TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 354, Number 1, Pages 287–333
S 0002-9947(01)02839-2
Article electronically published on August 29, 2001

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 [RT, 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

Received by the editors August 12, 1999 and, in revised form, January 2, 2001.
2000 *Mathematics Subject Classification.* Primary 20C20; Secondary 20C33, 20D06, 20E28.
Research of both authors partially supported by NSA grants.

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 ϕ be the Brauer character of G afforded by V. We show in Lemma 1.7 below that ϕ essentially lifts to an ordinary irreducible character χ of G. Thus we need only find $v \in V$ such that $\chi_{C_G(v)}$ 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 ε.

Then there exists a vector $v \in V$ such that $V_{C_H(v)}$ is self-dual for all $H \leq G$ such that $(r, |H|) = 1$, 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 $(r, |H|) = 1$ 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 ε respectively $0,\ -,\ 0$,
(g) $n = 1,\ p = 3,\ r \in \{7,\ 13\}$,
(h) $n = 2,\ p = 2,\ r \in \{3,\ 7\},\ \varepsilon = -$.

We can assume that r is odd in the Main Theorem because the $k(GV)$ conjecture has been proved [Gl1] 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 [Ri2] and Koehler and Pahlings [KP] 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 [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 $|V| = r^{2^n}$. We have $F(G) = EZ(G)$. Let $\overline{G} = G/F(G) \cong Sp(2n, 2)$. Thus $E/Z(E)$ is the natural module for $\overline{G}$.

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

Thanks to some results on cohomology, we can lift $\overline{L}$ 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 $|A| = |\overline{A}| = \left|\overline{A}^*\right| = |A^*|$, such that L normalizes A and A^*. Now $\dim C_V(A) = \dim C_V(A^*) = 1$. Let $W = \langle C_V(A), C_V(A^*)\rangle$. Then $\dim W = 2$, 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 is 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 $\overline{C_G(v)}$ has at most two orbits on the nonzero vectors of $E/Z(E)$. Hence we can't use [L1] 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 $V_{C_H(v)}$ 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. $E = E_0 * Z_4$, 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 ε to distinguish between Cases III and IV. For convenience, let $\varepsilon = 0$ in Cases I and II. We define $G = G^{\varepsilon}(n,p,r)$ 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 ϕ be the Brauer character of G afforded by V. If $v \in V, H \leq G$, and $(|H|, |V|) = 1$, then $V_{C_H(v)}$ is self-dual if and only if $\phi_{C_H(v)}$ is real-valued. Let $\theta \in Irr(E)$ be the restriction of ϕ to E. We will show in this section that θ extends to ordinary irreducible characters ψ and χ of K and G, respectively. We will work for the most part with χ or ψ, rather than with ϕ 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 ψ 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 $O_2(H) \cong E, H/O_2(H) \cong O^{\varepsilon}(2n,2), H/Z(H) \cong Aut(E)$, 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]. □

In Case I, more can be said. The following result is well known, except perhaps for the final statement; ψ_S is the well-known Weil character of $S \cong Sp(2n,p)$.

Lemma 1.2. *Suppose we are in Case I. Let $\theta \in Irr(E)$ be as above. There exists a split extension H of $C(E) \cong Sp(2n,p)$ by E. Let $S \cong Sp(2n,p)$ be a fixed complement to E in H. Then there exists $\Psi \in Irr(H)$ which extends θ, and Ψ_S is the sum of two irreducible characters ψ_1 and ψ_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 pth roots of unity, and $Q(\psi_1) = Q(\psi_2) = Q(\sqrt{\delta p})$, 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 ψ_1 and ψ_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 ψ_1 and ψ_2, see [Is1, p. 621]. If $(n,p) \neq (1,3)$, then $H = H'$. Thus θ 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 $SL(2,3) \times Z_3$ 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 $\chi \in Irr(G)$ with $Z(E) \nleq Ker\ \chi$. Then $\chi(x) = 0$ or $|\chi(x)|^2 = \left|C_{E/Z(E)}(x)\right|$. Moreover, if H and Ψ are as in Lemma 1.2, and $x \in S$, then $|\Psi(x)|^2 = \left|C_{E/Z(E)}(x)\right|$.*

Proof. All of this is well known. For the first statement, see [Gl2, Lemma 1.6]. For the second statement, see [Is1, 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 $PSL(2,q)$.

Proposition 1.4. *Let $n = 1$. There exists a subgroup $K = K^\varepsilon(1,p,r)$ of $N_{GL(V)}(E)$ such that $K/E \cong C_{Out(E)}(Z(E)) := C(E)$. 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 $r \equiv 1 (\mathrm{mod}\, 8)$. In Case III, we can take K to split over E when $r \equiv 7 (\mathrm{mod}\, 8)$; when $r \equiv 3 (\mathrm{mod}\, 8), GL(V)$ 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 $r \equiv 3 (\mathrm{mod}\, 8)$; when $r \equiv 7 (\mathrm{mod}\, 8), GL(V)$ 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 $S \cong SL(2,p)$. 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 ω_p is a primitive pth root of 1 in $\overline{F}$. Since p divides $r-1$, we have $\omega_p \in F$. Since Schur indices are trivial in positive characteristic, it follows that $GL(p,F) \cong GL(V)$ contains a subgroup isomorphic to H.

Next suppose we are in Case II and $r \equiv 1 (\mathrm{mod}\, 8)$. By [Hu, I.8.27], $PSL(2,r)$ contains a subgroup isomorphic to S_4. Since $SL(2,r)$ contains a unique involution, it follows that $SL(2,r)$ 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 $N \cap O_2(J) = Z(O_2(J))$. 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 $GL(V)$ contains a split extension of S_3 by $E = Q_8 * Z_4$.

Now suppose we are in Case II and $r \equiv 5(\mathrm{mod}\, 8)$. 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 $|Aut(E)|_3 = 3$. It follows that $|\langle T, S\rangle|$ divides $3\,|GL(2,r)|_2 = 96$. 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 $r \equiv 7(\mathrm{mod}\, 8)$, 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 $r \equiv 3(\mathrm{mod}\, 8)$, 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 [Go, 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 α is an involutory outer automorphism of D then the semidirect product $\langle\alpha\rangle D$ has class 3 and contains more than five involutions. Thus $\langle\alpha\rangle D \cong D_{16}$. 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 $r \equiv 7(\mathrm{mod}\, 8)$, 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 $r \equiv 3(\mathrm{mod}\, 8)$, 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 χ such that $\chi(1) = 2$ and $Q(\chi) = Q\left(\sqrt{-2}\right)$. 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 $\overline{GF(r)}$, whose $\overline{GF(r)}$-character $\overline{\chi}$ satisfies $\overline{\chi}(1) = 2$ and $(GF(r))(\overline{\chi}) = (GF(r))(\sqrt{-2})$. Since $r \equiv 3\,(\mathrm{mod}\, 8)$, $GF(r)$ 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 $r \equiv 7(\mathrm{mod}\, 8)$ 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 χ 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 α and α^3, for an element $\alpha \in \overline{GF(r)}$ of multiplicative order 8. But then $\left(\alpha+\alpha^3\right)^2 = -2$. Since $r \equiv 7 \,(\mathrm{mod}\, 8)\,, \sqrt{-2} \notin GF(r)$. 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 $K \cong K^{\varepsilon}(n,p,r)$ of $C(E)$ by E. Furthermore, there exists $\psi \in Irr(K)$ 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 $r \equiv 7 \,(\mathrm{mod}\, 8)\,,$ and $Q(\psi) = Q(\sqrt{-2})$ if $r \equiv 3 \,(\mathrm{mod}\, 8)\,.$*

Proof. First suppose $n = 1$. The existence of K was proved in Proposition 1.4. If we are in Case I, the existence of ψ and the fact that $Q(\psi) = Q_p$ follow from Lemma 1.2. If we are in Case II, then θ has three extensions to $K_0{:=}O^{3'}(K) * Z_4 \cong SL(2,3) * Z_4$. One of these extensions must be invariant in K and thus (since K/K_0 is cyclic) extends to K. Hence θ extends to an irreducible character of ψ of K. Of course $Q(\psi) \supseteq Q(\theta) = Q(i)$.

If we are in Case III and $r \equiv 7 \,(\mathrm{mod}\, 8)\,,$ 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 θ extends to $\psi \in Irr(K)$ and $Q\,(\psi) = Q\left(\sqrt{2}\right).$ If we are in Case III with $r \equiv 3 \,(\mathrm{mod}\, 8)\,,$ 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 θ extends to $\psi \in Irr(K)$ with $Q\,(\psi) = Q\left(\sqrt{-2}\right).$ If we are in Case IV and $r \equiv 3 \,(\mathrm{mod}\, 8)\,,$ then, as in the proof of Proposition 1.4, $K \cong GL(2,3)$ and θ extends to $\psi \in Irr(K)$ with $Q(\psi) = Q(\sqrt{-2})$. If we are in Case IV with $r \equiv 7 \,(\mathrm{mod}\, 8)\,,$ 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 θ has three extensions to $K' \cong SL(2,3)$, one of which must be rational valued and extendible to K. Let $\psi \in Irr(K)$ extend θ. Then $[Q\,(\psi) : Q] \le 2$. Restriction to a 2-Sylow subgroup of K shows that $\sqrt{2} \in Q\,(\psi)\,.$ Hence $Q\,(\psi) = Q\left(\sqrt{2}\right),$ as desired.

We assume from now on that $n \ge 2$. If we are in Case I, then the existence of K and ψ 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 $O_2(H) \cong E$, $Z(H) = Z(E)$, and $H/O_2(H) \cong Sp(4,2) \cong S_6$. Furthermore, Lemma 1.1 implies that H' has a faithful irreducible character α of degree 4, whose restriction θ to $O_2(H) \cong E$ is also faithful and irreducible. Since $H'/E \cong A_6$ has no nontrivial linear characters, α is the unique irreducible character of H' lying over θ. 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 $H' \le SL(4,r)$.

The restriction to E of $V{:=}\, GF(r)^4$ is tensor decomposable. We have $V = V_1 \otimes V_2$ and $E = E_1 * E_2$, where $E_1 \cong D_8 * Z_4$, $E_2 \cong D_8$, $E_1 \le GL\,(V_1) \otimes id.$ and $E_2 \le id. \otimes GL\,(V_2)\,.$ 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 $K_1 \le K(1,2,r)$. Write $K_1 = E_1\,\langle t \rangle\,,$ 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 $[\langle t \rangle\,, H']$ induces $Sp(4,2)' \cong A_6 \cong H'/E$ on $E/Z\,(E)\,,$ we have $[\langle t \rangle\,, H'] \le H'\,(Z\,(GL\,(4,r)))\,.$ Since t normalizes $H'Z(GL(4,r))$, t normalizes its derived group, $H'' = H'$. Let $K = \langle t \rangle\, H'$. Then $|K{:}H'| = 2$ and $K/E \cong Sp(4,2)$, so K can serve as $K\,(2,2,r)\,.$ Since $\alpha \in Irr\,(H')$ is the unique extension of $\theta \in Irr\,(E)$, α is invariant in K. Since K/H' is cyclic, α extends to $\psi \in Irr\,(K)$. 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 $H/E \cong Sp\,(2n, 2)$. Since $(H/E)' = H/E$, any faithful $\theta \in Irr\,(E)$ has a unique extension to H, whose field of values must be $Q\,(\theta) = Q\,(i)$. Since $GF\,(r)$ contains $\sqrt{-1}$, we view $E \leq H \leq GL(V)$, and there exists $\psi \in Irr(H)$ 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 $E_1 \cong E_2 \cong Q_8, E_1 \leq GL(V_1) \otimes id.$, and $E_2 \leq id. \otimes GL(V_2)$. Let $t \in GL\,(V_1 \otimes V_2)$ be the involution that sends $v_1 \otimes v_2$ to $v_2 \otimes v_1$ for all $v_1 \in V_1, v_2 \in V_2$. Let $K_1 \cong K_2 \cong K^-(1, 2, r)$, with $K_1 \leq GL(V_1) \otimes id., K_2 \leq id. \otimes GL(V_2)$, and $K_1^t = K_2$. Then $\langle t \rangle\,(K_1 * K_2)\,/E \cong O^{\,+}(4, 2)$, and so $\langle t \rangle\,(K_1 * K_2)$ can serve as $K^+(2, 2, r)$. Let θ_1 and θ_2 be the unique faithful irreducible characters of E_1 and E_2, respectively. Let $\psi_1 \in Irr(K_1) = Irr(K^-(1, 2, r))$ extend θ_1 as in the statement of this proposition. Then $\psi_2 := {\psi_1}^t$ extends θ_2, and $Q\,(\psi_1) = Q\,(\psi_2) = Q\left(\sqrt{-2}\right)$ if $r \equiv 3\,(\mathrm{mod}\,8)$, while $Q\,(\psi_1) = Q\,(\psi_2) = Q\left(\sqrt{2}\right)$ if $r \equiv 7\,(\mathrm{mod}\,8)$. By [Is2, Theorem 5.2], $\psi_1 \times \psi_2$, viewed as an irreducible character of $K_1 * K_2$, extends to a tensor induced irreducible character ψ of $K = \langle t \rangle\,(K_1 * K_2)$; indeed we have $\psi = (\psi_1 \times 1)^{\otimes \langle t \rangle (K_1 * K_2)}$, viewed as an irreducible character of K. By the formula for tensor induced characters, $Q\,(\psi) = Q(\psi_1) = Q\,(\psi_1 \times \psi_2) = Q\left(\sqrt{\pm 2}\right)$, 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 α which extends the unique faithful irreducible character θ of E. Since $(H'/E)' = H'/E$, it follows that α is rational-valued. Thus we may assume that $E \leq H' \leq GL(V)$. 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 $2^{2n-1}, E_1 \leq GL(V_1) \otimes id.$, and $E_2 \leq id. \otimes GL(V_2)$.

