2, the ordinary irreducible constituents of $(\psi_1)_{S_1}$ and $(\psi_2)_{S_2}$ remain irreducible in “characteristic $r$” (since $r$ need not be a prime, we are abusing language). It follows that the four ordinary irreducible constituents of $\psi_{M'} = (\psi_1)_{S_1} \times (\psi_2)_{S_2}$ remain irreducible in characteristic $r$; see e.g. [A, 27.15]. Since none of these four constituents are linear, $M'$ stabilizes no one-dimensional subspaces of $V$, the desired contradiction.

Thus $\overline{H}$ falls under (a), (b), (c), or (d) of Proposition 4.3. Suppose first that $\overline{H}$ falls under conclusion (a). Then $SL(2, p^2) \cong H' \leq C_K(u)^t \cong Sp(4, p)$, where $u$ is the central involution of $L$. By Lemma 1.2, the restriction of $\psi$ to $C_K(u)$ has two irreducible constituents, $\psi_1$ and $\psi_2$, of degrees $(p^2 - 1)/2$ and $(p^2 + 1)/2$ respectively. Since $(p^2 - 1)/2$ is the smallest nontrivial character degree of $H'$, $\psi_1$ restricts irreducibly to $H'$. We claim that $\psi_2$ also restricts irreducibly to $H'$. Indeed, if this were not the case, then $\psi_2|H' = 1_{H'} + \alpha$, where $\alpha \in \text{Irr}(H')$ and $\alpha(1) = (p^2 - 1)/2$. Now if $x \in H'$ has order $p^2 + 1$, then the character table of $SL(2, p^2)$ (see e.g. [D, p. 228]) shows that $\psi(x) = \psi_1(x) + 1 + \alpha(x) = 3$. Since $p > 3$, this contradicts Lemma 1.3. Thus $\psi_1$ and $\psi_2$ restrict irreducibly to $H'$. By [CMS], $(\psi_1)_H$ and $(\psi_2)_H$ remain irreducible in “characteristic $r$.” As in the preceding paragraph, it follows that $H'$ stabilizes no one-dimensional subspace of $V$, contradicting $H = C_G(v)$.

Suppose that $\overline{H}$ falls under conclusion (b) or (c) of Proposition 4.3. Then $p = 5$ and $H = H' \leq C_K(u)^t \cong Sp(4, 5)$. Since $p \equiv 1(\text{mod } 4)$, Lemma 1.2 implies that $\psi_{H'}$ is real-valued. We have $N_K(v) = H' \times Z(E) = C_K(v) \times Z(E)$. Thus Lemma 1.11 implies that $v$ is a real vector, contradicting $v \notin W_1$.

Now suppose $\overline{H}$ falls under conclusion (d) of Proposition 4.3. As in the preceding paragraph, it suffices to show that $\psi_{H'}$ is real-valued. Now $H \cong A_7$, and so (by [A, p. 10]) if $x \in H$ is not a real element of $H$, then the image of $x$ in $H/Z(H)$ has order 7. Since 7 divides $|A_7|$ to the first power, it suffices to prove that $\psi(x)$ is real
for an element $x \in L'$ of order 7. By Corollary 3.5, $x$ and $x^{-1}$ are conjugate in $N_K(L)$. Hence $\psi(x) = \psi(x^{-1})$ and so $\psi(x)$ is real, as desired.

It remains to consider $p = 3$. Suppose $v \in W_0 \setminus W_1$ and let $H \cong C_G(v)$ as above. Then $H \cong \mathcal{H}$. By Proposition 4.3, either $H \leq MZ$ or $\mathcal{H}$ is contained in an $\widehat{S}_6$ subgroup of $\mathcal{G}$; note that conclusion (a) is subsumed under (c) when $p = 3$.

First consider the possibility that $\mathcal{H}$ is contained in an $\widehat{S}_6$ subgroup of $\mathcal{G} \cong Sp(4,3)$. Then $\mathcal{T}/Z(\mathcal{G}) \cong A_4$ is contained in $\mathcal{T}/Z(\mathcal{G})$, which is contained in a maximal $S_6$ subgroup of $\mathcal{T}/Z(\mathcal{G}) \cong PSp(4,3)$. From the list of maximal subgroups of $A_6$ and $S_6$, we see that every solvable overgroup of $\mathcal{T}/Z(\mathcal{G})$ in $S_6$ normalizes $\mathcal{T}/Z(\mathcal{G})$. Thus if $\mathcal{H}$ is solvable, then $\mathcal{H} \leq N_{\mathcal{T}}(\mathcal{L}) = N_{\mathcal{G}}(\mathcal{L})$. Then $\mathcal{H}$ fixes or permutes $\mathcal{L}$ and $\mathcal{T}$, and so $H \leq N_G(L)$ by Lemma 3.10, contradicting $v \notin W_1$.

Hence $\mathcal{H}$ is not solvable, and so $\mathcal{H}/Z(\mathcal{G})$ is isomorphic to $A_5$, $S_5$, $A_6$, or $S_6$. If $\mathcal{H}/Z(\mathcal{G})$ is isomorphic to $A_5$ or $A_6$, then $H \cong \mathcal{H}$ is isomorphic to $A_5$ or $A_6$. Since these two groups are real, $\chi_H$ is real-valued. Thus $v$ is a real vector by Definition 1.8, contradicting $v \notin W_1$.

To handle the $S_5$ and $S_6$ cases, we first claim that $\mathcal{L}/Z(\mathcal{G})$ is contained in a unique $S_6$ subgroup of $PSp(4,3)$. To see this, we use the isomorphism $PSp(4,3) \cong \Omega(5,3)$. Now $\Omega(5,3)$ has a single conjugacy class of $S_6 \cong O^-(4,3)$ subgroups, so it suffices to show that $\mathcal{L}/Z(\mathcal{G})$ is contained in a unique $O^-(4,3)$ subgroup of $\Omega(5,3)$.

