THE 2-TRANSITIVE PERMUTATION REPRESENTATIONS
OF THE FINITE CHEVALLEY GROUPS

BY

CHARLES W. CURTIS, WILLIAM M. KANTOR AND GARY M. SEITZ

ABSTRACT. The permutation representations in the title are all determined, and no surprises are found to occur.

1. Introduction. The permutation representations of the finite classical groups have been a source of interest among group theorists from Galois and Jordan up to the present time. Information about permutation representations has been used to classify various types of groups, and to investigate subgroups of the known simple groups acting, with some transitivity assumptions, in geometrical situations. Unusual or sporadic behavior of permutation representations of certain groups has led to the discovery of new simple groups, and suggests looking for new permutation representations of the known groups. In investigations of finite groups in connection with various classification problems, Chevalley groups acting as permutation groups may occur in the course of the discussion, and one can ask what are the possibilities in such a situation. (Throughout this paper, a Chevalley group will always have a trivial center and be generated by its root subgroups.)

These are some types of questions which serve as motivation for a systematic study of 2-transitive permutation representations of finite Chevalley groups, of normal or twisted types. The conclusion we have reached is that there are no surprises: the only such permutation representations are the known ones. A more precise statement of the main result is as follows.

Main Theorem. Let $G$ be a Chevalley group of normal or twisted type, and let $G < G^* < \text{Aut } G$. Suppose that $G^*$ has a faithful 2-transitive permutation representation. Then one of the following holds.

(i) $\text{PSL}(l, q) < G^* < \text{PTL}(l, q), l > 3$, and $G^*$ acts in one of its usual 2-transitive representations of degree $(q^l - 1)/(q - 1)$.

(ii) $G = \text{PSL}(2, q), \text{PSU}(3, q), \text{Sz}(q)$, or $^2G_2(q)$, and the stabilizer of a point is a Borel subgroup.

(iii) $G^*$ is $\text{PSL}(2, 4) < \text{PSL}(2, 5) \approx A_5$ or $\text{PTL}(2, 4) \approx PGL(2, 5) \approx S_5$.

(iv) $G^*$ is $\text{PSL}(2, 9) \approx A_6$ or $\text{PSL}(2, 9) \cdot \text{Aut } GF(9) \approx S_6$.

(v) $G^*$ is $\text{PSL}(2, 11)$ in one of its 2-transitive representations of degree 11.

(vi) $G^*$ is $\text{PTL}(2, 8) \approx ^2G_2(3)$.
(vii) $G^*$ is $PSL(3, 2) \cong PSL(2, 7)$ or $Aut\ PSL(3, 2) \cong PGL(2, 7)$.
(viii) $G^*$ is $PSL(4, 2) \cong A_8$ or $Aut\ PSL(4, 2) \cong S_8$.
(ix) $G^*$ is $Sp(2n, 2)$ in one of its 2-transitive representations of degree $2^{n-1}(2^n \pm 1)$, with the stabilizer of a point being $GO^+(2n, 2)$.
(x) $G^*$ is $G_2(2) \cong PSU(3, 3) \cdot Aut\ GF(9)$ or $Aut\ G_2(2) \cong P\Gamma U(3, 3)$.

It should be noted that (vi) is the only case where $G^*$, but not $G$, is 2-transitive.

Several special cases of this theorem have already appeared: Parker [27] for $G^* = PSp(4, 3)$, Clarke [11] for $G = PSp(2n, q)$ for certain $n$ and $q$, Bannai [2], [3], [4] for $G^* = PSL(l, q)$, $PSp(2n, 2)$ or $PSp(l, q)$ with $l > 14$, and Seitz [32] for $G = PSp(4, q)$, $PSU(4, q)$, $PSU(5, q)$, $G_2(q)$ with $q > 3$, and $3D_4(q)$. Moreover, Seitz [32] showed that, for a given Weyl group of rank $\geq 3$, there are at most a finite number of exceptions $G$ to the main theorem having that Weyl group, where $G^* \supset G$ is assumed to be contained in the subgroup of $Aut\ G$ generated by $G$ and the diagonal and field automorphisms.