Let $E_1 \leq K_1 \leq GL(V_1) \otimes id.$ 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 $Sp(4, 2)$ case, t normalizes $H' = H''$ and $K := \langle t \rangle\,H'$ serves as $K^\varepsilon(n, p, r)$. Moreover K contains the subgroup $\langle t \rangle\,E = \langle t \rangle\,E_1 * E_2$. Since $|\langle t \rangle\,E{:}E| = 2$, θ extends to $\langle t \rangle\,E$. If $\psi_1 \in Irr\,(\langle t \rangle\,E_1) = Irr\,(K^+\,(1, 2, r))$ is as in the statement of this proposition, then ψ_1 has the same field of values as either of the two extensions of θ to $\langle t \rangle\,E$. By the $n = 1$ case of this proposition, this field of values is $Q\left(\sqrt{2}\right)$ if $r \equiv 7\,(\mathrm{mod}\,8)$ and $Q\left(\sqrt{-2}\right)$ if $r \equiv 3\,(\mathrm{mod}\,8)$.

Since $(H'/E)' = H'/E$, α is the unique extension of θ to H'. Hence α is invariant in K. Since K/H' is cyclic, α extends to $\psi \in Irr(K)$. 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 $Q(\psi) = Q\left(\sqrt{2}\right)$ if $r \equiv 7\,(\mathrm{mod}\,8)$ and $Q\,(\psi) = Q\left(\sqrt{-2}\right)$ if $r \equiv 3\,(\mathrm{mod}\,8)$, 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 ψ to K' is rational-valued.*

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

Lemma 1.7. *Let $G = N_{GL(V)}(E)$ as at the beginning of this section. Let $Z = Z(GL(V))$. 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 $\psi \in Irr(K)$ extend θ as in Proposition 1.5. Then there exists a unique $\chi \in Irr(G)$ such that $\chi_K = \psi$ and such that $\chi_{EZ} = \phi_{EZ}$. For* *such χ, 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 $\widehat{\theta} = \phi_{EZ}$. Then $\widehat{\theta}$ is an ordinary irreducible character of EZ which extends θ. Let λ be the unique and linear irreducible constituent of $\widehat{\theta}_Z$. Now G is the central product of K and Z, with $K \cap Z = Z(E)$. Since $\psi_{Z(E)} = \theta_{Z(E)}$ is a multiple of $\lambda_{Z(E)}$, there exists a unique $\chi \in Irr(G)$ such that $\chi_K = \psi$ and χ_Z is a multiple of λ. 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 $\chi(xz) = \theta(x)\lambda(z) = \widehat{\theta}(xz)$, so $\chi_{EZ} = \phi_{EZ}$.

Now let $\overline{V} = \overline{GF(r)} \otimes V$. Let $\rho : G \to GL\left(\overline{V}\right)$ be the natural inclusion and let $\sigma : G \to GL\left(\overline{V}\right)$ be a representation whose Brauer character is the restriction of χ to the r'-elements of G. Since $\chi_{EZ} = \phi_{EZ}$, we may, after replacing σ by an equivalent representation, assume that $\rho(x) = \sigma(x)$ for all $x \in EZ$. Let $\tau(x) = \rho(x) = \sigma(x)$ for $x \in EZ$. If $g \in G$ and $x \in EZ$, then $\rho(g^{-1}xg) = \sigma\left(g^{-1}xg\right)$, 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 $x \in EZ$. Thus $\rho(g) = \mu(g)\sigma(g)$ for a scalar $\mu(g)$. Clearly μ: $G \to \overline{GF(r)}^*$ is a homomorphism. Now $EZ \leq Ker\ \mu$ and $G/EZ \cong C(E)$. 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 $\chi_{C_G(v)}$ 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 $V_{C_H(v)}$ is self-dual.*

Proof. The Brauer character of $C_H(v)$ on V is $\phi_{C_H(v)}$. Since ϕ agrees with χ up to sign on the r'-elements of G by Lemma 1.7, it follows that $\phi_{C_H(v)}$ is real-valued. Hence $V_{C_H(v)}$ and its dual have the same Brauer character. Since $V_{C_H(v)}$ 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 ψ be as above. Suppose that $v \in V$ and $N_K\langle v\rangle = H \times Z(E)$ for a subgroup H of K. Suppose that ψ_H is real-valued and that $|H : C_H(v)| \leq 2$. Then v is a real vector. In particular, v is real if $N_K\langle v\rangle = H \times Z(E)$, ψ_H is real-valued, and H is almost perfect.*

Proof. By Definition 1.8, it suffices to show that $\chi_{C_G(v)}$ is real-valued. Let $Z = Z(GL(V))$. Then $N_G\langle v\rangle = HZ$.

If $H \leq C_G(v)$, then $C_G(v) = H$ and $\chi_{C_G(v)} = \chi_H = \psi_H$ is real-valued. If $|H{:}C_H(v)| = 2$, then $C_G(v)$ has index 2 in $H \times \langle -1\rangle$ and $C_G(v) \cong H$. Since χ extends ψ, the restriction of χ 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 $C_V(L')$ 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 $r \equiv 1 (\mathrm{mod}\, 4)$ and we are in Case II, or $r \equiv 3 (\mathrm{mod}\, 4)$ and we are in Case III or IV. We have $G = KZ$. If $r \equiv 3 (\mathrm{mod}\, 8)$ 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 $r \equiv 7 (\mathrm{mod}\, 8)$ 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 $N_G \langle v \rangle$ 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 $\{\overline{x}, \overline{x}^{-1}\}$ 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 $G_0 Z$, 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 $N_G \langle v \rangle$ is abelian for every $v \in V^\#$. Hence the image of $N_G \langle v \rangle$ in $\overline{G} \cong S_4$ is also abelian. Since the inverse image in G of $O_2\left(\overline{G}\right)$ is nonabelian, the image of $N_G \langle v \rangle$ 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 $N_G \langle v \rangle = Z \times C_G(v)$ 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 ω be an element of order 3 in the multiplicative group of $GF(r)$. Let

$$c = \begin{pmatrix} 0\,0\,1 \\ 1\,0\,0 \\ 0\,1\,0 \end{pmatrix}, \qquad d = \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix}.$$

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 (in homogeneous coordinates) of the transposes of the following twelve row vectors: $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, $[1,1,1]$, $[1,\omega,\omega^2]$, $[1,\omega^2,\omega]$, $[\omega,1,1]$, $[1,\omega,1]$, $[1,1,\omega]$, $[\omega^2,1,1]$, $[1,\omega^2,1]$, 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 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 $\det(t_0) = 1$, we have $\det(z) = 1$. 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 $Y = C_V(t_0) = [V,t]$. Then W and Y are irreducible S-modules of dimension 2 and 1, respectively, and $V = W \oplus Y$. We claim that $N_G\langle w\rangle \le SZ$ for all $\langle w\rangle \in P_1(W)\backslash\mathcal{B}$. To see this, suppose that $x \in N_G\langle w\rangle$ and $x \notin SZ$. Write $x = se$ with $s \in SZ$ and $e \in E\backslash Z(E)$. Then $[t_0,x] = [t_0,se] = [t_0,e] \in E\backslash Z(E)$. Hence a noncentral subgroup of E fixes $\langle w\rangle$, contradicting the fact that $\langle w\rangle \notin \mathcal{B}$. This proves the claim.

Since $W = C_V(t)$, the explicit list of vectors in $\mathcal{B}$ shows that $|\mathcal{B} \cap P_1(W)| = 4$. Let $\overline{S}$ be the image of S in $PGL(W)$, so that $\overline{S} \cong A_4$. As in the proof of Lemma 2.1, at most 6 points in $P_1(W)$ are fixed by involutions in $\overline{S}$ and at most 8 points in $P_1(W)$ are fixed by elements of order 3 in $\overline{S}$. Hence if $|P_1(W)| > 4+6+8 = 18$, there exists $\langle w\rangle \in P_1(W)$ such that $N_G\langle w\rangle \le Z(S)Z = \langle t\rangle Z$. It follows that $C_G\langle w\rangle = \langle t\rangle$ and so $V_{C_G(w)}$ is self-dual. Since r is odd, $r \equiv 1 \pmod 3$, 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 $|\mathcal{B}| \le 6 \cdot 5 = 30$. 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 α and β be the Brauer characters of S afforded by $[V,u]$ and $C_V(u)$, respectively. Thus $\alpha(1) = 2$ and $\beta(1) = 3$. Since $(10,r) = 1$, β 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 β is the restriction to $3'$-elements of an ordinary irreducible character of A_5. Since β is real-valued, it follows that elements of order 5 in S have distinct eigenvalues on $C_V(u)$. Similarly elements of order 3 in S have distinct eigenvalues if r is not a power of 3, and fix at most $r+1$ points in $P_1(C_V(u))$ if r is a power of 3. Let $\mathcal{C}$ be the set of all points in $P_1(C_V(u))$ fixed by some nonidentity element of $S/\langle u\rangle \cong A_5$. It follows that $|\mathcal{C}| \leq 6 \cdot 3 + 10(r+1) + 15(r+1+1) = 25r + 58$. Since $r \equiv 1 \pmod 5$, we have $r \geq 31$, and so we may choose $\langle v\rangle \in P_1(C_V(u)) - \mathcal{B} - \mathcal{C}$. Since $u \in N_K\langle v\rangle$ and $\langle v\rangle \notin \mathcal{B}$, we have $N_G\langle v\rangle \leq SE$, as above. Since $\langle v\rangle \notin \mathcal{C}$, we have $N_G\langle v\rangle = \langle u\rangle Z$ and so $C_G(v) = \langle u\rangle$. Thus $V_{C_G(v)}$ is self-dual. □

Lemma 2.3. *Suppose that* $n = 1$ *and* $p \geq 5$. *If* $p = 5$, *assume that* $r = 11$. *Then* V *contains a real vector.*

Proof. K is a semidirect product SE, with $S \cong SL(2,p)$ and E extraspecial of order p^3 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 $N = \langle T, x\rangle = N_S(T)$. 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 $\rho : K \to GL(\overline{V})$ be the natural inclusion, and let $\sigma{:}K \to GL(\overline{V})$ be a representation whose Brauer character is the restriction of ψ to the r'-elements of K. Since $\psi_E = \phi_E = \theta$ we may replace σ by an equivalent representation so that $\rho_E = \sigma_E$. It follows as in the proof of Lemma 1.7 that $\rho(x) = \mu(x)\sigma(x)$ for a linear character $\mu{:}K \to \overline{GF(r)}^*$, 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 ψ. By Lemma 1.2, ψ_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 $N_S(v) \geq N$. Since $\overline{V}$ is the reduction of a characteristic zero module that affords ψ, the final assertion of Lemma 1.2 implies that $N_S\langle v\rangle$ 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 $t^y = t[t,y]$. If $[t,y] \neq 1$, then $[t,y] \in E \backslash Z(E)$ 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 ψ_S are real on p'-elements (see [D, p. 228]), it follows that $\psi_{N_S\langle v\rangle}$ is real. Since $|N_S\langle v\rangle : C_S(v)| \leq 2$ and $N_K\langle v\rangle = N_S\langle v\rangle \times Z(E)$, 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 $N_K\langle v\rangle = N_S\langle v\rangle \times Z(E)$, and the restriction of ψ 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. $E_1 \leq GL(V_1) \otimes id.$ and $E_2 \leq id. \otimes GL(V_2)$. 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 $GL(V_1) \otimes id.$ and $id. \otimes GL(V_2)$ respectively, such that $K_1 \cong K_2 \cong K^-(1,2,r)$ and such that t interchanges K_1 and K_2.

Let $J = K_1K_2 \langle t \rangle$. Then J is isomorphic to $K^-(1,2,r)\ wr\ Z_2$, 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 $r \equiv 3 (\mathrm{mod}\, 4)$, 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 (with slight abuse of notation) $v_1 \in V_1$ and $v_2 = tv_1 \in V_2$ such that $N_{K_1} \langle v_1 \rangle \cong N_{K_2} \langle v_2 \rangle$ is a 2-group; this uses the hypothesis $r \neq 7$. Since $r \equiv 3 (\mathrm{mod}\, 4)$ and $E_1 \cong E_2 \cong Q_8$, we have $N_{E_i} \langle v_i \rangle = Z(E_i) = Z(E)$ for $i = 1, 2$.