Let $V_5(3)$ be the natural module for $\Omega(5,3)$. Since $\mathcal{L}/Z(\mathcal{G}) \cong A_4$ has no faithful representation of degree 2 over $GF(3)$, the dimension of $[O_2(\mathcal{L}/Z(\mathcal{G})), V_5(3)]$ must be at least 3. Hence $O_2(\mathcal{L}/Z(\mathcal{G}))$ centralizes at most a two-dimensional subspace of $V_5(3)$. Since $\mathcal{L}$ stabilizes two maximal totally isotropic subspaces of $\mathcal{E}$, the Atlas tells us that $\mathcal{L}/Z(\mathcal{G})$ fixes two isotropic points in $P_1(\mathcal{V}_5(3))$. Hence $\mathcal{T}/Z(\mathcal{G})$ centralizes two isotropic one-dimensional subspaces of $V_5(3)$. The containment $\mathcal{T}/Z(\mathcal{G}) \leq \mathcal{M}/Z(\mathcal{G}) \cong O^+(4,3)$ shows that $\mathcal{T}/Z(\mathcal{G}) = O^+(\mathcal{T}/Z(\mathcal{G}))$ centralizes a one-dimensional plus type subspace of $V_5(3)$. Now if $\mathcal{T}/Z(\mathcal{G})$ fixes, or equivalently centralizes, more than one one-dimensional minus type subspace of $V_5(3)$, then the centralizer of $\mathcal{T}/Z(\mathcal{G})$ in $V_5(3)$ would have dimension greater than 2, which we have shown is not the case. This proves our claim.

From the list of maximal subgroups of $A_6$, it is clear that any two $A_4$ subgroups of $A_6$ are conjugate under $Aut(A_6)$. Hence each $A_4$ subgroup of $A_6$ is contained in exactly two $A_5$ subgroups of $A_6$. It follows that each $A_4$ subgroup of $S_6$ is contained in exactly two $S_5$ subgroups of $S_6$. Since every $S_5$ subgroup of $PSp(4,3)$ is contained in an $S_6$ subgroup of $PSp(4,3)$, it follows that $\mathcal{T}$ is contained in exactly two $\widehat{S}_5$ subgroups of $Sp(4,3)$.

Let $S'_1$ and $S'_2$ be the inverse images in $C_K(u)' \cong Sp(4,3)$ of the two $\widehat{S}_5$ overgroups of $\mathcal{T}$ in $\mathcal{G}$, and let $S'$ be the inverse image in $C_K(u)'$ of the unique $\widehat{S}_6$ overgroup of $\mathcal{T}$ in $\mathcal{G}$. If $\mathcal{P} = \mathcal{S}_i$ for $i \in \{1, 2\}$, then $H \leq S_i Z$ and so $H = S'_i$. Each $S'_i$ fixes at most one point in $P_1(W)$, since otherwise $S'_i$ would centralize $W$, contradicting Lemma 3.6(b). In the unlikely event that $\mathcal{P} \cong \mathcal{S}_6$, then $H' = S'$. Again $S'$ fixes at most one point in $P_1(W)$, and if $(v) \in P_1(W)$ is fixed by $S'$, then $S'_1$ and $S'_2$ fix $(v)$ and no other point in $P_1(W)$. We conclude that the set of points in $P_1(W)$ fixed by some $\mathcal{S}_5$ or $\mathcal{S}_6$ overgroup of $L'$ has cardinality at most 2.
The remaining possibility is that $H \leq MZ$. Then $\overline{T} \leq \overline{H} \leq M \cong SL(2,3)$ wr $Z_2$. Let $\overline{B} \cong SL(2,3) \times SL(2,3)$ be the base group of this wreath product. Then $\overline{T}$ is diagonally embedded in $\overline{B}$.

We claim that $\overline{B} \cap O_2(\overline{T}) = O_2(\overline{M}) \cong Q_8 \times Q_8$. Suppose the contrary. Then, since $O_2(\overline{M})/Z(\overline{M})$ is the direct sum of two irreducible $\overline{L}$-modules of cardinality 4, we must have $\overline{B} \cap O_2(\overline{T}) \cong O_2(\overline{L})Z(\overline{M}) \cong Q_8 \times Z_2$. Let $\overline{T}$ be a 3-Sylow subgroup of $\overline{L}$, and let $\overline{R}$ be a 3-Sylow subgroup of $\overline{H}$ containing $\overline{T}$. Suppose $|\overline{R}| = 9$.

Let $\overline{O}$ be the centralizer in $\overline{R}$ of $\overline{B} \cap O_2(\overline{H})$. Then $\overline{C}$ is the centralizer of $\overline{O}$ in $\overline{R}$ of $\overline{O}_2(\overline{L})/Z(\overline{L})$, and so $|\overline{C}| = 3$. Thus $\overline{C} \notin \overline{T}$ and $\overline{C}$ centralizes $\langle \overline{T}, O_2(\overline{L}) \rangle = L'$. Thus $L' \leq N_{\overline{G}}(L') = N_{\overline{G}}(\overline{L})$. By Lemma 3.3, however, $|N_{\overline{G}}(\overline{L})| = 96$, a contradiction. Hence $|\overline{C}| = |\overline{T}|$ and 3 divides $|\overline{L}|$ to the first power. It follows that $\overline{C} \cap \overline{L} = L'$ or $\overline{C} \cap \overline{B} \cong L' \times Z_2$. Thus $L' = O_3'(\overline{H} \cap \overline{B})$ is normal in $\overline{H}$ and so $\overline{L} \subseteq N_{\overline{G}}(L') = N_{\overline{G}}(\overline{L})$. As above, this implies via Lemma 3.10 that $H \leq N_{G}(L)$, contradicting $v \notin W_1$. This establishes our claim.