The method of proof is basically as follows. Assume for simplicity that $G^* = G$ and that the Weyl group $W$ of $G$ has rank $\geq 3$. Furthermore, assume that $G$ is of normal type; while the proof for groups of twisted type is the same, it is more awkward to state. Let $\theta = 1_G + \chi$ be the character of the given permutation representation, where $\chi$ is irreducible, and let $B$ be a Borel subgroup of $G$. Using the main theorem in [32], it is easy to show that our main theorem holds if either $\langle \theta, 1_B^G \rangle = 1$, $\chi(1)$ is divisible by the characteristic $p$ of $G$, or $\theta(1)$ is a power of $p$. Thus, if $G$ is a counter-example, then $\chi$ is a constituent of $1_B^G$ and $p \nmid \chi(1)$. According to an extension of a result of Green [19] and D. G. Higman, this is only possible if $G$ is defined over $\mathbb{F}_p$ and $p \mid |W|$. A major part of the proof is aimed at showing that, with few exceptions, a suitably chosen parabolic subgroup $P$ of $G$ is transitive, that is, $\langle \theta, 1_P^G \rangle = 1$; this is proved by checking that $p$ divides the degree of each nonprincipal constituent of $1_P^G$. From this we deduce the semiregularity of certain root groups $U_r$. It then follows that $\chi(1)||G : C(U_r)||$. On the other hand, using structural properties of some parabolic subgroups, we show that $p^k | \theta(1)$ for a suitably large $k$. Elementary number theory is then used to show that these two divisibility conditions are incompatible, thereby proving the theorem. We remark that it is surprising how few properties of 2-transitive groups are needed.

Some parts of our proof use ideas similar to those used by Bannai [2], [3], [4]. However, he uses a detailed knowledge of all the characters of $GL(n, q)$, whereas the character-theoretic information we use is much more elementary.

The organization of the paper is as follows. Part I is concerned with general properties of Chevalley groups. These include the structure of certain parabolic subgroups, normalizers of root groups, and characters of both Weyl groups and Chevalley groups. Some of the proofs are computational, and are not given in complete detail. More information is given concerning the structure of certain parabolic subgroups than is actually needed in the proof of the Main Theorem.

In Part II the Main Theorem is proved. Given the information in Part I, together
with the main result of Seitz [32], the proof turns out to be surprisingly short. In fact, the only involved part centers around the exceptional situations $F_4(2)$ and $Sp(2n, 2)$.

For the sake of completeness, we have handled cases already essentially done by Bannai. This includes $Sp(2n, 2)$, and also $PSL(l, q)$. We note that Bannai's treatment [2] of $PSL(l, q)$ is incomplete, as it uses a result of F. Piper [29] which turns out to be almost, but not quite, correct. Also for the sake of completeness, we verify that the Tits group $^2F_4(2)'$ has no 2-transitive representation.

The study of 2-transitive representations of Chevalley groups contained in [32] and the present paper were initiated by a simple proof in the case $PSL(l, q) \leq G^* \leq PTL(l, q)$, based on the first lemma and the main theorem of Perin [28].

We are indebted to Professor T. Beyer for his invaluable assistance with the proof of (6.8).

PART I. PROPERTIES OF CHEVALLEY GROUPS

2. Notation and preliminary results. Let $\Delta$ be a root system in Euclidean space $E^n$, and let $k$ be a finite field of characteristic $p$, such that $|k| = q$. A Chevalley group $G$ associated with $\Delta$, and defined over $k$, is a finite group generated by certain $p$-groups $U_a$, $a \in \Delta$, called root subgroups, defined as in [36] for a Chevalley group of normal type, and in [34], [36] and [9] for a Chevalley group of twisted type. If $\Delta_0$ is a root system generated by some subset of a fundamental system of roots in $\Delta$, then $G_0 = \langle U_a' \mid a \in \Delta_0 \rangle$ is a Chevalley group associated with the root system $\Delta_0$.

The groups under consideration in the main theorem are assumed to have indecomposable root systems. We shall have to consider subgroups, however, for which this is not necessarily the case.