Let $v = v_1 \otimes v_2$. Then $N_E \langle v \rangle = Z(E)$ and $N_K \langle v \rangle$ is a 2-group. Since $4 \nmid (r-1)$, this implies that $N_K \langle v \rangle = C_K \langle v \rangle \times Z(E)$. Now $C_K \langle v \rangle$ is isomorphic to a 2-subgroup of $K/E \cong S_3\ wr\ Z_2$. Hence $C_K \langle v \rangle$ has exponent at most 4. Since $Q(\psi) = Q\left(\sqrt{\pm 2}\right)$ by Proposition 1.5, it follows that ψ is rational on $C_K \langle v \rangle$. 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, $N_E \langle v \rangle = Z(E)$. Hence $C_K(v) \cong S_3\ wr\ Z_2$, and $N_K \langle v \rangle = C_K(v) \times Z(E)$. Since $S_3\ wr\ Z_2$ is a real group, ψ 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 an $S_3\ wr\ S_3$ subgroup and such that $N_E \langle v \rangle = Z(E)$. The image of $C_K(v)$ in $K/E \cong O^-(6,2)$ can't be all of $O^-(6,2)$, since $Aut(E)$ doesn't split over $Inn(E)$ 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 ${O^-}_2(6,2)$, we have $C_K(v) \cong S_3\ wr\ S_3$ and $N_K \langle v \rangle = C_K(v) \times Z(E)$. It follows as in the preceding paragraph that ψ 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 $E = E_0 * Z_4$, with $E_0 = E_1 * E_2$, 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 $J = K_1K_2 \langle t \rangle$, with $J/E \cong O^+(4,2) \cong S_3\ wr\ Z_2$, and $K_1 \cong K_2 \cong K^-(1,2,r) \cong$

$GL(2,3)$. 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 $N_E\langle v\rangle = Z(E)$. Hence $N_J\langle v\rangle = C_J(v) \times Z(E)$ and $C_J(v) \cong S_3\ wr\ Z_2$. Let $Z = Z(GL(V))$. Then $C_{EZ}(v) = 1$. Hence if $C_G(v)$ properly contains $C_J(v)$, then $C_G(v)EZ/EZ$ 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 $\chi_{C_G(v)}$ 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 $r \notin \{3,7\}$. If $r = 3$, then G contains a subgroup H of order $2^7 \cdot 5$ such there is no $v \in V$ for which $V_{C_H(v)}$ is self-dual.*

Proof. Suppose we can find $v \in V$ such that $3 \nmid |N_K\langle v\rangle|$ whenever $3|r-1$, such that $5 \nmid |N_K\langle v\rangle|$ whenever $5|r-1$, and such that $C_E(v) = 1$. Since K is a $\{2,3,5\}$-group, our assumptions imply that $N_K\langle v\rangle/C_K(v)$ is a 2-group. Since $Z(E) \leq N_K\langle v\rangle$ and $4 \nmid r-1$, we have $|N_K\langle v\rangle : C_K(v)| = 2$ and $N_K\langle v\rangle = C_K(v) \times Z(E)$. 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 ψ 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 $3 \nmid r-1$ and $n_5 = 0$ if $5 \nmid r-1$.

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 $N = K_1 * N_{K_2}\langle x\rangle$ 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 $\langle x\rangle$ 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 ψ to $K_1 * K_2$. Since this restriction is faithful and since $\psi(1) = 4$, ψ 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 ψ to K_2' equals 2α, where $\alpha \in Irr(K') = Irr(SL(2,3))$, $\alpha(1) = 2$, and α extends to K_2. The character table of $SL(2,3)$ shows that $\alpha(x) = -1$, and so $\psi(x) = -2$. The fixed point space of x on V has dimension $\left(\phi_{\langle x\rangle}, 1_{\langle x\rangle}\right)$. 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 $\left(\phi_{\langle x\rangle}, 1_{\langle x\rangle}\right) = (1/3)(4-2-2) = 0$. 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 $|K{:}N|\,(2(r+1)) = 80(r+1)$, 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 ϕ, or equivalently θ, 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 $\langle z\rangle = Z(E)$, then t and tz have the same eigenspaces. Hence $n_2 \le 5(2(r+1)) = 10(r+1)$.

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 $H_0 \ge E$ 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 $C_E(v) \le Z(C_H(v))$ and $C_H(v)/C_E(v) \cong Z_4$. See [MW, Theorem 6.8(a)]. It follows that $C_H(v) \cong Z_8$ 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 of $V_{C_H(v)}$ is $[V,\langle t\rangle]$, the -1-eigenspace of t. Suppose $C_H(v) = \langle x\rangle \times \langle t\rangle$, with $\langle x\rangle \cong Z_4$. Then $\langle t,x^2\rangle$ must centralize $C_V(t)$. Hence $\langle t,x^2\rangle$ acts faithfully on $[V,\langle t\rangle]$, an irreducible $C_H(v)$-module. This contradicts Schur's Lemma. It follows that $C_H(v) \cong Z_8$.

We claim that ϕ is not real-valued on $C_H(v)$. To see this, it suffices to show that η, the Brauer character of $C_H(v)$ afforded by $[V,\langle t\rangle]$, 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 η extends to a faithful irreducible Brauer character $\widehat{\eta}$ of S, such that $\widehat{\eta}(1) = 2$ and $\widehat{\eta}$ is an ordinary irreducible character of S. Thus η and $\widehat{\eta}$ take values $\pm\sqrt{-2}$ on elements of order 8. Hence η 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 $\overline{N}$ of $O^-(6,2)$. Since $\overline{N}/O_3(\overline{N})$ acts faithfully on $O_3(\overline{N})/Z(O_3(\overline{N})) \cong Z_3 \times Z_3$, we have $\overline{N}/O_3(\overline{N}) \cong GL(2,3)$ and $\left|\overline{N}{:}C_{\bar{N}}\left(Z\left(O_3\left(\overline{N}\right)\right)\right)\right| = 2$. Let $F \le K$ be a subgroup of order 27 whose image in $K/E \cong O^-(6,2)$ is $O_3(\overline{N})$. Let $\pi : K \to K/E$ be the natural homomorphism. Since FE is a normal subgroup of $\pi^{-1}(\overline{N})$, the Frattini argument implies that $\pi^{-1}(\overline{N}) = EN$, where N is the normalizer in $\pi^{-1}(\overline{N})$ of F. Since $Z(F)$ is fixed point free on $E/Z(E)$, we have $N \cap E = Z(E)$ and so $N/Z(E) \cong \pi^{-1}(\overline{N})/E = \overline{N}$. 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 μ of N with $\mu^2 = 1$. Since $Z(F)$ acts faithfully on V, η_F contains a faithful irreducible constituent ω, and $\omega(1) = 3$. Since ω and $\overline{\omega}$ are conjugate under N, η_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_N has an irreducible submodule X of dimension 6, and $X = [V, Z(F)]$. Let $Y = C_V(Z(F))$. Then $V_N = X \oplus Y$. Since N acts transitively on $F/Z(F)$ and on $Irr(F/Z(F))$, 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 ω 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 $N \backslash M$. 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 3×3 matrices of determinantal 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 $|F{:}C_F(u)| = 9$ involutions, $|C_L(u)| = 72$ and $C_L(u)/Z(F) \cong SL(2,3)$. By [A], $\Omega^-(6,2)$ contains no elements of order 18. Thus $C_L(u)$ contains no elements of order 9, and so $C_L(u) \backslash Z(F)$ contains an element of order 3. Since $O_2(C_L(u)) \cong Q_8, C_L(u)$ 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 β 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 $\alpha \in Irr(M)$ and $\alpha(1) = 3$. Now α_S has two irreducible constituents, of degrees 1 and 2. It follows that $\alpha(a) = 1$. Now if a centralizes Y, then $\eta(a) = \alpha(a) + \overline{\alpha(a)} + \beta(a) = 4$. By Lemma 1.3, this implies that $\left|C_{E/Z(E)}(a)\right| = 16$. 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 $\overline{a}$ of a in $K/E \cong O^-(6,2)$ also has order 4. Since $\overline{a}$ is a unipotent transformation on $E/Z(E) = GF(4)^3$, this implies that $\overline{a}$ has two Jordan blocks, of sizes 1 and 2. But then $\overline{a}^2 = 1$, 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 $N_S \langle y \rangle = Z(S)$. It follows that $|C_N(y){:}C_N(Y)| \leq 2$. Moreover $|C_N(y){:}F|$ equals 2 or 4 and $C_N(y)' = F$. We claim that $|N_K \langle y \rangle|_3 = 27$; i.e. we claim that $F \in Syl_3 (N_K \langle y \rangle)$. If not, let $\widehat{F} \leq N_K \langle y \rangle$ with $F \leq \widehat{F}$ and $\left|\widehat{F}\right| = 81 = |K|_3$. Then $\widehat{F} \leq N_K(F)$. Since $\overline{N}$ is maximal in $O^-(6,2)$ and since $N_E(F) = Z(E)$, we have $N_K(F) = N$. Hence $\widehat{F} \leq N_N \langle y \rangle$. Thus $\widehat{F} \leq O^{3'}(M) = SF$. Since F centralizes Y, it follows that $N_S \langle y \rangle$ contains a subgroup of order 3, contradicting $N_S \langle y \rangle = Z(S)$. This proves the claim. It follows that 3 does not divide $|N_K \langle y \rangle : C_K \langle y \rangle|$.

Let $\overline{H}$ be a maximal subgroup of $K/E \cong O^-(6,2)$ that contains the image $\overline{N_K \langle y \rangle}$ of $N_K \langle y \rangle$. Since F acts irreducibly on $E/Z(E)$, so does $\overline{H}$. By [A], $\overline{H}$ is either conjugate in $O^-(6,2)$ to $\overline{N}$, or $\overline{H} \cong S_3 \; wr \; S_3$. In particular, $\overline{H}$ and $N_K \langle y \rangle$ are $\{2,3\}$-groups. Thus $N_K \langle y \rangle / C_K \langle y \rangle$ is a cyclic 2-group whose order divides $r-1$.

Since $r \equiv 3 (\bmod 4)$, we have $|N_K\langle y\rangle : C_K(y)| = 2$ and $N_K\langle y\rangle = C_K(y) \times Z(E)$. Suppose that $\overline{H} \cong S_3\ wr\ S_3$. 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 $Q(\psi) = Q\left(\sqrt{\pm 2}\right)$, it follows that the restriction of ψ to $C_K(y)$ is rational-valued. Since $N_K\langle y\rangle = Z(E) \times C_K(y)$, 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 $F \leq N_K\langle y\rangle'$, 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 $N_K\langle y\rangle'$, like $\overline{H}'$, has Q_8 Sylow 2-subgroups. Then $\overline{N_K\langle y\rangle}$ acts as $SL(2,3)$ or $GL(2,3)$ on $O_3\left(\overline{H}\right)/Z\left(O_3\left(\overline{H}\right)\right)$. Since 27 is the exact power of 3 dividing $|N_K\langle y\rangle|$ and $\left|\overline{N_K\langle y\rangle}\right|$, this is impossible. Hence $\overline{N_K\langle y\rangle}'$ has cyclic 2-Sylow subgroups, and so $\overline{N_K\langle y\rangle}'$ has a normal 2-complement, which must be $\overline{F}$. Thus $\overline{N_K\langle y\rangle}$ is contained in $N_{K/E}\left(\overline{F}\right) = \overline{N}$. It follows that $N_K\langle y\rangle \leq NE$. Since $N_E\langle y\rangle = Z(E)$, and since $\overline{N_K\langle y\rangle}$ has a normal 3-Sylow subgroup, so does $N_K\langle y\rangle$. Since $F \in Syl_3\left(N_K\langle y\rangle\right)$, we have $N_K\langle y\rangle \leq N_{NE}(F) = N$. We conclude that $N_K\langle y\rangle = N_N\langle y\rangle = Z(E) \times C_N(y)$. Since $|C_N(y) : F|$ divides 4, the exponent of $C_N(y)$ divides 12. As above, this implies that the restriction of ψ to $C_N(y)$ is rational-valued. By Lemma 1.11, y is a real vector, as desired. □

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 $G/EZ \cong K/E \cong Sp(2n,p), Sp(2n,2)$, or $O^+(2n,2)$ respectively. Let $\overline{K} = K/E$ and let $\overline{E} = E/Z(E)$, so that $\overline{E}$ is the natural module for $\overline{K}$. Let $\overline{E} = \left\langle \overline{e}_1, \overline{f}_1 \right\rangle \oplus ... \oplus \left\langle \overline{e}_n, \overline{f}_n \right\rangle$ be a decomposition of $\overline{E}$ into a direct sum of mutually orthogonal hyperbolic planes. Let $\overline{A} = \langle \overline{e}_1, ..., \overline{e}_n \rangle$ and $\overline{A}^* = \left\langle \overline{f}_1, ..., \overline{f}_n \right\rangle$. Then $\overline{K}$ 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 $\left\{\overline{e}_1, ..., \overline{e}_n, \overline{f}_1, ..., \overline{f}_n\right\}$ of $\overline{E}$, $\overline{L}$ consists of all matrices of the form

$$\left[\begin{array}{c|c} g & \\ \hline & g^{-T} \end{array}\right]$$

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 dual $\overline{L}$-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 $G = N_{GL(V)}(E)$ 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, $H^2\left(\overline{L}, \overline{A}\right) = 0$, and so $H^2\left(\overline{L}, \overline{A}^*\right) = 0$. Since $\overline{E} = \overline{A} \oplus \overline{A}^*$, we have $H^2\left(\overline{L}, \overline{E}\right) = 0$. Hence K contains a subgroup $\widetilde{L}$ such that $\widetilde{L}E/E = \overline{L}$ and $\widetilde{L} \cap E = Z(E)$. By Lemma 3.1, the Schur multiplier of $\widetilde{L}/Z(E)$ is trivial and so $\widetilde{L} = \widetilde{L}' \times Z(E)$. Hence $L{:=}\widetilde{L}'$ 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, $H^1\left(L, \overline{A}\right) = 0$. 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 $e_iZ(E)/Z(E) = \overline{e}_i$ 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 $E_n * E_{6-n}$, 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 $V_6 = V_n \otimes V_{6-n}$, with $E_n \leq GL(V_n) \otimes id.$ and $E_{6-n} \leq id. \otimes GL(V_{6-n})$. 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 $G_n \otimes id.$ normalizes E_6 and centralizes E_{6-n}.