Since $O_2(\overline{M}) \leq \overline{T}$, we have $O_2(\overline{M}) = \langle \overline{T}, O_2(\overline{M}) \rangle \leq \overline{H}$, since $H \leq MZ$, we have $H' \leq M$. It follows that $O_2(\overline{M}) \leq H'Z \cap M = H'(Z \cap M) = H'$. Let $B \cong SL(2,3) \times SL(2,3)$ be the inverse image in $C_K(u)^{\prime} \cong Sp(4,3)$ of $\overline{B}$, the base group of $\overline{M}$. Let $\phi$ be the Brauer character of $G$ afforded by $V$, as in Section 1. An argument similar to the one we gave above for $p > 3$ shows that $\psi_B = \phi_B$; note that $\phi_B$ is an ordinary character of $B$, since $(6, r) = 1$. It follows as when $p > 3$ that $\phi_B$ is the sum of irreducible characters of degrees $(p - 1)^2/4, (p^2 - 1)/4, (p^2 - 1)/4$, and $(p + 1)^2/4$. Hence $V_B$ is the direct sum of irreducible submodules of dimensions 1, 2, 2, and 4. These remain irreducible when restricted to $O_2(M) = O_3(B) \leq H'$. It follows that $O_2(\overline{M})$ fixes exactly one point in $P_1(V)$, and so at most one point in $P_1(W)$. Hence there is at most one point in $P_1(W)$ that can be fixed by any subgroup $H$ satisfying $L' \leq H \leq MZ$ and $O_2(\overline{M}) \leq H$.

Thus if we remove at most $3 = 2 + 1$ one-dimensional subspaces of $W$ from $W_0$, we have shown that the remaining vectors in $W_0$ belong to $W_1$, as desired.

**Theorem 5.4.** Suppose we are in Case I with $n \geq 2$ or in Case II with $n \geq 3$. Then $W$ contains a real vector.

**Proof.** Let $N = N_G(L)$. Lemma 3.4 implies that $N = \langle t \rangle LZ$, where $t \in N_K(L)$ induces the transformation $\overline{t} \in Sp(2n, p)$ of Lemma 3.3. If $p$ is odd, then $\overline{t}$ has order 4. Since $K$ splits over $E$, we may take $t$ to have order 4. If $p = 2$, then $\overline{t}$ has order 2 and $t^2 \in N_K(L) = Z(E)$. If $r \equiv 1(\text{mod } 8)$, then, after multiplying $t$ by a scalar if necessary, we may take $t$ to have order 2. If $r \equiv 5(\text{mod } 8)$, then, after multiplying $t$ by a scalar, we may take $t$ to have order 2 or 8.

Now $N$ acts monomially on $W$ with respect to the basis $\{w, w^*\}$, by Lemma 3.6. Let $C = C_W(N)$, so that $L' \leq C$. Let $D = N/C$. Since $t$ inverts $L/L'$, we may write, with slight abuse of notation, $D = \langle t, x \rangle Z$, where $x$ is the image in $D$ of an element of $L$ of determinantal order $p - 1$, and $Z \leq Z(G)$ is the group of scalar transformations on $W$. If $p = 2$, then $t^2 \in Z(G)$ and so $\langle t \rangle$ acts faithfully on $W$. Since $x$ acts diagonally on $W$ with respect to the basis $\{w, w^*\}$, it follows that the order $m$ of $x$ divides $\text{gcd}(p - 1, r - 1)$.

Let $-1 \in Z(G)$ be the scalar of order 2. We claim that $C \leq L \times \langle -1 \rangle$. Indeed $C$ is certainly contained in $L \times Z$, so it suffices to show that if an element $a \in L$ acts as a scalar $\alpha$ on $W$, then $\alpha = \pm 1$. Since $a$ is conjugate in $N$ to $a^{-1}$ by Corollary 3.5, we
see that $a$ acts on $W$ as $\alpha$ and as $\alpha^{-1}$, and the claim follows. Thus $C \leq L \times \langle -1 \rangle$. If $p = 2$, then $L = L' \leq C$ and so $C = L$.

Now let $W_1$ be as in Definition 5.1. Suppose we can show that $C_N(v) \leq C$ for a vector $v \in W_1$. We claim that $v$ must be a real vector. To see this, we may certainly assume that $C_G(v) \leq N_G(L) = N$. By Definition 1.8, it suffices to show that $\chi_C$ is real-valued. By Corollary 3.5, $\chi_L$ is real-valued. Since $-1 \in Z(G)$, it follows that $\chi_{L \times \langle -1 \rangle}$ is real-valued. Thus $\chi_C$ is real-valued, proving the claim.

We showed above that $t$, viewed as an element of $G$, has order 4 when $p$ is odd, and order 2 or 8 when $p = 2$. We now consider the order of $tC$ in $N/C = D$; by abuse, we call this the order of $t \in D$. When $p = 2$, we have $t^2 \in Z(G)$, and so the order of $t \in D$ is the same as the order of $t$. When $p$ is odd, $t^2$ may lie in $C$, so the order of $t \in D$ is either 2 or 4.

Suppose now that $D$ is abelian and $t \in D$ has order 2. Since $t$ inverts $x$ in $D$, we have $m = 2$. We replace $w^*$ by a scalar multiple so that $t$ interchanges $w$ and $w^*$.

Since the eigenspaces of $t$ are $\langle x \rangle$-invariant, it follows that $(t, x)$ acts diagonally on $W$ with respect to the basis $\{w + w^*, w - w^*\}$. If $v \in W - \langle w + w^* \rangle$, then $C_D(v) \leq Z$, since $D = \langle t, x \rangle, Z$. Since $Z$ is the group of scalar transformations on $W$, $C_D(v) = 1$. Hence $C_N(v) \leq C$ for all $v \in W_1 - \langle w + w^* \rangle$. The preceding paragraph shows that every such vector $v$ is real.