Unless otherwise stated, $G$ will denote throughout the paper a Chevalley group, with an indecomposable root system $\Delta$, such that $Z(G) = 1$. Let $B$ be a Borel subgroup of $G$, $U$ the Sylow $p$-subgroup of $B$, and $H$ a $p$-complement of $B$. Then $U \subseteq B$, $B = UH$, and $H$ is abelian. There exists a subgroup $N \supseteq H$ such that $W = N/H$ can be identified with a group generated by the reflections $s_1, \ldots, s_n$ corresponding to a fundamental set of roots $\alpha_1, \ldots, \alpha_n$ in the root system $\Delta$. Letting $R = \{s_1, \ldots, s_n\}$, the pair $(W, R)$ is an indecomposable Coxeter system [8], and the subgroups $B, N$ define a Tits system (or $(B, N)$-pair) in $G$, with Weyl group $W$. We shall view the elements of $W$ as belonging to $G$ when this causes no confusion.

We shall use the notations $U_{\alpha_i} = U_i$ and $U_{-\alpha_i} = U_{-i}$, $1 \leq i \leq n$. We may assume that $s_i \in \langle U_i, U_{-i} \rangle$ for $1 \leq i \leq n$.

Throughout the paper, the Dynkin diagram of an indecomposable root system will be labeled as in Table 1.

The correspondence we shall use between classical group notation and $BN$-notation is given in Table 2.

The primes in the first column of Table 2 indicate, as usual, the derived groups. The identifications between different parts of the table were given in [30] and [34]. (See [9] for a summary.)
Table 1

\[
\begin{align*}
A_n, n \geq 1 & \quad \bullet \quad 2 \quad \cdots \quad n-1 \quad n \\
B_n, n \geq 2 & \quad \bullet \quad 2 \quad \cdots \quad n-1 \quad n \\
C_n, n \geq 2 & \quad \bullet \quad \cdots \quad n \quad n \\
D_n, n \geq 4 & \quad \bullet \quad 2 \quad \cdots \quad n-2 \quad n-1 \\
E_6 & \quad \bullet \quad \cdots \\
E_7 & \quad \bullet \quad \cdots \\
E_8 & \quad \bullet \quad \cdots \\
F_4 & \quad \bullet \quad 1 \quad 2 \quad 3 \quad 4
\end{align*}
\]

Table 2

<table>
<thead>
<tr>
<th>Classical Group Notation</th>
<th>(B, N)-Notation</th>
<th>Type of ( \Delta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{PSO}(2n+1, q)' )</td>
<td>( B_n(q) )</td>
<td>( B_n )</td>
</tr>
<tr>
<td>( \text{PSp}(2n, q) )</td>
<td>( C_n(q) )</td>
<td>( C_n )</td>
</tr>
<tr>
<td>( \text{PSO}^+(2n, q)' )</td>
<td>( D_n(q) )</td>
<td>( D_n )</td>
</tr>
<tr>
<td>( \text{PSO}^-(2n, q)' )</td>
<td>( 2D_n(q) )</td>
<td>( B_{n-1} )</td>
</tr>
<tr>
<td>( \text{PSU}(2n, q) )</td>
<td>( 2A_{2n-1}(q) )</td>
<td>( C_n )</td>
</tr>
<tr>
<td>( \text{PSU}(2n+1, q) )</td>
<td>( 2A_{2n}(q) )</td>
<td>( BC_n )</td>
</tr>
</tbody>
</table>

All the root systems are given explicitly at the end of [8]. The root system \( BC_n \) is not reduced and consists of the union of the vectors on pp. 252 and 254 of [8]. In this system, roots have lengths 1, \( \sqrt{2} \), or 2. A root \( \alpha \in \Delta \) has length 2 if and only if \( \alpha/2 \) is a root, and in this case, \( U_{\alpha} = U_{\alpha/2} \) in the corresponding Chevalley group.

For each subset \( I \subseteq \{1, \ldots, n\} \), set

\[
W_I = \langle s_j | j \notin I \rangle;
\]

\[
G_I = \langle B, U_{-j} | j \notin I \rangle = \langle B, W_I \rangle = BW_I B;
\]
$L_I = \langle U_I, U_{-j} | j \notin I \rangle$; and

$Q_I = \langle U_\alpha | \alpha > 0 \text{ and } \alpha = \sum m_j \alpha_j \text{ with } m_j > 0 \text{ for some } j \in I \rangle$.

(Of course, $W_I = 1$, $G_I = B$, $L_I = 1$, and $Q_I = U$ in case $I = \{1, \ldots, n\}$.)

We have already used, and will continue to use, abbreviations, such as $G_i = G\{i\}$, $L_{ij} = L\{i, j\}$, etc.