We claim that $G_n \otimes id.$ is the full centralizer of E_{6-n} in G. To see this, let $Z = Z(GL(V_6))$. Since $G/EZ \cong O^+(12, 2)$, the image in G/EZ of $C_G(E_{6-n})$ is contained in $(G_n \otimes id.)EZ/EZ \cong O^+(2n, 2)$. Thus

$$C_G(E_{6-n}) = (G_n \otimes id.)C_{EZ}(E_{6-n}) = (G_n \otimes id.)E_nZ = G_n \otimes id.$$

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 $\overline{L}_6, L_n$ corresponds to the set of all matrices of the form

$$\begin{bmatrix} \begin{array}{c|c} g & 0 \\ \hline 0 & I \end{array} & \\ & \begin{array}{c|c} g^{-T} & 0 \\ \hline 0 & I \end{array} \end{bmatrix}$$

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 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 $L_n = L_n' \leq (G_n \otimes id.)' \leq K_n \otimes id.$ for $n \geq 3$. From the natural isomorphism between G_n and $G_n \otimes id.$ 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 $E = E_0 Z_4$, 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 $r \not\equiv 3 (\mathrm{mod}\, 4)$, we can find $L \leq N_{GL(V)}(E_0) \leq N_{GL(V)}(E)$ such that $L \cong GL(n,2)$ and $L \cap E = L \cap E_0 = 1$, with $LE/E \cong LE_0/E_0 \cong L(EZ)/EZ = \overline{L}$. Furthermore, we can find elementary abelian L-invariant subgroups A and A^* of E_0, which map isomorphically onto $\overline{A}$ and $\overline{A}^*$. 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 $\overline{t} \in GL(\overline{E})$ to be the transformation that sends $\overline{e}_i$ to $\overline{f}_i$ and $\overline{f}_i$ to $-\overline{e}_i$ for $1 \leq i \leq n$. Clearly $\overline{t}$ lies in $Sp(2n,p)$, $Sp(2n,2)$ and $O^+(2n,2)$ in Cases I, II, and III, respectively, $\overline{t}$ interchanges $\overline{A}$ and $\overline{A}^*$, and $\overline{t}$ induces the inverse transpose automorphism of $\overline{L} \cong GL(n,p)$.

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

(a) $N_{\overline{K}}(\overline{L}) = N_{\bar{K}}(\overline{L}') = \langle \bar{t} \rangle \overline{L}$.

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

Proof. Once we establish (b), it will follow that $N_{\bar{K}}(\overline{L})$ and $N_{\bar{K}}\left(\overline{L}'\right)$ permute $\overline{A}$ and $\overline{A}^*$. Since $N_{\bar{K}}\left(\overline{A}\right) \cap N_{\bar{K}}(\overline{A}^*) = \overline{L}$, 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 $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ induces the inverse transpose automorphism of $SL(2,p)$, $\overline{A}$ and $\overline{A}^*$ are isomorphic modules for $\overline{L}' \cong SL(2,p)$. It remains to show that $\overline{E}$ contains $p+1$ irreducible $\overline{L}'$-modules, $p-1$ of which are nondegenerate. By [Go, p. 79], $\overline{E}$ contains exactly $p+1$ irreducible $\overline{L}'$-submodules.

In terms of the basis $\{\overline{e}_1, \overline{e}_2, \overline{f}_1, \overline{f}_2\}$ of $\overline{E}$, we have $\overline{A} = \langle \overline{e}_1, \overline{e}_2 \rangle$, and $\overline{A}^* = \langle \overline{f}_1, \overline{f}_2 \rangle$. Now let $\overline{u}_1$ and $\overline{u}_2$ be the standard generators of $\overline{L}'$:

$$\overline{u}_1 = \left[\begin{array}{cc|cc} 1 & 1 & & \\ 0 & 1 & & \\ \hline & & 1 & 0 \\ & & -1 & 1 \end{array}\right], \qquad \overline{u}_2 = \left[\begin{array}{cc|cc} 1 & 0 & & \\ 1 & 1 & & \\ \hline & & 1 & -1 \\ & & 0 & 1 \end{array}\right]$$

with respect to our hyperbolic basis of $\overline{E}$. Then $\overline{B} := \langle \overline{e}_1 + \overline{f}_2, \overline{e}_2 - \overline{f}_1 \rangle$ is nondegenerate and invariant under $\overline{u}_1$ and $\overline{u}_2$. Hence $\overline{B}$ is an irreducible $\overline{L}'$-submodule of $\overline{E}$. Let $\overline{L}_1$ be the stabilizer in $\overline{L}$ of $\overline{B}$. One can check that $\overline{L}_1 \cap Z\left(\overline{L}\right) = \langle -1 \rangle$. Since $\overline{L}'$ induces $SL(2,p) = Sp(2,p)$ on $\overline{B}$, we have $\overline{L}_1 = \overline{L}' C_{\bar{L}_1}\left(\overline{B}\right)$. But $C_{\bar{L}_1}\left(\overline{B}\right) \leq$

$\overline{L}_1 \cap Z(\overline{L}) = \langle -1 \rangle$. Thus $C_{\bar{L}_1}(\overline{B}) = 1$ and $\overline{L}_1 = \overline{L}'$. Hence $|\overline{L} : \overline{L}_1| = p-1$. Thus $\overline{B}$ belongs to an $\overline{L}$-orbit of size $p-1$, and so $\overline{E}$ contains $p-1$ irreducible nondegenerate $\overline{L}'$-submodules, as desired. ☐

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

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

It remains to find $t \in N_K(L)$ such that $tE/E = \bar{t}$. If p 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 $tE/E = \bar{t}$. 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 $sE/E = \bar{t}$. Then L and L^s are both complements to E in LE. By Lemma 3.1, $H^1(L, \overline{E}) = H^1(L, \overline{A}) \oplus H^1(L, \overline{A}^*) = 0$. Hence L and L^s are conjugate in $LE/Z(E)$. Thus there exists $u \in E$ such that $L^{su}Z(E) = LZ(E)$. Hence $L^{su} = (L^{su}Z(E))' = L$, and so $t = su$ satisfies $tE/E = \bar{t}$ and $t \in N_K(L)$.

Next suppose that $3 \leq n \leq 5$. Let $A_6 = \langle e_1, ..., e_6 \rangle$ and $A_6^* = \langle f_1, ..., f_6 \rangle$ 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 $V_6 = W_1 \otimes ... \otimes W_6$ with $\dim W_i = 2$ and $\langle e_i, f_i \rangle \leq id. \otimes ... \otimes GL(W_i) \otimes ... \otimes id. := H_i$ 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 $s = s_1...s_6 w$, where $s_i \in H_i$ interchanges $\overline{e}_i$ and $\overline{f}_i$ 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 $u = u_1...u_6$, where $u_i \in \langle e_i,\ f_i \rangle \leq H_i$, for $1 \leq i \leq 6$.

Let $V_n = W_1 \otimes ... \otimes W_n$ and $V_{6-n} = W_{n+1} \otimes ... \otimes W_6$. Let $E_n = \langle e_1, ..., e_n,\ f_1, ..., f_n \rangle$ and $E_{6-n} = \langle e_{n+1}, ..., e_6,\ f_{n+1}, ..., f_6 \rangle$. Then $E_6 = E_n * E_{6-n}$, 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

$$\begin{aligned} L_n &= L_6 \cap C_{G_6}(E_{6-n}) = (L_6 \cap C_{G_6}(E_{6-n}))^{s_1 \dots s_6 u_1 \dots u_6} \\ &= (L_6 \cap C_{G_6}(E_{6-n}))^{s_1 \dots s_6 u_1 \dots u_n} = (L_6 \cap C_{G_6}(E_{6-n}))^{s_1 \dots s_n u_1 \dots u_n s_{n+1} \dots s_6} \\ &= L_n^{s_1 \dots s_n u_1 \dots u_n s_{n+1} \dots s_6}. \end{aligned}$$

It follows that

$$L_n^{s_1 \dots s_n u_1 \dots u_n} = (L_6 \cap (G_n \otimes id.))^{(s_{n+1} \dots s_6)^{-1}} = L_n.$$

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

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 ϕ 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 $N_K(A) \leq N_K\langle w\rangle$. 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

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

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 $\overline{E}$. Hence $N_E\langle v\rangle Z(E)/Z(E)=\overline{A}_i$ for some $i\le 3$. Since $Z(E)\le N_E\langle v\rangle$, this implies that $N_E\langle v\rangle = B_i$. Hence $LA_i\le N_G\langle v\rangle$. 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 $S_3\cong\overline{L}\le\overline{C}$. Now $\overline{L}$ (and even $\overline{L}'$) is contained in a unique 3-Sylow normalizer $\overline{M}$ of S_6. We claim that if $\overline{C}\nleq\overline{M}$, then v is a real vector.

To see this, suppose first that $\overline{C}\nleq\overline{M}$ and $\overline{C}$ 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 so 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 $\overline{C}\le\overline{M}$. 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 $O_3(\overline{M})\le\overline{C}\le\overline{M}$. Let $T=O_3(C_G(v))\cong Z_3\times Z_3$, and let $\widetilde{M}$ be the inverse image in G of $\overline{M}\le G/EZ$. Let $M=N_{\widetilde{M}}(TO_3(Z))$. Since $TO_3(Z)\in Syl_3\left(\widetilde{M}\right)$, the Frattini argument gives $\widetilde{M}=EZM$. Since $C_{\overline{E}}\left(O_3(\overline{M})\right)$ $=C_{\overline{E}}(O_3(O^+(4,2)))=1$, we have $M\cap E\le C_E(O_3(M))=Z(E)$ and $M\cap EZ=Z$. Clearly $\langle L,T\rangle\le C_G(v)$.

We claim that M is the unique 3-Sylow normalizer of $\widetilde{M}$ that contains L. Indeed, if this were not the case, then $\langle L,L^e\rangle\le M$ for some $e\in E\backslash Z(E)$. Hence $[L,e]\le M$. Since 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 $M/TZ\cong D_8$ 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 $Irr(S)$ 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 $3\nmid r-1$, then $3|r^2-1$, and so S fixes exactly 4 points in $P_1\left(GF\left(r^2\right)\otimes V\right)$, 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 $|P_1(\langle w_1,w_2\rangle)|=r+1\ge 6$, it follows that we may choose $v\in W_0$ so that S does not fix v. Thus either $\overline{C}\nleq\overline{M}$ or $\overline{C}\le\overline{M}$ and $O_3\left(\overline{M}\right)\nleq\overline{C}$. Hence v is a real vector, as shown above. This completes the proof. □

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

Proof. First suppose we are in Case III with $n\ge 3$. 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, $N_K\langle w\rangle=N_K(A)$. Furthermore $N_K(A)E/E$ is a maximal parabolic of $K/E\cong O^+(2n,2)$ with Levi complement $\overline{L}\cong GL(n,2)$, 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 $N_K \langle w \rangle = N_K \langle w \rangle' Z(E)$. Since $C_G(w) \leq N_K \langle w \rangle' Z$, we have $C_G(w) = N_K \langle w \rangle' = K\,'$. Let $C = C_G(w)$. By Corollary 1.6, ψ_C is rational-valued. Hence χ_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 $E = E_1 * E_2$, where E_1 is extraspecial of plus type of order 2^{2n-1} and $E_2 \cong Q_8$. We have $\overline{E} = \overline{E}_1 \perp \overline{E}_2$ 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 $E_2 \leq id. \otimes GL(V_2)$. Furthermore K contains a central product $K_0 = K_1 * K_2$, where $K_1 \cong K^+(n-1, 2, r)$ and $K_2 \cong K^-(1, 2, r)$, with $K_1 \leq GL(V_1) \otimes id.$, and $K_2 \leq id. \otimes GL(V_2)$. Let $\overline{A}_1 \leq \overline{E}_1$ 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 θ 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 $P_1(V_2)$ 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 $N_{K_2} \langle w_2 \rangle = Z(K_2)$. 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 $[A_1^h, A_1] = 1$ for all $h \in H$. It follows that $\overline{A}_1^H$, the H-submodule of $\overline{E}$ generated by $\overline{A}_1$, must lie in $\overline{A}_1^{\perp} = \overline{A}_1 \perp \overline{E}_2$. Since $\overline{E}_2$ is anisotropic, it follows that $\overline{A}_1$ is the unique maximal totally singular subspace of $\overline{A}_1^H$. Hence H normalizes $\overline{A}_1$ and so H normalizes $A_1Z(E)$, the inverse image of $\overline{A}_1$ in E. Since $A_1 \leq H$ and $H \cap Z(E) = 1$, we have $A_1^h \leq A_1Z(E) \cap H = A_1$ for all $h \in H$. Thus $H \leq N_G(A_1)$, as claimed.

Let $N = N_G(A_1)$. Then $N \leq N_G\left(\overline{A}_1\right) = N_G(A_1Z(E))$. If $x \in N_G\left(\overline{A}_1\right)$, then A_1^x is one of the 2^{n-1} complements to $Z(E)$ in $A_1Z(E)$. Thus $N_G\left(\overline{A}_1\right) = E_1N$ and so the image $\overline{N}$ of N in $\overline{G} = G/EZ \cong O^-(2n, 2)$ is the maximal parabolic $N_{\overline{G}}\left(\overline{A}_1\right)$ 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 $C \lhd N$ 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 $\overline{L}_1 \times \overline{K}_2 \cong SL(n-1, 2) \times SL(2, 2)$ is a Levi complement of $\overline{N} = N_{\overline{G}}(\overline{A}_1)$. Thus $\overline{N} = (\overline{L}_1 \times \overline{K}_2)O_2(\overline{N})$. We have $[\overline{L}_1, O_2(\overline{N})] = O_2(\overline{N})$, e.g. by [GM, p. 553], and so $\overline{N}'' = \overline{N}''' = \overline{L}_1O_2\left(\overline{N}\right)$. 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 $\overline{L}_1O_2\left(\overline{N}\right)$. Thus $\overline{N} = \overline{C}\ \overline{K}_2$. Since $A_1 \leq C$ 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 $N_{K_2} \langle w_2 \rangle = Z(E)$, the centralizer in K_2Z of $w_1 \otimes w_2$ is trivial, and so $H = C$. Now

$$\overline{L}_1O_2\left(\overline{N}\right) \leq \overline{C} \leq \left(\overline{L}_1O_2\left(\overline{N}\right)\right)\left(\overline{C} \cap \overline{K}_2\right) = \overline{L}_1O_2\left(\overline{N}\right).$$

Thus $\overline{C} = \overline{L}_1O_2\left(\overline{N}\right)$. 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, ψ_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 $W_0 = W - \langle w \rangle - \langle w^* \rangle$.