If $W_1 = W_0$, then, since $p | r - 1$ and $4 | r - 1$ if $p = 2$, we have $r \geq 5$. Hence $W_1 - \langle w + w^* \rangle$ is nonempty and so $W$ contains a real vector, as desired. Thus we may assume $W_1 \neq W_0$. By Propositions 5.2 and 5.3, either $p = 3$ and $n = 2$ or $p = 2$ and $n = 3$. If $p = 3$ and $n = 2$, then, by Proposition 5.3, $W_0 - W_1$ is contained in the union of three one-dimensional subspaces of $W$. Since $|P_1(W)| = r + 1 \geq 8$, we see that $W_1 - \langle w + w^* \rangle$ contains at least $8 - 3 - 2 - 2 = 1$ one-dimensional subspace of $W$, and so $W$ contains a real vector, as desired.

Suppose then that $p = 2$ and $n = 3$. We claim that $v = w + w^*$ is a real vector. Indeed $|C_N(v) : L| = 2$ and $C_N(v) = \langle t \rangle L \cong Aut(L)$. If $C_N(v) = C_G(v)$, then the character table of $Aut(L)$ shows that $\chi$ is real on $C_G(v) - L$, while Corollary 3.5 shows that $\chi$ is real on $L$. Thus $v$ is a real vector if $C_G(v) = C_N(v)$. If $C_G(v) > C_N(v)$, then either $v \in W_1$ and $v$ is real, or Proposition 5.2 implies that $C_G(v) \cong C_N(v)$ is not contained in any $PSU(3, 3)$ subgroup of $Sp(6, 2)$, as can be seen from the list of maximal subgroups of $PSU(3, 3)$. Hence $v$ is a real vector, whether or not $C_N(v) = C_G(v)$, as desired.

Now suppose $D$ is abelian and $t \in D$ has order 4. Then we may assume $p$ is odd, as shown above. Now $t \in K$ squares to the central involution of $L$. If $n$ were even, then $t^2 \in L' \leq C_K(W)$ and so $t$, considered as an element of $D$, would have order 2. Hence $n$ is odd. By Proposition 5.2, $W_0 = W_1$.

If $D$ acts irreducibly on $W$, then $t^2$ acts as $-1$ on $W$, and $x$ acts as $\pm 1$ on $W$. Thus $|D : Z| = 2$, $r \equiv 3 \pmod{4}$, $t$ has no eigenspaces on $W$, and every nonzero vector in $W$ lies in a regular $D$-orbit. Thus $C_N(v) = C$ for all $v \in W_0 = W_1$, and so $W$ contains a real vector as in the fourth paragraph of this proof. If $D$ acts reducibly on $W$, then only two one-dimensional subspaces of $W$ can be eigenspaces for any element of $D - Z$. Since $t \in D$ has order 4, reducibility implies that $r \equiv 1 \pmod{4}$, so in particular $r > 3$. If we avoid these two subspaces, then we can find $v \in W_0 = W_1$ such that $C_D(v) \leq Z$. Thus $C_D(v) = 1$, $C_N(v) = C$, and $v$ is a real vector.

Next suppose $D$ is abelian and $t \in D$ has order 8. Then $p = 2$, and we may assume $r \equiv 5 \pmod{8}$ as shown above. Furthermore $t$ acts irreducibly on $W$, and $t^2$
is a scalar transformation of order 4. It follows that every nonzero vector in \( W \) lies in a regular \( D \)-orbit. Thus \( C_N(v) = C \) for all nonzero \( v \in W \). Since \( W_1 \) is nonempty by Proposition 5.2, it follows as above that \( W \) contains a real vector.

Finally, suppose \( D \) is nonabelian. Since \( m > 2 \) and \( m|p - 1 \), we have \( p > 3 \). By Propositions 5.2 and 5.3, we have \( W_0 = W_1 \). If \( v \in \langle w \rangle \cup \langle w^* \rangle \), then \( v \) is centralized by a nontrivial element of \( \langle x \rangle \) \( Z \), and so \( C_D(v) \neq 1 \). Hence it suffices to show that \( C_D(v) = 1 \) for some vector \( v \in W \), since \( v \) would then lie in \( W_0 = W_1 \).

Thus it remains to show that \( D = \langle t, x \rangle \) has a regular orbit on \( W \). Let \( d = \gcd(p - 1, r - 1) \). Let \( \langle \sigma \rangle = GF(r)^* \) and let \( \alpha = \sigma^{(r - 1)/d} \). Since \( t \in D \) has order 2 or 4, we may assume that \( t \) takes \( w \) to \( \varepsilon w^* \) and \( w^* \) to \( w \) for \( \varepsilon \in \{\pm 1\} \). Since \( t \) inverts \( x \) and \( x \) has order dividing \( d \), we have

\[
  t = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}, \quad x = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}
\]

with respect to the basis \( \{w, w^*\} \) of \( W \), with \( \gamma \in \langle \alpha \rangle \). Let \( \tilde{D} \) be the subgroup of \( GL(2, r) \) generated by

\[
  \left( \begin{array}{cc} 0 & 1 \\ \varepsilon & 0 \end{array} \right), \quad \left( \begin{array}{cc} \alpha & 0 \\ 0 & \alpha^{-1} \end{array} \right), \quad \text{and} \quad \left( \begin{array}{cc} \sigma & 0 \\ 0 & \sigma \end{array} \right).
\]

Then, with respect to the basis \( \{w, w^*\} \), we have \( D \leq \tilde{D} \). Thus it suffices to show that \( \tilde{D} \) has a regular orbit on \( GF(r)^2 \).