(2.1) **Lemma.** Let $\alpha, \beta$ be independent roots. Then

$$[U_\alpha, U_\beta] \subseteq \prod_{i,j > 0; \alpha + j\beta \in \Delta} U_{i\alpha + j\beta}.$$

**Proof.** [36, pp. 24, 181].

We remark that $i, j \in \mathbb{Z}$ in (2.1) unless $\Delta$ has type $BC_n$, in which case $2i, 2j \in \mathbb{Z}$.

On several occasions we shall need more precise versions of these commutator relations (cf. (4.8)).

(2.2) **Lemma.** Let $I \subseteq \{1, \ldots, n\}$.

(i) $Q_I \leq G_I$, $Q_L_I \leq G_I$, and $G_I = Q_L_I H$.

(ii) $Q_I$ is the largest normal $p$-subgroup of $G_I$.

(iii) $L_I$ is a product of pairwise commuting covering groups of Chevalley groups, and its structure can be found by deleting the vertices in $I$ from the Dynkin diagram of $G$.

**Proof.** The commutator relations imply (i). Since $Q_I \leq U$, $Q_I$ is a $p$-group. Since $H$ is a $p'$-group, to prove (ii) it will suffice to show that $L_I$ has no proper normal $p$-subgroup. Let $w_0$ be the element of maximal length in $W_I$. Since $U \cap L_I$ is a Sylow $p$-subgroup of $L_I$, and $(U \cap L_I) \cap (U \cap L_I)^W_0 = 1$, it is clear that $L_I$ has no proper normal $p$-subgroup, so that (ii) is proved. Statement (iii) follows from the fact that the structure of a Chevalley group of rank $> 1$ is determined by the root subgroups and the commutator relations, which are in turn all determined from what remains of the Dynkin diagram after deleting the vertices in $I$.

(2.3) **Lemma** (Tits). If $L$ is a proper subgroup of $G$ such that $U \leq L$ then $L \leq G_i$ for some $i$.

**Proof.** See [32, (1.6)].

(2.4) **Lemma** (Borel and Tits). Let $V_1$ be a subspace of $E_n$ such that the root system $\Delta_1 = \Delta - V_1$ contains a basis of $V_1$, and let $W_1$ be the Weyl group of $\Delta_1$. Let $\alpha, \beta \in \Delta - \Delta_1$ be such that $\alpha \equiv \beta$ (mod $V_1$) and $|\alpha| = |\beta|$ (where $|\cdot|$ denotes a length function invariant by the Weyl group). Then $\alpha \in \beta W_1$.

**Proof.** [7]. (This will only be needed for very special cases in (4.2), where it is easy to check by direct calculation.)

(2.5) **Lemma.** Let $\Sigma = \{U_\alpha | \alpha \in \Delta\}$. If $\alpha \in \Delta$ and $w \in W$, then $(U_\alpha)^w = U_{(w)\alpha}$, so that, in particular, $\Sigma = \{U_\alpha | 1 \leq i \leq n, w \in W\}$. $W$ acts on $\Sigma$ by conjugation.

The permutation groups $(W, \Delta)$ and $(W, \Sigma)$ are isomorphic, with the isomorphism induced by the correspondence $\alpha \leftrightarrow U_\alpha$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
C. W. CURTIS, W. M. KANTOR AND G. M. SEITZ

Proof. This result holds for arbitrary groups having split \((B, N)\)-pairs ([31]).

(2.6) Proposition. View \(G\) as a subgroup of Aut \(G\), and let \(G^k\) be the subgroup of Aut \(G\) generated by \(G\) together with all the diagonal and field automorphisms of \(G\). Then \(G^k \subseteq\) Aut \(G\), and the index divides 6. Aut \(G\) is generated by \(G^k\) and the graph automorphisms of \(G\). If \(G \leq G^* \leq\) Aut \(G\), then \(G^*\) has a normal subgroup \(G^+ = G^k \cap G^*\) containing \(G\) of index dividing 6 such that \(G^+\) has a Tits system given by subgroups \(B^+, N^+\) satisfying \(B = G \cap B^+\) and \(N = G \cap N^+\). Moreover, \(G^+ = B^+ G\).

Proof. See [36].

(2.7) Lemma. Let \(L, M\) be subgroups of a group \(T\). Then \((1^T_L, 1^T_M)\) is the number of \((L, M)\)-double cosets in \(T\).