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 $\overline{E}$ 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 $[L', AZ] = A$ or $[L', A^*Z] = A^*$. Thus 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 (Lemma 3.4) centralizes u and interchanges $\langle w \rangle$ and $\langle w^* \rangle$. Thus u acts as 1 or -1 on W and so $u \in N_G \langle v \rangle$. 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 $H \cap EZ = 1$, $\overline{H}$ is isomorphic to a subgroup of $N_{G/EZ}\left(\overline{A}\right) \cap N_{G/EZ}\left(\overline{A}^*\right) = \overline{L}$. 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 $\overline{P} = \overline{L}\ \overline{U}$, where $\overline{U} = O_p\left(\overline{P}\right)$. 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 $H_1 \leq \langle t \rangle LZ$. 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 $n^2 - \binom{n}{2}$. If $p = 2$, then $\overline{U}$ is an indecomposable module for $\overline{L} = \overline{L}'$ of composition length 2, with socle of dimension $n^2 - \binom{n}{2} - n$ 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 $n^2 - \binom{n}{2} \leq n$ in Case I. Since $n \geq 2$, this can't occur.

Suppose now that we are in Case II. If $\log_2 |O_2(H)| = n^2 - \binom{n}{2} - n$, 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 $\log_2 |O_2(H)| = n^2 - \binom{n}{2}$ and $O_2(H) \cap N_G(A) = 1$, since that would imply that $n^2 - \binom{n}{2} \leq n$, which is false. The remaining possibility is that $\log_2 |O_2(H)| = n^2 - \binom{n}{2}$ and $\log_2 |O_2(H) \cap N_G(A)| = n^2 - \binom{n}{2} - n$. 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 $H_1 \leq N_G(L)$. But then Lemma 3.4 implies that $H_1 \leq \langle t \rangle LZ$ 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 $\overline{A}^*$ nontrivially. Let $H_0 = H \cap N_G(\overline{A}) \cap N_G(\overline{A}^*)$. 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 $H_0 \cap EZ = 1$ and the image in G/EZ of $N_G(\overline{A}) \cap N_G(\overline{A}^*)$ is $\overline{L}$. Thus $H_0 \leq N_G(L)$ even when $p = 2$ and $n = 3$.

By Lemma 3.4, $N_G(L) = \langle t \rangle LZ$, and so $H_0 \leq LZ$. 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 $\overline{H}_0 \leq \overline{L}$ and $L' \leq H_0$ 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 $\overline{H}$ be the image of H in the symplectic group $\overline{G} := G/EZ \cong K/E$. In this section we use the classification of finite simple groups to show that $\overline{L}'$ has few overgroups in $\overline{G}$, and therefore $\overline{H} \leq N_G(\overline{L})$ 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]. □

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* $\overline{G}$ *be the symplectic group* G/EZ *and let* $\overline{H}$ *be the image of* H *in* $\overline{G}$. *Then* $H \cong \overline{H}$ *and* $H \leq N_G(L)$.

Proof. By Lemma 3.10, $H \cap EZ = 1$ and so $H \cong \overline{H}$. Suppose $H \nleq N_G(L)$. Since $\overline{A}$ and $\overline{A}^*$ are the unique nonzero proper $\overline{L}'$-submodules of $\overline{E}$, Lemma 3.10 implies that $\overline{H} \nleq N_{\overline{G}}(\overline{L})$ and that $\overline{H}$ acts irreducibly on $\overline{E}$. We claim that $\overline{H}$ acts primitively on $\overline{E}$. To see this, suppose that $\overline{E} = \overline{E}_1 \oplus ... \oplus \overline{E}_k$ is an imprimitivity decomposition for $\overline{H}$. We claim that $\overline{L}'$ has exactly $p+2$ orbits on the nonzero vectors of $\overline{E}$. Two of these orbits are $\overline{A} - \{0\}$ and $\overline{A}^* - \{0\}$. Let $\Omega = \overline{E} - \overline{A} - \overline{A}^*$. Then Ω is the direct product, as $\overline{L}'$-sets, of $\overline{A} - \{0\}$ and $\overline{A}^* - \{0\}$. Let π be the permutation character of $\overline{L}'$ on $\overline{A} - \{0\}$. Then the permutation character of $\overline{L}'$ on $\overline{A}^* - \{0\}$ is π^α, where α is the inverse transpose automorpism of $\overline{L}'$. Since g^{-1} is conjugate to g^α for all $g \in \overline{L}$, we have $\pi^\alpha = \pi$. Hence the number of orbits of $\overline{L}'$ on Ω is the inner product $(\pi\pi^\alpha, 1) = (\pi^2, 1)$. The last inner product equals (π, π), the rank of the transitive permutation group $\overline{L}'$ on $\overline{A} - \{0\}$. Matrix computation shows that the stabilizer in $\overline{L}'$ of $[100\cdots0]^T$ has p orbits on $\overline{A} - \{0\}$. Indeed, each of the $p-1$ scalar multiples of $[100\cdots0]^T$ constitutes an orbit of size one, and the remaining vectors in $\overline{A} - \{0\}$ form a single $\overline{L}'$-orbit. This proves the claim. It follows that $k \leq p+2$, since any two elements of $\overline{E} = \overline{E}_1 \oplus \cdots \oplus \overline{E}_k$ that lie in the same $\overline{L}'$-orbit have the same number of nonzero components. By [C], however, the minimal degree of a nontrivial permutation representation of $\overline{L}' \cong SL(n,p)$ is $(p^n-1)/(p-1)$. Since $k \leq p+2 < (p^n-1)/(p-1)$, it follows that $\overline{L}'$ acts trivially on $\{\overline{E}_1, \cdots, \overline{E}_k\}$. Since $\overline{A}$ and $\overline{A}^*$ are the unique nonzero proper $\overline{L}'$-submodules of $\overline{E}$, it follows that $k = 2$ and $\{\overline{E}_1,\ \overline{E}_2\} = \left\{\overline{A},\ \overline{A}^*\right\}$. Hence $\overline{H}$ permutes $\overline{A}$ and $\overline{A}^*$. By Lemma 3.10, $H \leq N_G(L)$, a contradiction.

We next show that $F(\overline{H}) = Z(F^*(\overline{H}))$. To see this, suppose that $\overline{Q}$ is a nonabelian Sylow subgroup of $F(\overline{H})$. Since $\overline{H}$ is primitive on $\overline{E}$, every characteristic abelian subgroup of $\overline{Q}$ is cyclic. We use the notation of Lemma 4.0. Thus $\overline{Q} = \overline{D}\ \overline{T}$. If $\overline{D} = \overline{Y}$ and $\overline{Q} = \overline{T}$, then $\overline{L}'$ would centralize $\overline{T}$ contradicting $\mathrm{End}_{\overline{L}'}\left(\overline{E}\right) \cong GF(p) \oplus GF(p)$. Hence $\overline{D}$ is extraspecial. Now $\overline{L}'$ acts nontrivially on $\overline{DU}/\overline{U} \cong \overline{D}/Z\left(\overline{D}\right)$. Let $\left|\overline{D}/Z(\overline{D})\right| = q^{2a}$ for a prime q and $a \geq 1$. Since $\overline{D}$ acts faithfully on $\overline{E}$, we have $q^a \leq \dim \overline{E} = 2n$. Since H is irreducible on $\overline{E}$, 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 $\overline{L}' \cong SL(n,p)$. By [LS], $p^{n-1} - 1 \leq 2a$. Since p is odd, we have $3^{n-1} \leq 2a+1 \leq 2\log_2(2n)+1$, contradicting $n \geq 3$. Thus $F(\overline{H})$ is abelian and so $F(\overline{H}) = Z(F^*(\overline{H}))$. Moreover $F(\overline{H})$ is cyclic, since $\overline{H}$ is primitive on $\overline{E}$.

Since $\mathrm{End}_{\overline{L}'}\left(\overline{E}\right) \cong GF(p) \oplus GF(p)$, it follows that $\overline{L}'$ centralizes no component of $\overline{H}$. Suppose that $\{\overline{S}_1, ..., \overline{S}_k\}$ is an $\overline{L}'$-orbit of components of $\overline{H}$, with $k > 1$. Since $(p^n-1)/(p-1)$ is the minimal degree of a nontrivial permutation representation of $\overline{L}'$, by [C], we have $k \geq (p^n-1)/(p-1)$. For some integer $m \geq k$, there exists components $\overline{S}_{k+1}, ..., \overline{S}_m$ of $\overline{H}$ such that $\overline{N}{:=}\overline{S}_1...\overline{S}_m$ is a normal subgroup of $\overline{H}$. By

Clifford's Theorem, $\overline{E}_{\overline{N}}$ is completely reducible. Let $\overline{X}$ be an irreducible summand of $\overline{E}_{\overline{N}}$. Since $\overline{E}$ is a primitive $\overline{H}$-module, $\overline{X}$ is a faithful $\overline{N}$-module. Now $\overline{X}$ may be viewed as an irreducible module for $\overline{S}_1 \times ... \times \overline{S}_m$, on which no $\overline{S}_i$ acts trivially. It follows from [As, 27.15] that $\dim \overline{X} \geq 2^m \geq 2^k \geq 2^{(p^n-1)/(p-1)} > 2n = \dim \overline{E}$, a contradiction.

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

Let $\overline{S}$ be the unique component of $\overline{H}$. Since $\overline{L}'$ induces inner automorphisms of $\overline{S}$, we have $\overline{L}' \leq \overline{S}C_{\overline{H}}\left(\overline{S}\right)$. Since $\overline{L}'$ also centralizes $Z\left(F^*\left(\overline{H}\right)\right)$, we have $\overline{L}' \leq \overline{S}C_{\overline{H}}\left(F^*\left(\overline{H}\right)\right) = \overline{S}F^*\left(\overline{H}\right) = F^*\left(\overline{H}\right)$. It follows that $\overline{L}' \leq \overline{S}$ and $\overline{S}$ is normal in $\overline{H}$. Since we are assuming that $\overline{H} \nleq N_{\overline{G}}(\overline{L}) = N_{\overline{G}}\left(\overline{L}'\right)$, it follows that $\overline{S} > \overline{L}', \overline{S}$ acts irreducibly on $\overline{E}$, and $\mathrm{End}_{\overline{S}}\left(\overline{E}\right) \cong GF(p)$. Moreover $Z\left(F^*\left(\overline{H}\right)\right) \leq \mathrm{End}_{\overline{S}}\left(\overline{E}\right)$. Thus $Z\left(F^*\left(\overline{H}\right)\right) \leq Z\left(\overline{H}\right)$. Finally $F^*\left(\overline{H}\right) = \overline{S}Z\left(\overline{H}\right)$ and so $\overline{H}/Z\left(\overline{H}\right) \leq Aut\left(\overline{S}\right)$.

Suppose $\overline{S}/Z(\overline{S})$ is an alternating group A_m. Since $n \geq 3$ and p is odd, the inclusion $\overline{L}' \leq \overline{S}$ 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 $\overline{S} \cong A_m$, then the minimal degree of a nontrivial representation of $\overline{S}$ in characteristic p is at least $m-2$; see [J]. If $\overline{S} \cong \widehat{A}_m$, then, by [W], the minimal degree of a nontrivial representation of $\overline{S}$ 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 $\overline{S}$ is at least $m-2$, whether $\overline{S} \cong A_m$ or $\overline{S} \cong \widehat{A}_m$. 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 $\overline{S}/Z\left(\overline{S}\right)$ can't be an alternating group.

Suppose next that $\overline{S}/Z(\overline{S})$ is a sporadic simple group. Now $|\overline{L}'|$ divides $\left|\overline{S}\right|$ and $\left|\overline{S}\right|$ divides $|Sp(2n,p)|$. If $\overline{S}/Z(\overline{S})$ is not the Monster group, then these two divisibility relations easily eliminate $\overline{S}$ as a possible overgroup of $\overline{L}'$. Indeed we first note that the p-part of $|SL(n,p)|$ must divide $\left|\overline{S}/Z\left(\overline{S}\right)\right|$; this severely limits the possibilities for n and p. If $\overline{S}/Z(\overline{S})$ is the Monster group, then $Z\left(\overline{S}\right) = 1$. By Lemma 3.10, $H \cap EZ = 1$, so that $H' \cong \overline{S}$. Lemma 3.10 also implies that H centralizes the central involution of u 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 $\overline{S}/Z(\overline{S})$ 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 ℓ 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 $2n$, [LS] implies that $(q^\ell - 1)/2 \leq 2n$; note that the Suzuki groups and the exceptions in [LS, p.419] can't have order divisible by $|SL(n,p)|$.

Let $\widehat{S}$ be the universal covering group of $\overline{S}/Z(\overline{S})$. Thus $\widehat{S}$ 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 ${}^2F_4$, then $\widehat{S}$ has a nontrivial irreducible representation in characteristic q of degree at most 5ℓ. Since $\widehat{S}$ 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 5ℓ. See [A, p. xvi]. From [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 [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 ${}^2F_4$. 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 $p^n - 1 \leq 248$ lead to $256 \leq 4n+1$ and $3^{n-1} \leq 249$, 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 ϕ is the restriction of χ to the r-regular elements of G. Since $\chi_K = \psi$ by Lemma 1.7, it follows that ϕ_K is the restriction of ψ to the r-regular elements of K. Thus $\phi_{H'}$ is the sum of two nonlinear irreducible Brauer characters, contradicting our assumption that $H \leq C_G(v)$.