Write \( \tilde{D} = \tilde{D}_+ \cup \tilde{D}_- \), where

\[
  \tilde{D}_+ = \left\{ \left( \begin{array}{cc} \alpha^i \sigma^j & 0 \\ 0 & \alpha^{-i} \sigma^j \end{array} \right) : i, j \in \mathbb{Z} \right\}, \quad \tilde{D}_- = \left\{ \left( \begin{array}{cc} 0 & \alpha^i \sigma^j \\ \varepsilon \alpha^{-i} \sigma^j & 0 \end{array} \right) : i, j \in \mathbb{Z} \right\}.
\]

Let \( v = [1 \ \sigma]^T \). A straightforward computation shows that \( v \) is not centralized by any nonidentity matrix in \( \tilde{D}_+ \). If \( v \) is centralized by a matrix in \( \tilde{D}_- \), then we must have \( \sigma^2 \in \langle \alpha, -1 \rangle \). Hence \( (r - 1)/2 = |\langle \sigma^2 \rangle| \leq |\langle \alpha, -1 \rangle| \leq 2d \). Thus \( r - 1 \leq 4d \). If \( d < p - 1 \), then \( r - 1 \leq 4d \) implies that \( r - 1 \leq 2(p - 1) \). Since \( p \) divides \( r - 1 \) and \( r \) and \( p \) are odd, we must have \( 2p \leq r - 1 \), and so \( 2p \leq 2(p - 1) \), a contradiction. Thus \( d = p - 1 \) and so \( r - 1 \leq 4(p - 1) \) and \( p - 1 \) divides \( r - 1 \). Since \( p \) also divides \( r - 1 \), we have \( p(p - 1) \leq r - 1 \leq 4(p - 1) \). Thus \( p \leq 4 \), contradicting \( p > 3 \). Hence \( v \) lies in a regular \( \tilde{D} \)-orbit, as desired.

**Proof of Main Theorem.** Recall that Lemma 1.9 says that if \( (n, p) \neq (1, 3) \) and \( v \in V \) is a real vector, then \( V_{C_H(v)} \) is self-dual for all \( H \leq G \) such that \( (r, |H|) = 1 \).

If \( n = 1 \) and \( p = 2 \), then Lemma 2.1 says that \( V \) contains a real vector if \( r \notin \{5, 7, 13\} \). This establishes (a). If \( n = 1 \) and \( p = 3 \), then Lemma 2.2 says that there exists \( v \in V \) such that \( V_{C_G(v)} \) is self-dual, provided that \( r \notin \{7, 13\} \). If \( n = 1 \) and \( p \geq 5 \), then Lemmas 2.2 and 2.3 show that there exists \( v \in V \) such that \( V_{C_G(v)} \) is self-dual or that \( V \) contains a real vector. This establishes (b).

If \( n = 2 \) and \( p = 2 \), then Lemmas 2.4, 2.5, and 3.7 show that \( V \) contains a real vector, except possibly when \( r \notin \{3, 7\} \) and \( \varepsilon = - \). This establishes (c). If \( n = 3 \), \( p = 2 \), and \( \varepsilon = - \), then \( V \) contains a real vector if \( r \neq 7 \), by Lemmas 2.4 and 2.6.

Now we turn to the generic cases. If \( p = 2, n = 3, \) and \( \varepsilon = + \) or \( \varepsilon = 0 \), then \( V \) contains a real vector by Proposition 3.8 or Theorem 5.4. Together with the last sentence of the preceding paragraph, this establishes (d). If \( n \geq 2 \) and \( p \) is odd, or if \( p = 2, n \geq 3, \) and \( \varepsilon = 0 \), then \( V \) contains a real vector by Theorem 5.4. If \( p = 2, n \geq 4, \) and \( \varepsilon = - \), then Proposition 3.8 says that \( V \) contains a real vector provided
Lemma 6.1. A coprime $F[G]$-module $V$ is self-dual if and only if its Brauer character $\phi_V$ is real-valued. If $V$ and $V'$ are algebraically conjugate coprime $F[G]$-modules, then $V$ is self-dual if and only if $V'$ is self-dual.

Proof. The first statement is well known. The second statement follows from the first. Indeed $\phi_{V'} = \phi_V^\sigma$ for some $\sigma \in \text{Gal}(Q[G]/Q)$, because coprime power maps on the complex $|G|$th roots of unity lift to Galois automorphisms of $Q[G]$.

Lemma 6.2. Let $V$ be a coprime $F[G]$-module. Let $K/F$ be a field extension. Suppose that $K \otimes_F V$ is self-dual. Then $V$ is self-dual.

Proof. This follows from the first part of Lemma 6.1.

Lemma 6.3. Let $V$ be a faithful irreducible coprime $F[G]$-module and let $K = \text{End}_F[V]$. Then the irreducible constituents of $K \otimes_F V$ are absolutely irreducible, and if $U$ is any one of them, then the permutation actions of $G$ on the vectors of $V, U$, respectively are equivalent.

Proof. This is [RT] Lemma 10).

For much of the proof of Theorem 6.4, the main result of this section, we closely follow [RT] pp. 1154-1156.

Theorem 6.4. Let $V$ be a faithful irreducible coprime $F[G]$-module, where $F$ is a finite field and $G$ is solvable. Suppose that $\text{char}(F) > 13$. Then there exists $v \in V$ such that $V_{C_G(v)}$ is self-dual.

Proof. Suppose the result were true under the additional assumption that $V$ is an absolutely irreducible $F[G]$-module. We claim this would suffice to prove the theorem. Indeed let $K = \text{End}_F[V]$. By Lemma 6.3,

$$K \otimes_F V = U_1 \oplus \ldots \oplus U_t$$

where each $U_i$ is an absolutely irreducible $K[G]$-module. By [AS] 26.2], $U_i$ is algebraically conjugate to $U_i$ for $1 \leq i \leq t$. Moreover, each $U_i$ is a faithful $K[G]$-module. By our assumption, there exists $u \in U_1$ such that the restriction of $U_1$ to $C_G(u)$ is self-dual. By Lemma 6.3, $C_G(u) = C_G(v)$ for some $v \in V$. Now

$$K \otimes_F V_{C_G(v)} = (K \otimes_F V)_{C_G(v)} = (U_1)_{C_G(v)} \oplus \ldots \oplus (U_t)_{C_G(v)}$$
Thus we may assume that \( V \) is absolutely irreducible, so that \( F = K = \text{End}_{F[G]} V \). Suppose the theorem is false. Let \((G,V)\) be an absolutely irreducible counterexample to the theorem with \(|G| | V|\) minimal.