The proof is omitted.

(2.8) Lemma. Let \(I, J \subseteq \{1, \ldots, n\}\). Then \((1^W_I, 1^W_J) = (1^W_W, 1^W_W)\) is the number of \((W_I, W_J)\)-double cosets in \(W\).

Proof. The statement follows easily from the axioms of a Tits system and the Bruhat decomposition (see Remarque 2, p. 28 of [8]), together with (2.7).

(2.9) Lemma. Let \(G\) be a Chevalley group, and let \(G^* \subseteq\) Aut \(G\) be as in (2.6). Then \(1^G_{B^+} G = 1^G_B\), and each irreducible constituent of \(1^G_{B^+}\) remains irreducible when restricted to \(G\).

Proof. The equality follows from the fact that \(B^+ G = G^+\) and Mackey's Subgroup Theorem. (2.7) and (2.8) imply that

\[
(1^G_B, 1^G_B) = (1^W_W, 1^W_W) = (1^{B^+}_B, 1^{G^+}_{B^+}),
\]

proving the second statement.

We remark in passing that (2.9) proves that if \(G^+\) has a 2-transitive permutation representation with character \(\theta = 1 + \chi\), and if \(\chi \in 1^G_{B^+}\), then \(G\) has a 2-transitive permutation representation.

(2.10) Proposition. Let \(G\) be a Chevalley group and \(G^k\) be as in (2.6). Let \(G \leq \tilde{G} \leq G^k\), and let \(\tilde{B}\) be a Borel subgroup of \(\tilde{G}\). Suppose that \(n \geq 2\), and \(\tilde{G}\) has a subgroup \(L\) such that \(\tilde{L} \tilde{B} = \tilde{G}\). Then either \(G \leq L\) or one of the following holds:

(i) \(G = PSL(3, 2)\) and \(|L| = 3 \cdot 7\).
(ii) \(G = PTL(3, 8)\) and \(|L| = 3^2 \cdot 73\).
(iii) \(G = PSL(4, 2) \approx A_8\), and \(L \approx A_7\).
(iv) \(G = PSp(4, 2) \approx S_6\), and \(L \approx A_6\).
(v) \(G = G_2(2)\), and \(L = G^+\).
(vi) \(G = 2F_4(2)\), and \(L = G^+\).
(vii) \(G = PSp(4, 3) \approx PSU(4, 2)\), and \(L \cap G\) is a maximal parabolic subgroup of \(PSU(4, 2)\) of order \(2^6 \cdot 3 \cdot 5\).

Proof. This result is Theorem A of [32].
3. Properties of the classical groups. In this section we shall discuss some general properties of the classical groups $PSp(2n, q)$, $PSO^+(l, q)'$, and $PSU(l, q)$. We define $SO^±(l, q)$ as follows. Let $V$ be an $l$-dimensional vector space having a nondegenerate quadratic form, and let $G$ be the group of isometries of $V$. If $V$ has maximal index, then $G = GO^+(l, q)$; otherwise, $G = GO^-(l, q)$. Then $SO^±(l, q)$ is the set of elements of $GO^±(l, q)$ with determinant 1 or Arf invariant 0, depending on whether $q$ is odd or even. Recall that, as in [15], an orthogonal space $V$ is nondegenerate if $\text{rad}(V)$ contains no nonzero singular vectors.

We are primarily interested in the structure of the parabolic subgroups of the classical groups (see (2.2)). Further discussion of these groups will be found in §§6 and 8. Basic information on the classical groups can be found in the books of Artin [1] and Dieudonné [15]. Some of the arguments given here are in outline form, with details left to the reader. Some information of a numerical nature is tabulated in Table 3 at the end of this section; there, $\rho$ is the reflection character (see (5.4)), while $\sigma = \frac{1}{G} G - \rho$. We first state the main results; the proofs will be given later in this section.

(3.1) Proposition. Let $G = PSO^+(l, q)'$, $l \geq 7$.

(i) $Q_1$ is elementary abelian of order $q^{l-2}$.

(ii) $L_1 \cong SO^+(l - 2, q)'$, and acts on $Q_1$ as a group of $F_q$-linear transformations, preserving a nondegenerate quadratic form. If $q$ is even and $l$ is odd, then the radical of the form is $U_s$, where $s$ is the short root of maximal height.