Even if $\overline{S} \not\cong Sp(2n,p)$, H has a normal subgroup H_0 such that $H_0 \leq C_K(u)'$ and $H_0 \cong \overline{S}$. Now ψ_{H_0} has a nontrivial irreducible constituent α with $\alpha(1) \leq (p^n-1)/2$. Let ℓ be the untwisted rank of $\overline{S}/Z(\overline{S})$. If $\ell \geq n$, then [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 [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 [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 $GF(p^a)$, 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 $1 < d \leq 2n/d < 2n$. 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 [KL, 5.4.6]) that $\overline{E}$ is a $GF(p^a)[\overline{S}]$-module which is realized over no proper subfield of $GF(p^a)$. Since $End_{\bar{L}'}(\overline{E}) = GF(p) \oplus GF(p)$, it follows that $a = 1$. Thus $\overline{S}$ is defined over $GF(p)$.

Now suppose that $\overline{S}$ is an exceptional group of Lie type, necessarily defined over $GF(p)$. Define $n(\overline{S})$ to be 11, 11, 7, 7, 5, 5, or 4 for $\overline{S}$ 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 $p^{n(\overline{S})}-1$ does not divide $\left|\overline{S}\right|$. Hence $|SL(n,p)|$ does not divide $\left|\overline{S}\right|$ if $n \geq n\left(\overline{S}\right)$. It follows that $n < n\left(\overline{S}\right)$. Since H has a normal subgroup $H_0 \cong S$ as above, we can consider the restriction of ψ to H_0 and conclude that $\overline{S}$ has a nontrivial irreducible character of degree at most $\left(p^{n(\overline{S})-1}-1\right)/2$. In each of the seven cases, this quantity is less than the minimal degree of a cross-characteristic projective representation of $\overline{S}/Z(\overline{S})$, by [LS] or [SZ]. This contradiction shows that $\overline{S}/Z(\overline{S})$ can't be an exceptional group.

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

The inequalities $\ell<n$ and $d=\ell+1>n$ show that $\overline{S}$ is not of type A_ℓ. If $\overline{S}$ 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 $|\overline{L}'|$ doesn't divide $|\overline{S}|$, a contradiction.

Thus $\overline{S}/Z(\overline{S})$ is a simple orthogonal or symplectic group defined over $GF(p)$. We may assume that $\overline{S}$ is not of type D_2 or ${}^2D_2$. Since $|SL(3,p)|$ doesn't divide $|PSp(4,p)|$, it follows that 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, $2n \leq \left((n+1)^2/2\right)-1 \leq \left(d^2/2\right)-1$.

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

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

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 $\dim \overline{E}=2n<2d<d(d-1)/2-2$.

Third, spin modules of small dimension exist when $\overline{S}/Z(\overline{S})$ is a simple orthogonal group. If $\overline{S}$ 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 $\overline{S}$ is of type B_ℓ or D_ℓ. Since p is odd and $\overline{S}$ is absolutely irreducible on $\overline{E}$, $\overline{S}$ can't preserve both a symplectic and a symmetric bilinear form on $\overline{E}$. Hence we need only consider those spin representations which embed a spin group of type B_ℓ or D_ℓ into $Sp(2n,p)$, rather than into $\Omega^+(2n,p)$. Now [KL, 5.4.9] tells us that if $\overline{S}$ is of type B_ℓ, then $\ell \equiv 1 \pmod 4$ or $\ell \equiv 2 \pmod 4$, and the spin module has dimension 2^ℓ. If $\overline{S}$ is of type D_ℓ, then $\ell \equiv 2 \pmod 4$, and the spin module has dimension $2^{\ell-1}$. Since $\ell \geq 3$, it follows that ℓ is at least 5 in the B_ℓ case and at least 6 in the D_ℓ case. Thus in the B_ℓ 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_ℓ case, we have $n = 2^{\ell-2}$, $d = 2\ell$, and $\ell \geq 6$, again contradicting $d > n$.

We conclude that $\overline{S}$ 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 $\overline{L}'$-submodules. Two of these, namely $\langle \overline{e}_1, \overline{e}_2 \rangle$ and $\langle \overline{f}_1, \overline{f}_2 \rangle$, are totally isotropic. In addition, there are $(p-1)/2$ pairs of mutually orthogonal nondegenerate irreducible $\overline{L}'$-submodules; one such pair is $\langle \overline{e}_1 + \overline{f}_2, \overline{e}_2 - \overline{f}_1 \rangle$ and $\langle \overline{e}_2 + \overline{f}_1, \overline{f}_2 - \overline{e}_1 \rangle$. Now $\overline{G} = G/EZ \cong Sp(4,p)$ contains a subgroup $M \cong SL(2,p)\ wr\ Z_2$ which permutes the two nondegerate subspaces above. Clearly $\overline{L}'$ 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 $C_G(u) = C_G(u)'Z$, where $C_G(u)' \cong Sp(4,p)$ 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 $M \leq C_G(u)'$ 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.*

	Order	*Number of Classes*	*Restrictions*
(1)	$p^2(p^2-1)^2$	1	-
(2)	$p^2(p^4-1)$	1	-
(3)	$p(p^2-1)(p-1)$	1	$p > 3$
(4)	$p(p^2-1)(p+1)$	1	$p > 3$
(5)	$p(p^2-1)/2$	1	$p > 7$
(6)	1920	2	$p \equiv \pm 1 (\bmod 8)$
	960	1	$p \equiv \pm 3 (\bmod 8)$
(7)	720	2	$p \equiv \pm 1 (\bmod 12)$
	360	1	$p \equiv \pm 5 (\bmod 12)$, $p \neq 7$
	2520	1	$p = 7$

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 $\Omega_5(p)$. 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 $L' \leq$*

$H \leq C_G(v)$. 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)* $\overline{H} \cong SL(2,p^2), \left|\overline{H} : \overline{H}'\right| \leq 2,$ *and* $\overline{H}'$ *preserves a* $GF(p^2)$*-vector space structure on* $\overline{E}$.
- *(b)* $p = 5$ *and* $\overline{H} \cong \widehat{A}_6 \cong SL(2,9)$.
- *(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* $\overline{H} \cong \widehat{A}_7$.
- *(e)* $p = 3$ *and* $\overline{H}$ *is isomorphic to a subgroup of* $\widehat{S}_6$.

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 $\overline{G}$-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 $\overline{L}$-conjugates of $\overline{M}$. It follows that, for some $x \in L$, H is contained in $M^xEZ \cap C_G(u) = M^xZ$. 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 $|\overline{X}:\overline{X}'| = 2$ 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 $\overline{H} \leq N_{\overline{G}}(\overline{L}') = N_{\overline{G}}(\overline{L})$. 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 $\overline{L}' \leq \overline{H} \leq \overline{X}$, then $\overline{H} \leq N_{\overline{G}}(\overline{L}')$. 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_5 by an elementary abelian group of order 16. There is a basis $\mathcal{B} = \{v_1, v_2, v_3, v_4, v_5\}$ of $V_5(p)$ such that $O_2(\overline{X}/Z(\overline{G}))$ acts diagonally on $V_5(p)$ with respect to $\mathcal{B}$, and a complement to $O_2(\overline{X}/Z(\overline{G}))$ in $\overline{X}/Z(\overline{G})$ permutes the vectors in $\mathcal{B}$. 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 $\overline{u} \in \overline{X}$ has order 3, then 8 divides $|C_{\overline{G}}(\overline{u})|$.

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

$$\left(\begin{array}{c|c} \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} & \\ \hline & \begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix} \end{array}\right)$$

Comparing with [Sr, p. 489], we see that $\overline{u}_1$ belongs to class A_{31} of [Sr] and so $|C_{\overline{G}}(\overline{u}_1)| = 2 \cdot 3^3 \cdot (3-1)$, which is not divisible by 8. We remark that the image of $\overline{u}_1$ in $\Omega_5(p)$ 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. [L1, 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 $\overline{X} \cong \widehat{A}_7$. Since $SL(2,7)$ is a maximal subgroup of $\widehat{A}_7$, 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 $\overline{X} \cong \widehat{A}_6 \cong SL(2,9)$, 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 $n \geq 3$ 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.*

(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 and* $n=3$.

Proof. First we show that $\overline{L}$ 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 $\overline{L}$-orbits. Let $\Omega = P_1(\overline{E}) - P_1(\overline{A}) - P_1(\overline{A}^*)$. Then Ω is the direct product, as $\overline{L}$-sets, of $P_1(\overline{A})$ and $P_1(\overline{A}^*)$. Let π be the permutation character of $\overline{L}$ on $P_1(\overline{A})$. Then the permutation character of $\overline{L}$ on $P_1(\overline{A}^*)$ is π^α, where α is the inverse transpose automorphism of $\overline{L}$. Since g^{-1} is conjugate to g^α for all $g \in \overline{L}$, we have $\pi^\alpha = \pi$. Hence the number of orbits of $\overline{L}$ on Ω is the inner product $(\pi^2, 1)$. Since $\overline{L}$ is doubly transitive on $P_1(\overline{A})$, we have $(\pi^2,1) = (\pi,\pi) = 2$. Hence Ω is the union of two $\overline{L}$-orbits, namely $\mathcal{S} = \{\overline{a}+\overline{b}{:}\overline{a} \in P_1(\overline{A}), \overline{b} \in P_1(\overline{A}^*)$, and $(\overline{a},\overline{b}) = 0\}$ and $\mathcal{N} = \{\overline{a}+\overline{b} : \overline{a} \in P_1(\overline{A}), \overline{b} \in P_1(\overline{A}^*)$, and $(\overline{a},\overline{b}) = 1\}$. We have $\left|P_1(\overline{A})\right| = \left|P_1(\overline{A}^*)\right| = 2^n - 1$, while $|\mathcal{S}| = (2^n-1)(2^{n-1}-1)$ and $|\mathcal{N}| = (2^n-1)2^{n-1}$.

By Lemma 3.10, $H \cong \overline{H}$. We may assume that $H \not\leq N_G(L)$, 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 $\overline{A}^h = (\overline{A}^h \cap \overline{A}) \cup (\overline{A}^h \cap \overline{A}^*)$. Since $\overline{A}^h \cap \overline{A}$ and $\overline{A}^h \cap \overline{A}^*$ are subspaces of $\overline{A}^h$, it follows that $\overline{A}^h = \overline{A}$ or $\overline{A}^h = \overline{A}^*$. 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 $End_{\overline{L}}(\overline{E}) \cong GF(2) \oplus GF(2)$. 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 [L1] has determined all primitive rank 3 affine groups. The doubly transitive affine groups were determined earlier by Hering [He].

First suppose that $\overline{H}$ is transitive on $\overline{E}$. By Hering's Theorem [L1, 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, $SL(2n,2) \lhd \overline{H}$, $Sp(2n,2) \lhd \overline{H}$, or $\left|\overline{E}\right| = 2^6$ and $G_2(2)' \lhd \overline{H}$. 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 $\left|\overline{E}\right|$ 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 [L1], 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 $\overline{E}_{\overline{L}} = \overline{A} \oplus \overline{A}^*$, 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 $\overline{H}\le N_{\overline{G}}(\overline{L})$, and so $\overline{H}$ would fix or permute $\overline{A}$ and $\overline{A}^*$, 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 $\overline{L}$ centalizes 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 $End_{F^*(\overline{H})}(\overline{E})$ is a field which properly contains $GF(2)$. Then $\overline{L}\le F^*(\overline{H})$, contradicting $End_{\overline{L}}(\overline{E})=GF(2)\oplus GF(2)$, and so $\overline{H}\,\overline{E}$ does not belong to class (A6). In class (A7), the point stabilizer normalizes a group of the form $\Omega^{\varepsilon}(2a,q)$, which has $\overline{E}$ as its natural module ([L1, p. 483]). Since $End_{\overline{L}}(\overline{E})=GF(2)\oplus GF(2)$, 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 $n\neq 4$, 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 $\overline{L}\cong GL(3,2)$ 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 $\overline{H}\le Aut(\overline{S})$. 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). □

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 χ be as in Section 1. Since $\chi(1) = 8$ and $O_2(H) \nleq Ker\ \chi$, it follows that $\chi_H = 1_H + \alpha$, where $\alpha \in Irr(H)$ and $\alpha(1) = 7$. Let λ be a linear constituent of $\alpha_{O_2(H)}$. Then $\alpha = \omega^H$, where $\omega \in Irr(I_H(\lambda))$ is an extension of λ. Now $I_H(\lambda)/Ker\lambda \cong S_4 \times Z_2$, and so ω^2 is the principal character of $I_H(\lambda)$. It follows from Clifford's Theorem that α and χ_H are real-valued. By Definition 1.8, v is a real vector. Thus $v \in W_1$, a contradiction.

Let $N = N_K\langle v\rangle$. Since $L = L' \leq N \leq N_G\langle v\rangle = C_G(v)Z = NZ$, 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 $\overline{N} = \overline{C_G(v)}$.