We claim that \( V \) is a primitive \( K[G]\)-module. To see this, suppose that \( V \) is induced from a \( K[H]\)-module \( W \), where \( H < G \). If \( L \) is any extension field of \( K \), then \((L \otimes_K W)^G = L \otimes_K V\). Thus the absolute irreducibility of \( V \) implies the absolute irreducibility of \( W \). Since \( H/C_H(W) \) acts faithfully on \( W \) and since \(|H/C_H(W)||W| < |G||V|\), there exists \( w \in W \) such that \( W_{C_H(w)} \) is self-dual. Let \( T \) be a transversal to \( H \) in \( G \). We have \( V = \bigoplus_{t \in T} W_t \). Let \( v = \sum_{t \in T} wt \). Since \( H \cap C_G(v) \) centralizes \( wt \), it follows that \( W^t |_{H \cap C_G(v)} \) is self-dual, though not necessarily faithful, for each \( t \in T \). Hence the last module, induced to \( C_G(v) \), is a self-dual \( C_G(v)\)-module. By Mackey’s Theorem, \( V_{C_G(v)} = (W^G)_{C_G(v)} \) is a direct sum of such induced modules. Hence \( V_{C_G(v)} \) is self-dual, contradicting the fact that \( (G,V) \) is a counterexample to our theorem. This proves the claim.

We claim next that whenever \( N < G \), all irreducible summands of \( V_N \) are absolutely irreducible. To see this, choose \( N < G \) maximal subject to \( V_N \) having an irreducible summand \( W \) which is not absolutely irreducible. Then \( N < G \). Let \( L = \text{End}_{K[N]} W \). Since \( V_N \) is homogeneous, \( \text{End}_{K[N]} V \) is a full matrix ring over \( L \), and so \( L = Z(\text{End}_{K[N]} V) \). As in [RT, p. 1155], the maximality of \( N \) implies that \( C_G(L) = N \), \( G/N \cong \text{Gal}(L/K) \), and \( V_N = W \).

Let \( W_1 \) be an irreducible summand of \( L \otimes_K W \). By Lemma 6.3, \(|W_1| = |W|\) and \( W_1 \) is absolutely irreducible. As in [RT, p. 1155], we have \( L \otimes_K V = W_1^G \). Thus \((W_1^G)^N = L \otimes_K W \). Hence if \( t \in G \), then \( W_t^1 \) is isomorphic to an irreducible summand of \( L \otimes_K W \), and so is algebraically conjugate to \( W_1 \).

Since \(|N| < |G|\), \(|W_1| = |W| = |V|\), and \( N \) acts faithfully on \( W_1 \) there exists \( w_1 \in W_1 \) such that \( W_1 |_{C_N(w_1)} \) is self-dual. By Lemma 6.3, there exists \( w \in W \) such that \( C_N(w_1) = C_N(w) \). Since \( V_N = W \), we may view \( w \) as a vector in \( V \). Let \( T \) be a transversal to \( NC_G(w) \) in \( G \). Mackey’s Theorem yields

\[
(L \otimes_K V)_{C_G(w)} = \left( W_1^G \right)_{C_G(w)} = \bigoplus_{t \in T} \left( W_1^t |_{N \cap C_G(w)} \right)_{C_G(w)} = \bigoplus_{t \in T} \left( W_1^t |_{C_N(w_1)} \right)_{C_G(w)}.
\]

As we remarked above, \( W_1 \) and \( W_t^1 \) are algebraically conjugate \( L[N]\)-modules. Hence each \( W_t^1 |_{C_N(w_1)} \) is algebraically conjugate to \( W_1 |_{C_N(w_1)} \), and hence is self-dual. It follows that \((L \otimes_K V)_{C_G(w)} = L \otimes_K V_{C_G(w)} \) is self-dual. By Lemma 6.2, \( V_{C_G(w)} \) is self-dual, contradicting the fact that \( (G,V) \) is a counterexample to our theorem. This proves the claim.

Now we claim that whenever \( N < G \) and \( N \not\in Z(G) \), \( V_N \) must be irreducible. To see this, suppose that \( N < G \), \( N \not\in Z(G) \), and \( V_N = eW \) with \( e > 1 \). By the previous step, \( W \) is an absolutely irreducible \( K[N]\)-module. Let \( \sigma : N \rightarrow GL(W) \) be a representation afforded by \( W \). For \( g \in G \), let \( \zeta_g \in GL(W) \) satisfy \( \zeta_g^{-1}(n \sigma) \zeta_g = (g^{-1}ng) \sigma \) for all \( n \in N \). Let \( T \) be a transversal to \( N \) in \( G \) with \( 1 \in T \) and arrange so that \( \zeta_1 = \text{id} \) and \( \zeta_m = \zeta_t(m \sigma) \) for all \( t \in T \) and \( m \in N \).
The absolute irreducibility of \( W \) implies that for \( g, h \in G \), there exists \( \alpha(h, g) \in K^* \) such that \( \zeta_{g h} = \alpha(h, g) \zeta_h \). Let \( \tilde{G} = \{(g, z) \mid g \in G, z \in K^*\} \) with product \( (g_1, z_1)(g_2, z_2) = (g_1g_2, \alpha(g_1, g_2) z_1 z_2) \). Let \( \tilde{Z} = \{(1, z) \mid z \in K^*\} \). Then \( K^* \cong \tilde{Z} \leq Z(\tilde{G}) \), and \( \tilde{G}/\tilde{Z} \cong G \). Let \( \tilde{N} = \{(n, 1) \mid n \in N\} \). Then \( N \cong \tilde{N} \triangleleft \tilde{G} \).

Endow \( W \) with a \( K[\tilde{G}] \)-module structure by defining \( \sigma : \tilde{G} \to GL(W) \) by \( (g, z) \sigma = z \zeta_g \). Identifying \( N \) and \( \tilde{N} \), we see that this extends the natural action of \( N \). In particular, \( W \) is an absolutely irreducible \( K[\tilde{G}] \)-module.

View \( V \) as a \( K[\tilde{G}] \)-module on which \( \tilde{Z} \) acts trivially. As in [RT, p. 1156], we have \( V = W \otimes_K X \) for some absolutely irreducible \( K[\tilde{G}] \)-module \( X \) on which \( \tilde{N} \) acts trivially. Note that if \( \tilde{z} \in \tilde{Z} \), there is a scalar \( \lambda \in K^* \) such that \( \tilde{z} \) acts as multiplication by \( \lambda \) on \( W \) and as multiplication by \( \lambda^{-1} \) on \( X \).

Since \( N \nsubseteq Z(G) \) and \( V_N = e W \), we have \( \dim_K W > 1 \). Thus \( \dim_K X < \dim_K V \). Since \( e > 1 \), we have \( \dim_K W < \dim_K V \). Since \( |\tilde{Z}| = |K| - 1 \), we have \( |G/C_G(X)| < |G|/|V| \) and \( |G/C_G(W)|/|W| < |G|/|V| \). Thus there exist vectors \( w \in W \) and \( x \in X \) such that \( \tilde{W}_{C_G(w)} \) and \( X_{C_G(x)} \) are self-dual.

Let \( v = w \otimes x \). We will show that \( V \) is a self-dual \( C_G(v) \)-module. To see this, let \( g \in C_G(v) \). Then \( (g, 1) \in C_G(v) \). Hence there is a scalar \( \lambda \in K^* \) such that \( w(g, 1) = \lambda w \) and \( x(g, 1) = \lambda^{-1} x \). From the description of the action of \( \tilde{Z} \) on \( X \) and \( W \) above, we see that there exists \( z \in \tilde{Z} \) such that \( (g, 1)z \) centralizes both \( w \) and \( x \). Let \( \tilde{g} = (g, 1)z \). Let \( \phi_V, \phi_W, \) and \( \phi_X \) be the Brauer characters of \( \tilde{G} \) afforded by \( V, W, \) and \( X \), respectively. Then \( \phi_V = \phi_W \phi_X \) and \( \tilde{Z} \leq \text{Ker} \phi_V \). Now \( \phi_W(\tilde{g}) \) is real, since \( \tilde{g} \in C_G(w) \). Similarly \( \phi_X(\tilde{g}) \) is real. Thus \( \phi_V(g, 1) = \phi_V(\tilde{g}) \) is real. It follows that \( \phi_V \), considered as a Brauer character of \( G \), has real restriction to \( C_G(v) \). Hence \( V_{C_G(v)} \) is self-dual. Thus our assumption that \( V_N = e W \) has led to a contradiction. It follows that \( V_N \) is irreducible whenever \( N \triangleleft G \) and \( N \nsubseteq Z(G) \).

Since \( V \) is an absolutely irreducible \( K[G] \)-module, \( Z(G) \) consists of scalar transformations on \( V \). We claim that \( F(G) = EZ(G) \) for extraspecial group \( E \); this will be the first time we use the assumption that \( G \) is solvable. To see the claim, note first that if \( A \) is a noncentral normal abelian subgroup of \( G \), then the previous two steps imply that \( V_A \) is absolutely irreducible, which implies that \( \dim_K V = 1 \). Since \( V \) is a faithful \( G \)-module, we have \( A \leq Z(G) = G \), a contradiction. Hence every normal abelian subgroup of \( G \) is central. It follows that \( O_p(G) \) is nonabelian for some prime \( p \). Of course \( p \) does not divide \( |V| \). Let \( P = O_p(G) \). Since \( V \) is a primitive \( G \)-module, the structure of \( P \) is given by Lemma 4.0. If \( p = 2 \), then, in the notation of Lemma 4.0, we have \( U \leq Z(G) \). Since \( U = C_T(U) \), we have \( U \leq T \leq Z(G) \). Hence \( T \leq Z(G) \) whether or not \( p = 2 \). Since \( P \) is nonabelian, Lemma 4.0 then implies that \( P \leq \left< E \right> Z(G) \) for an extraspecial subgroup \( E \) of \( P \). Since \( V_P \) is absolutely irreducible, we have \( \dim_K V = p^n \) and \( |P| = p^{2n+1} \), for some positive integer \( n \). It follows that \( P \) is the unique nonabelian Sylow subgroup of \( F(G) \) and that \( F(G) = EZ(G) \), as desired.

Thus \( \dim_K V = p^n \), \( F(G) = EZ(G) \), and \( E \) acts irreducibly on \( V \). We claim that \( G \) acts irreducibly on \( F(G)/Z(G) \). Indeed by [AW, I, 1.10], we may take \( E < G \); this requires solvability if \( p = 2 \). Then \( F(G)/Z(G) \) and \( E/Z(E) \) are isomorphic \( G\)-
modules. Furthermore, by [MW I.1.10 (iii)], \( E/Z(E) = E_1/Z(E) \times \ldots \times E_m/Z(E) \)
for chief factors \( E_i/Z(E) \) of \( G \) with \( [E_i, E_j] = 1 \) for \( 1 \leq i < j \leq m \). If \( m > 1 \), then
\( E_1 \) is a normal extraspecial subgroup of \( G \), of order \( p^{2n_1+1} \), where \( n_1 < n \). Previous steps of our proof imply that \( V_{E_1} \) is absolutely irreducible. Hence \( \dim_K V = p^{n_1} \), a contradiction. This proves the claim.