Suppose first that $\overline{N}$ falls under conclusion (a) of Proposition 4.4. Then $\overline{N} \cong Sp(2n,2)$. Since $N_G\langle v\rangle = C_G(v)Z$, 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 $K_0 \cong K^+(n,2,r)$. Thus $K_0/E_0 \cong O^+(2n,2)$. Clearly $K_0 \leq G$. Up to conjugacy in G/EZ, we have $\overline{N} = \overline{K}_0$ or $\overline{N} = \overline{K}'_0$, so we assume without loss of generality that $\overline{N} = \overline{K}_0$ or $\overline{N} = \overline{K}'_0$. 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 $(N \cap K_0)E_0 = K_0$ 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 $Aut(E_0)' \cong K_0'/Z(E_0)$ 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 $\overline{N}$ is A_9, S_9, or $Sp(6,2)$. We saw above that $\overline{N} = \overline{C_G(v)}$, and Proposition 4.4 implies that $C_G(v) \cong \overline{C_G(v)}$. 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 χ 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 α irreducible of degree 7, or $\chi_H = \lambda + \mu + \beta$, with $\lambda(1) = \mu(1) = 1$ and β 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 χ 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 χ_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 $\overline{G} \cong Sp(6,2)$ contains a unique conjugacy class of $PSU(3,3)$ subgroups, and a unique conjugacy class of $G_2(2)$ subgroups. Let $\overline{L} \leq \overline{M}' \leq \overline{M}$, 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 $\left|N_{\overline{G}}(\overline{L}){:}(\overline{L})\right| = 2$. Thus $N_{\overline{G}}(\overline{L}) \leq \overline{M}$. If $\overline{L} \leq (\overline{M}')^x$ for some $x \in \overline{G}$, then the $\overline{M}'$-conjugacy of $\overline{L}$ and $(\overline{L})^{x^{-1}}$ implies that $x^{-1}y \in N_{\overline{G}}(\overline{L})$ 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 $\overline{G}$ containing $\overline{L}$.

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 $\widetilde{M}/Z(E)$. 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 $\left|H^1(\overline{M}', \overline{E})\right| = 2$ and there are exactly two conjugacy classes of complements to $E/Z(E)$ in $\widetilde{M}/Z(E)$; 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 $e \in E\backslash Z(E)$, 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 $\widetilde{M}/Z(E)$ yields at most one overgroup of L in $\widetilde{M}$ 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 $\widetilde{M}$, 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 $P_1(W)$, 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 $\langle {N_i}', A\rangle = \widetilde{M}$ centralizes w, contradicting Lemma 3.6 (b). We conclude that each N_i fixes at most one point in $P_1(W)$. 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, $H \cong \overline{H}$ and either H is contained in one of the $(p-1)/2$ distinct L-conjugates of MZ, or $\overline{H}$ 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 $\overline{L}' \leq \overline{H} \leq \overline{M} \cong SL(2,p)\ wr\ Z_2$. By Lemma 3.10, $\overline{H} \nleq N_{\overline{G}}(\overline{L}')$. Since $p \geq 5$, $\overline{L}'/Z(\overline{L}')$ is a maximal subgroup of $\overline{M}'/Z(\overline{M}') \cong PSL(2,p) \times PSL(2,p)$. Since

$\overline{H} \cap \overline{M}' > \overline{L}'$, it follows that $\overline{H} \cap \overline{M}' = \overline{M}'$. Thus $\overline{H} = \overline{M}$ or $\overline{H} = \overline{M}'$. Hence $M' \leq H \leq MZ$, with $M' \cong SL(2,p) \times SL(2,p)$.

To derive a contradiction, it will suffice to show that M' stabilizes no one-dimensional subspace of V. The subgroup $M'E$ of K is a central product $K_1 * K_2$, where, for $i = 1, 2$, K_i is a semidirect product S_iE_i with $S_i \cong SL(2,p)$ and E_i extraspecial of order p^3 and exponent p. We take $M' = S_1 \times S_2$. Let $\pi : K_1 \times K_2 \rightarrow M'E$ be the natural surjection. Let $\theta \in \mathrm{Irr}(E)$ be as in Section 1, and let λ be the unique and linear constituent of $\theta_{Z(E)}$. Composing λ with π gives a linear character $\lambda_1 \times \lambda_2$ of $Z(K_1) \times Z(K_2) = Z(K_1 \times K_2)$. For $i = 1, 2$, let θ_i be the unique irreducible character of E_i lying over λ_i and let $\psi_i \in Irr(K_i)$ be the unique extension of θ_i to K_i. Now $\psi_1 \times \psi_2$, viewed as an irreducible character of $K_1 * K_2 = M'E$, lies over λ. 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 λ. But if $\psi \in \mathrm{Irr}(K)$ is as in Section 1, then $\psi_{M'E}$ is irreducible of degree p^2 and also lies over λ. 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 ϕ 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 μ of G with $EZ \leq Ker\mu$ such that $\chi(g) = \mu(g)\phi(g)$ for all $g \in G$ of order prime to r. Since $\chi_K = \psi$ and $M' = M''$, it follows that the Brauer character of M' afforded by V coincides with the restriction of ψ to the r'-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. [As, 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 $SL(2,p^2) \cong H' \leq C_K(u)' \cong Sp(4,p)$, where u is the central involution of L. By Lemma 1.2, the restriction of ψ to $C_K(u)$ has two irreducible constituents, ψ_1 and ψ_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', ψ_1 restricts irreducibly to H'. We claim that ψ_2 also restricts irreducibly to H'. Indeed, if this were not the case, then $(\psi_2)_{H'} = 1_{H'} + \alpha$, where $\alpha \in Irr(H')$ 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 ψ_1 and ψ_2 restrict irreducibly to H'. By [GMS], $(\psi_1)_{H'}$ 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 $H = H' \leq C_K(u)' \cong Sp(4,5)$. Since $p \equiv 1 (\mathrm{mod}\ 4)$, Lemma 1.2 implies that $\psi_{H'}$ is real-valued. We have $N_K\langle v\rangle = H' \times Z(E) = C_K(v) \times Z(E)$. 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 ψ_H is real-valued. Now $H \cong \widehat{A}_7$, 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 $v \in W_0 \backslash W_1$ and let $H \cong C_G(v)$ as above. Then $H \cong \overline{H}$. By Proposition 4.3, either $H \leq MZ$ or $\overline{H}$ is contained in an $\widehat{S}_6$ subgroup of $\overline{G}$; note that conclusion (a) is subsumed under (e) when $p = 3$.

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

Hence $\overline{H}$ is not solvable, and so $\overline{H}/Z(\overline{G})$ is isomorphic to $A_5, S_5, A_6,$ or S_6 . If $\overline{H}/Z(\overline{G})$ is isomorphic to A_5 or A_6 , then $H \cong \overline{H}$ is isomorphic to $\widehat{A}_5$ or $\widehat{A}_6$. Since these two groups are real, χ_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 $\overline{L}'/Z(\overline{G})$ 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 $\overline{L}/Z(\overline{G})$ 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 $\overline{L}/Z(\overline{G}) \cong A_4$ has no faithful representation of degree 2 over $GF(3)$, the dimension of $[O_2(\overline{L}'/Z(\overline{G})), V_5(3)]$ must be at least 3. Hence $O_2(\overline{L}'/Z(\overline{G}))$ centralizes at most a two-dimensional subspace of $V_5(3)$. Since $\overline{L}$ stabilizes two maximal totally isotropic subspaces of $\overline{E}$, the Atlas tells us that $\overline{L}/Z(\overline{G})$ fixes two isotropic points in $P_1(V_5(3))$. Hence $\overline{L}'/Z(\overline{G})$ centralizes two isotropic one-dimensional subspaces of $V_5(3)$. The containment $\overline{L}'/Z(\overline{G}) \leq \overline{M}/Z(\overline{G}) \cong O^+(4,3)$ shows that $\overline{L}'/Z(\overline{G}) = O^{3'}(\overline{L}'/Z(\overline{G}))$ centralizes a one-dimensional plus type subspace of $V_5(3)$. Now if $\overline{L}'/Z(\overline{G})$ fixes, or equivalently centralizes, more than one one-dimensional minus type subspace of $V_5(3)$, then the centralizer of $\overline{L}'/Z(\overline{G})$ 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 $\overline{L}'$ 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 $\overline{L}'$ in $\overline{G}$, and let S be the inverse image in $C_K(u)'$ of the unique $\widehat{S}_6$ overgroup of $\overline{L}'$ in $\overline{G}$. If $\overline{H} = \overline{S}_i$ 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 $\overline{H} \cong \widehat{S}_6$, then $H' = S'$. Again S' fixes at most one point in $P_1(W)$, and if $\langle v \rangle \in P_1(W)$ is fixed by S', then S_1' and S_2' fix $\langle v \rangle$ and no other point in $P_1(W)$. We conclude that the set of points in $P_1(W)$ fixed by some $\widehat{S}_5$ or $\widehat{S}_6$ overgroup of L' has cardinality at most 2.

The remaining possibility is that $H \le MZ$. Then $\overline{L}' \le \overline{H} \le \overline{M} \cong SL(2,3)\ wr\ Z_2$. Let $\overline{B} \cong SL(2,3) \times SL(2,3)$ be the base group of this wreath product. Then $\overline{L}'$ is diagonally embedded in $\overline{B}$.

We claim that $\overline{B} \cap O_2(\overline{H}) = O_2(\overline{M}) \cong Q_8 \times Q_8$. 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 $\overline{B} \cap O_2(\overline{H}) \le O_2(\overline{L})Z(\overline{M}) \cong Q_8 \times Z_2$. 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 $\left|\overline{R}\right| = 9$. Let $\overline{C}$ be the centralizer in $\overline{R}$ of $\overline{B} \cap O_2(\overline{H})$. Then $\overline{C}$ is the centralizer in $\overline{R}$ of $O_2(\overline{L}')/Z(\overline{L}')$, and so $\left|\overline{C}\right| = 3$. Thus $\overline{C} \nleq \overline{L}'$ and $\overline{C}$ centralizes $\left\langle \overline{T}, O_2(\overline{L}')\right\rangle = L'$. Thus $L' \times \overline{C} \le N_{\overline{G}}(L') = N_{\overline{G}}(\overline{L})$. By Lemma 3.3, however, $\left|N_{\overline{G}}(\overline{L})\right| = 96$, a contradiction. Hence $\overline{R} = \overline{T}$ and 3 divides $\left|\overline{H}\right|$ to the first power. It follows that $\overline{H} \cap \overline{B} = L'$ or $\overline{H} \cap \overline{B} \cong L' \times Z_2$. Thus $L' = O^{3'}(\overline{H} \cap \overline{B})$ is normal in $\overline{H}$ and so $\overline{H} \le N_{\overline{G}}(L') = N_{\overline{G}}(\overline{L}\ )$. As above, this implies via Lemma 3.10 that $H \le N_G(L)$, contradicting $v \notin W_1$. This establishes our claim.

Since $O_2(\overline{M}) \le \overline{H}$, we have $O_2(\overline{M}){=}[\overline{L}', O_2(\overline{M})] \le \overline{H}'$. Since $H \le MZ$, we have $H' \le M$. It follows that $O_2(M) \le H'Z \cap M = H'(Z \cap M) = H'$. Let $B \cong SL(2,3) \times SL(2,3)$ be the inverse image in $C_K(u)' \cong Sp(4,3)$ of $\overline{B}$, the base group of $\overline{M}$. Let ϕ 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 ϕ_B is an ordinary character of B, since $(6,r) = 1$. It follows as when $p > 3$ that ϕ_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 $O_2(M){=}O_2(B) \le H'$. It follows that $O_2(M)$ 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 $L' \le H \le MZ$ and $O_2(M) \le H$.

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 $n \ge 2$ or in Case II with $n \ge 3$. 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 $t^2 \in N_E(L) = Z(E)$. If $r \equiv 1 (\mathrm{mod}\, 8)$, then, after multiplying t by a scalar if necessary, we may take t to have order 2. If $r \equiv 5 (\mathrm{mod}\, 8)$, 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 $C = C_N(W)$, so that $L' \le C$. 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 $Z \le Z(G)$ 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 $\gcd(p-1, r-1)$.

Let $-1 \in Z(G)$ be the scalar of order 2. We claim that $C \le L \times \langle -1\rangle$. 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 α 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 α and as α^{-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 χ_C is real-valued . By Corollary 3.5, χ_L is real-valued. Since $-1 \in Z(G)$, it follows that $\chi_{L \times \langle -1 \rangle}$ is real-valued. Thus χ_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 $m \leq 2$. 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 $\langle t, x \rangle$ acts diagonally on W with respect to the basis $\{w + w^*, w - w^*\}$. If $v \in W - \langle w + w^* \rangle - \langle w - w^* \rangle$, 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 $v \in W_1 - \langle w + w^* \rangle - \langle w - w^* \rangle$. 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 $W_1 - \langle w + w^* \rangle - \langle w - w^* \rangle$ 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 $W_1 - \langle w + w^* \rangle - \langle w - w^* \rangle$ 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 χ is real on $C_G(v) - L$, while Corollary 3.5 shows that χ 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 $C_G(v) \cong \overline{C_G(v)} \cong PSU(3,3)$. However $C_N(v) \cong \overline{C_N(v)}$ 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 ± 1 on W. Thus $|D : Z| = 2$, $r \equiv 3 (\bmod 4)$, 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 $r \equiv 1 (\bmod 4)$, 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 $r \equiv 5 (\bmod 8)$ 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 $D = \langle t, x\rangle Z$ 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 εw^* and w^* to w for $\varepsilon \in \{\pm 1\}$. Since t inverts x and x has order dividing d, we have

$$t = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}, \qquad x = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}$$

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

$$\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}, \quad \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} \sigma & 0 \\ 0 & \sigma \end{pmatrix}.$$

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

Write $\widetilde{D} = \widetilde{D}_+ \cup \widetilde{D}_-$, where

$$\widetilde{D}_+ = \left\{ \begin{pmatrix} \alpha^i\sigma^j & 0 \\ 0 & \alpha^{-i}\sigma^j \end{pmatrix} : i, j \in \mathbf{Z} \right\}, \quad \widetilde{D}_- = \left\{ \begin{pmatrix} 0 & \alpha^i\sigma^j \\ \varepsilon\alpha^{-i}\sigma^j & 0 \end{pmatrix} : i, j \in \mathbf{Z} \right\}.$$

Let $v = [1\ \sigma]^T$. A straightforward computation shows that v is not centralized by any nonidentity matrix in $\widetilde{D}_+$. If v is centralized by a matrix in $\widetilde{D}_-$, then we must have $\sigma^2 \in \langle \alpha, -1\rangle$. Hence $(r-1)/2 = \left|\langle\sigma^2\rangle\right| \leq |\langle\alpha, -1\rangle| \leq 2d$. 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 p and r 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 $\widetilde{D}$-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 $r \in \{3, 7\}$ 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 that $r \notin \{3, 7, 11, 19\}$. If $p = 2, n \geq 4$, and $\varepsilon = +$, then V contains a real vector by Proposition 3.8. This establishes (e).