Let \( K = GF(r) \). Thus \( r \) is a power of prime greater than 13. We define the
“exceptional case” by the conditions that \( p = 2 \), \( r = 19 \), \( n \geq 4 \), and \( E \) is extraspecial
of minus type. If we are not in the exceptional case, let \( G = N_{GL(V)}(E) \) if \( p \) is
odd or if \( r \equiv 3(\text{mod} \ 4) \). If \( p = 2 \) and \( r \equiv 1(\text{mod} \ 4) \), let \( \bar{G} = N_{GL(V)}(E \ast Z_4) \).
Then \( G \leq N_{GL(V)}(E) \leq \bar{G} \). By the Main Theorem, there exists \( v \in V \) such that
\( V_{C_{G}(v)} \) is self-dual whenever \( H \leq \bar{G} \) and \( (|H|, |V|) = 1 \). Thus \( V_{C_{G}(v)} \) is self-dual,
contradicting the fact that \( (G, V) \) is a counterexample to Theorem 6.4. Hence we
are in the exceptional case.

To achieve the final contradiction, we resort to a standard counting argument.
For \( g \in G \), let \( f(g) = \dim C_{V}(g) / \dim V \). We have \( f(g) = 0 \) for \( g \in Z(G) \). If \( g \in G \setminus Z(G) \), then there exists \( e \in E \) such that \([g, e] \in Z(E)^\# \). Hence \( C_{V}(g^{-1}) \cap C_{V}(e^{-1}ge) \leq C_{V}([g, e]) = 0 \). It follows that \( f(g) \leq 1/2 \). If \( g \in G \setminus F(G) \), then \( g \) acts
nontrivially on \( E/Z(E) \) by [MW I.1.10]. Thus \([g, e] \in F(G) \setminus Z(G) \) for some \( e \in E \).
Since \( C_{V}(g^{-1}) \cap C_{V}(e^{-1}ge) \leq C_{V}([g, e]) \) and \( f([g, e]) \leq 1/2 \), we have \( f(g) \leq 3/4 \).

If \( z \in Z(G)^\# \) and \( g \in G \), then \( f(g) > 1/2 \) implies that \( f(gz) < 1/2 \). We now
estimate \( S = \sum_{g \in G^\#} |C_{V}(g)| \). If \( |S| < |V| \), then \( G \) must have a regular orbit on \( V \),
and so \( G \) can’t be a counterexample to our theorem. We have \( |C_{V}(g)| \leq |V|^{3/4} \) for
all \( g \in G^\# \). Moreover, for each \( g \in G \), we have \( \sum_{z \in Z(G)} |C_{V}(gz)| \leq |V|^{3/4} + 18 |V|^{1/2} \).

It follows that
\[
S < |G/Z(G)| \left( |V|^{3/4} + 18 |V|^{1/2} \right).
\]

Since \( n \geq 4 \), we have
\[
S < \left( 1 + 18/19^3 \right) |G/Z(G)| \left( |V|^{3/4} < 1.001 |G/Z(G)| \right) |V|^{3/4}.
\]

Now \( |G/Z(G)| = |G/F(G)| |E/Z(E)| \). Since \( G/F(G) \) acts faithfully and irreducibly on \( E/Z(E) \), the well known Palfy-Wolf bound [MW I.3.5] gives \( |G/F(G)| \leq |E/Z(E)|^{9/4} \). Hence
\[
|G/Z(G)| \leq |E/Z(E)|^{13/4} = 2^{13n/2}.
\]

Thus \( S < (1.001)^{2^{13n/2}} |V|^{3/4} \). It follows that if \( (1.001)^{2^{13n/2}} < |V|^{1/4} \), then \( G \)
has a regular orbit on \( V \).

If \( n \geq 5 \), then \( (1.001)^{2^{13n/2}} < 19^{2^{n}} = |V|^{1/4} \), so we may assume that \( n = 4 \).
Now \( G/F(G) \) is a subgroup of \( O^{-}(8, 2) \) and \( G/F(G) \) is irreducible on \( E/Z(E) \), the
natural module for \( O^{-}(8, 2) \). Hence \( G/F(G) \) is contained in a (not necessarily
solvable) maximal subgroup of \( O^{-}(8, 2) \) which is also irreducible on the
natural module. By [A p. 89], either \( G/F(G) \) is contained in a group of the form \( L_2(16):4 \)
or in a group of the form \( L_2(7) : 2 \). Since \( O_{2}(G/F(G)) = 1 \), in the former case we
see from [A p. 12] that \( |G/F(G)| \leq 136 \). In the latter case, solvability implies that
\( |G/F(G)| \leq 48 \). Now
\[
S < 1.001 |G/Z(G)| |V|^{3/4} < 1.001(136)2^{8}19^{12} < 19^{16} = |V|.
\]
Hence \( G \) has a regular orbit on \( V \), the final contradiction. \qed
Corollary 6.5. Let $G$ be a finite solvable group. Let $V$ be a faithful irreducible $G$-module over a finite field of characteristic $r$, where $r$ does not divide $|G|$ and $r \notin \{3, 5, 7, 11, 13\}$. Then $k(GV) \leq |V|$.

Proof. If $r = 2$, the result is known, as we remarked in the introduction to this paper. If $r > 13$, the result follows from Robinson’s result [R1, Theorem 1] and Theorem 6.4. □

Remark. Very probably a refinement of the counting argument at the end of the proof of Theorem 6.4 would eliminate 11 from the list of bad primes in the statement of Corollary 6.5. We forego this, however, in view of the already great length of this paper.

References


[He] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II, J. Algebra 93 (1985), 151-164. MR 86g:20016


THE EXTRASPECIAL CASE OF THE $k(GV)$ PROBLEM


License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use