Assertion (f) follows from Lemma 2.1; here $H = G$. Assertion (g) follows from [RT, p. 1150] for $r = 7$ and from computations with GAP for $r = 13$; in both cases $H = G$. Assertion (h) follows from Lemma 2.5 for $r = 3$, and from computations with GAP for $r = 7$. When $r = 3$ we have $|H| = 2^7 \cdot 5$; when $r = 7$, $H = G$. □

6. Solvable groups

Let G be a finite solvable group, F a finite field, and V a finite-dimensional $F[G]$-module with $(|G|, |V|) = 1$. Our goal in this section is to show that if G acts irreducibly on V and $\mathrm{char}(F) > 13$, then there exists $v \in V$ such that $V_{C_G(v)}$ is self-dual.

Our first three lemmas do not require solvability.

Lemma 6.1. *A coprime $F[G]$-module V is self-dual if and only if its Brauer character ϕ_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 $\sigma \in Gal(Q_{|G|}/Q)$, 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 $K = End_{F[G]}V$. 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 $char(F) > 13$. 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 $K = End_{F[G]}V$. By Lemma 6.3,

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

where each U_i is an absolutely irreducible $K[G]$-module. By [As, 26.2], U_i is algebraically conjugate to U_1 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

$$K \otimes_F V_{C_G(v)} = (K \otimes_F V)_{C_G(v)} = (U_1)_{C_G(v)} \oplus ... \oplus (U_t)_{C_G(v)}$$

Since the U_i are algebraically conjugate, Lemma 6.1 implies that each summand is self-dual. Hence $K \otimes V_{C_G(v)}$ is self-dual. By Lemma 6.2, $V_{C_G(v)}$ is self-dual. This proves our claim.

Thus we may assume that V is absolutely irreducible, so that $F = K = End_{F[G]}V$. 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 $V = \bigoplus_{t\in T} Wt$. Let $v = \sum_{t\in T} wt$. Since $H^t \cap C_G(v)$ centralizes wt, it follows that $W^t|_{H^t\cap C_G(v)}$ 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 $N \lhd G$, all irreducible summands of V_N are absolutely irreducible. To see this, choose $N \lhd G$ maximal subject to V_N having an irreducible summand W which is not absolutely irreducible. Then $N < G$. Let $L = End_{K[N]}W$. Since V_N is homogeneous, $End_{K[N]}V$ is a full matrix ring over L, and so $L = Z(End_{K[N]}V)$. As in [RT, p. 1155], the maximality of N implies that $C_G(L) = N$, $G/N \cong Gal(L/K)$, 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 $\left({W_1}^G\right)_N = L \otimes_K W$. Hence if $t \in G$, then ${W_1}^t$ 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 $W_1|_{C_N(\mathrm{w}_1)}$ 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

$$\begin{aligned}(L \otimes_K V)_{C_G(w)} &= ({W_1}^G)_{C_G(w)} \\ &= \bigoplus_{t\in T} \left({W_1}^t|_{N^t\cap C_G(w)}\right)^{C_G(w)} = \bigoplus_{t\in T} \left({W_1}^t|_{C_N(w_1)}\right)^{C_G(w)} .\end{aligned}$$

As we remarked above, W_1 and ${W_1}^t$ are algebraically conjugate $L[N]$-modules. Hence each ${W_1}^t|_{C_N(w_1)}$ 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 $N \lhd G$ and $N \not\leq Z(G)$, V_N must be irreducible. To see this, suppose that $N \lhd G$, $N \not\leq Z(G)$, and $V_N = eW$ with $e > 1$. By the previous step, W is an absolutely irreducible $K[N]$-module. Let $\sigma : N \to GL(W)$ be a representation afforded by W. For $g \in G$, let $\zeta_g \in GL(W)$ satisfy $\zeta_g^{-1}(n\sigma)\zeta_g = \left(g^{-1}ng\right)\sigma$, for all $n \in N$. Let T be a transversal to N in G with $1 \in T$ and arrange so that $\zeta_1 = id.$ and $\zeta_{tm} = \zeta_t(m\sigma)$ for all $t \in T$ and $m \in N$.

The absolute irreducibility of W implies that for $g, h \in G$, there exists $\alpha(g,h) \in K^{\#}$ such that $\zeta_g \zeta_h = \alpha(g,h)\zeta_{gh}$. Let $\widetilde{G} = \left\{(g,z)\,|g \in G, z \in K^{\#}\right\}$ with product $(g_1,z_1)\,(g_2,z_2) = (g_1 g_2, \alpha\,(g_1,g_2)\,z_1 z_2)$. Let $\widetilde{Z} = \left\{(1,z)\,|z \in K^{\#}\right\}$. Then $K^{\#} \cong \widetilde{Z} \leq Z(\widetilde{G})$, and $\widetilde{G}/\widetilde{Z} \cong G$. Let $\widetilde{N} = \{(n,1)\,|n \in N\}$. Then $N \cong \widetilde{N} \lhd \widetilde{G}$.

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

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

Since $N \nleq Z(G)$ and $V_N = eW$, 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 $|\widetilde{Z}| = |K| - 1$, we have $\left|\widetilde{G}/C_{\widetilde{G}}(X)\right|\,|X| < |G|\,|V|$ and $\left|\widetilde{G}/C_{\widetilde{G}}(W)\right|\,|W| < |G|\,|V|$. Thus there exist vectors $w \in W$ and $x \in X$ such that $W_{C_{\widetilde{G}}(w)}$ and $X_{C_{\widetilde{G}}(x)}$ 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 $(g,1) \in C_{\widetilde{G}}(v)$. 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 $\widetilde{Z}$ on X and W above, we see that there exists $\widetilde{z} \in \widetilde{Z}$ such that $(g,1)\widetilde{z}$ centralizes both w and x. Let $\widetilde{g} = (g,1)\widetilde{z}$. Let ϕ_V, ϕ_W, and ϕ_X be the Brauer characters of $\widetilde{G}$ afforded by V, W, and X, respectively. Then $\phi_V = \phi_W \phi_X$ and $\widetilde{Z} \leq Ker\ \phi_V$. Now $\phi_W(\widetilde{g})$ is real, since $\widetilde{g} \in C_{\widetilde{G}}(w)$. Similarly $\phi_X(\widetilde{g})$ is real. Thus $\phi_V(g,1) = \phi_V(\widetilde{g})$ is real. It follows that ϕ_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 $V_N = eW$ with $e > 1$ has led to a contradiction. It follows that V_N is irreducible whenever $N \lhd G$ and $N \nleq Z(G)$.

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 $P \leq EZ(G)$ 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 [MW, I, 1.10], we may take $E \lhd G$; 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)], $E/Z(E) = E_1/Z(E) \times ... \times E_m/Z(E)$ 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 $\widehat{G} = N_{GL(V)}(E)$ if p is odd or if $r \equiv 3 (\operatorname{mod} 4)$. If $p = 2$ and $r \equiv 1 (\operatorname{mod} 4)$, let $\widehat{G} = N_{GL(V)}(E * Z_4)$. Then $G \leq N_{GL(V)}(E) \leq \widehat{G}$. By the Main Theorem, there exists $v \in V$ such that $V_{C_H(v)}$ is self-dual whenever $H \leq \widehat{G}$ 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 $g \in F(G) \backslash Z(G)$, 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 $g \in G \backslash F(G)$, then g acts nontrivially on $E/Z(E)$ by [MW, I, 1.10]. Thus $[g, e] \in F(G) \backslash Z(G)$ 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

$$S < \left(1 + 18/19^4\right) |G/Z(G)| \, |V|^{3/4} < 1.001 \, |G/Z(G)| \, |V|^{3/4}.$$

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 $(1.001)2^{13n/2} < 19^{2^n/4} = |V|^{1/4}$, 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. □

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

[A] J. H. Conway, et al., Atlas of Finite Groups, Clarendon, Oxford, 1985. MR **88g:**20025

[As] M. Aschbacher, Finite Group Theory, Cambridge University Press, Cambridge, 1986. MR **89b:**20001

[C] B. Cooperstein, Minimal degree permutation representation of a classical group, Israel J. Math. 30 (1978), 213-235. MR **58:**22255

[D] L. Dornhoff, Group Representation Theory (A), Marcel Dekker, New York, 1971. MR **50:**458a

[Gd1] D. Goodwin, Regular orbits of linear groups with an application to the $k(GV)$-problem, I, J. Algebra 227 (2000), 395-432. MR **2001b:**20010

[Gd2] D. Goodwin, Regular orbits of linear groups with an application to the $k(GV)$-problem, II, J. Algebra 227 (2000), 433-473. MR **2001b:**20010

[Gl1] D. Gluck, On the $k(GV)$ problem, J. Algebra 89 (1984), 46-55. MR **86b:**20010

[Gl2] D. Gluck, Sharper character value estimates for groups of Lie type, J. Algebra 174 (1995), 229-266. MR **96m:**20021

[Go] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968. MR **38:**229

[Gr1] R. Griess, Automorphisms of extraspecial groups and nonvanishing degree 2 cohomology, Pac. J. Math. 48 (1973), 403-422. MR **57:**16429

[Gr2] R. Griess, Schur multipliers of the known finite simple groups, II, in Proc. Sympos. Pure Math, Vol. 37, Amer. Math. Soc., pp. 279-282, Providence, 1980. MR **82g:**20025

[Gr3] R. Griess, Sporadic groups, code loops, and nonvanishing cohomology, J. Pure Appl. Algebra 44 (1987), 191-214. MR **88c:**20024

[Gw] R. Gow, On the number of characters in a block and the $k(GV)$ problem for self-dual V, J. London Math. Soc. 48 (1993), 441-451. MR **94i:**20020

[GM] D. Gluck and K. Magaard, Character and fixed point ratios in finite classical groups, Proc. London Math. Soc. 71 (1995), 547-584. MR **96f:**20017

[GMS] R. Guralnick, K. Magaard, and J. Saxl, Small cross characteristic representations for odd characteristic symplectic groups, preprint, 1997.

[He] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II, J. Algebra 93 (1985), 151-164. MR **86k:**20046

[Hu] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967. MR **37:**302

[Is1] I. M. Isaacs, Characters of solvable and symplectic groups, Amer. J. Math. 95 (1973), 594-635. MR **48:**11270

[Is2] I. M. Isaacs, Character correspondences in solvable groups, Adv. Math. 43 (1982), 284-306. MR **83i:**20007

[J] G. D. James, On the minimal dimensions of irreducible representations of symmetric groups, Math. Proc. Camb. Phil. Soc. 94 (1983), 417-424. MR **86c:**20018

[K] R. Knörr, On the number of characters in a p-block of a p-solvable group, Illinois J. Math. 28 (1984), 181-210. MR **85d:**20006

[KL] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups, Cambridge University Press, Cambridge, 1990. MR **91g:**20001

[KP] C. Koehler and H. Pahlings, Regular orbits and the $k(GV)$-problem, preprint, 1999.

[L1] M. Liebeck, The affine permutation groups of rank three, Proc. London Math. Soc. 54 (1987), 477-516. MR **88m:**20004

[L2] M. Liebeck, Regular orbits of linear groups, J. Algebra 184 (1996), 1136-1142. MR **98g:**20023

[LS] V. Landazuri and G. Seitz, On the minimal degree of projective representations of the finite Chevalley groups, J. Algebra 32 (1974), 418-443. MR **50:**13299

[M] H. H. Mitchell, The subgroups of the quaternary abelian linear group, Trans. Amer. Math. Soc. 15 (1914), 379-396. CMP 95:18

[MW] O. Manz and T. R. Wolf, Representations of Solvable Groups, Cambridge University Press, Cambridge, 1993. MR **95c:**20013

[R1] G. R. Robinson, Some remarks on the $k(GV)$ problem, J. Algebra 172 (1995), 159-166. MR **96c:**20014

[R2] G. R. Robinson, Further reductions for the $k(GV)$-problem, J. Algebra 195 (1997), 141-150. MR **98d:**20004

[Ri1] U. Riese, Further reductions on the quasisimple case of the $k(GV)$-conjecture, J. Algebra 235 (2001), 45–65.

[Ri2] U. Riese, On the extraspecial case of the $k(GV)$-conjecture, preprint, 1999.

[RS] U. Riese and P. Schmid, Self-dual modules and real vectors for solvable groups, J. Algebra 227 (2000), 159-171. MR **2001f:**20024

[RT] G. R. Robinson and J. G. Thompson, On Brauer's $k(B)$ problem, J. Algebra 184 (1996), 1143-1160. MR **97m:**20014

[Si] P. Sin, Modular representations of the Hall-Janko group. Comm. Alg. 24 (1996), 4513-4547. MR **97j:**20016

[Sr] B. Srinivasan, The characters of the finite symplectic group $Sp(4, q)$, Trans. Amer. Math. Soc. 131 (1968), 488-525. MR **36:**3897

[SZ] G. Seitz and A. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups, II, J. Algebra 158 (1993), 233-243. MR **94h:**20017

[W] A. Wagner, An observation on the degrees of projective representations of the symmetric and alternating groups over an arbitrary field, Arch. Math. 29 (1977), 583-589. MR **57:**444

Department of Mathematics, Wayne State University, Detroit, Michigan 48202
E-mail address: `dgluck@math.wayne.edu`

Department of Mathematics, Wayne State University, Detroit, Michigan 48202
E-mail address: `kaym@math.wayne.edu`