(iii) Let $r$ be the positive root in $\Delta$ of maximal height. Then $G_2 = N(U_r) = C(U_r) H$, where $|U_r| = q$.

(iv) If $q$ is odd, then $U_r$ is an isotropic 1-space in $Q_1$, while if $q$ is even, $U_r$ is a singular 1-space.

(3.2) Proposition. Let $G = PSp(2n, q)$, $n \geq 2$.

(i) $|Q_1| = q^{2n-1}$. If $q$ is odd, then $Q_1$ is special with center of order $q$. If $q$ is even, $Q_1$ is elementary abelian.

(ii) Let $r$ be the root of maximal height. Then $Z(Q_1 L_1) = U_r$ has order $q$, and $G_1 = N(U_r) = C(U_r) H$. If $q$ is odd, then $U_r = Z(Q_1)$. All elements of each nontrivial coset of $U_r$ in $Q_1$ are conjugate in $Q_1 L_1$.

(iii) $L_1 \cong Sp(2n - 2, q)$, and acts on $Q_1/U_r$ as a group of $F_q$-transformations preserving a nondegenerate alternating form. If $q$ is odd, such a form is induced by the commutator function. If $q$ is even, $L_1$ acts indecomposably on $Q_1$.

(iv) There exists a positive root $s$ such that $U_s U_r / U_r$ is central in $U/U_r$, and is an isotropic 1-space of $Q_1/U_r$. Here, $|U_s| = q$.

(v) $Q_{12} = Q_2 U_1$, $Q_2 \leq G_{12}$, $Q_2 L_{12} \leq G_2$, $Q_2 L_{12} \leq C(U_2)$, and $G_{12} = (Q_2 L_{12}) U_1 H = C_{G_{12}}(U_2) U_1 H$.

(3.3) Proposition. Let $G = PSU(l, q)$, $l \geq 4$.

(i) $Q_1$ is special of order $q^{2l-1}$, with center of order $q$.

(ii) There exists a uniquely determined root $r$ such that $Z(Q_1) = Z(U_r)$ has order
q. If $l$ is odd, $U_r$ is special of order $q^3$, while if $l$ is even, $U_r$ is elementary abelian. All elements of each nontrivial coset of $Z(Q_1)$ in $Q_1$ are conjugate in $Q_1$. Moreover, $G_1 = N(Z(Q_1)) = C(Z(Q_1))H$.

(iii) $L_1 = SU(l - 2, q)$, and acts on $Q_1/Z(Q_1)$ as a group of $F_{q^2}$-linear transformations preserving a nondegenerate hermitian form. The commutator function induces a nondegenerate alternating form on the $F_{q^2}$-space $Q_1/Z(Q_1)$ preserved by $L_1$. (The forms are related by (3.7).)

(iv) There is a positive root $s$ such that $U_2Z(Q_1)/Z(Q_1)$ is central in $U/Z(Q_1)$ and is an isotropic 1-space of the unitary space $Q_1/Z(Q_1)$. Here, $|U_2| = q^2$.

(v) $Q_{12} = Q_2 U_1, Q_2 \leq G_{12}, Q_2 L_{12} \leq G_2, Q_2 L_{12} \leq C(U_2)$, and $G_{12} = (Q_2 L_{12}) U_1 H = C_{G_{12}}(U_2)U_1 H$.

These properties will be proved, for the most part, together. The case of $PSO(2n + 1, 2')$ is left to the reader. We can replace $G$ by the corresponding linear group $G = SO^*(l, q)$, $Sp(2n, q)$, or $SU(l, q)$, acting as usual on a vector space $V$ and preserving a nondegenerate quadratic form, a nonsingular alternating scalar product, or a nonsingular hermitian scalar product, respectively. In each case we let $(\ , \ )$ denote the underlying scalar product, and let $\dim V = l$. We are assuming that $\text{rad}(V) = 0$.

We can write $V = V_1 \perp \cdots \perp V_k \perp V_{k+1}$, with $V_1, \ldots, V_k$ hyperbolic planes, and $V_{k+1}$ either 0 or anisotropic of dimension 1 or 2. We select an ordered basis $v_1, \ldots, v_l$ for $V$ in such a way that $v_i, v_{i-1}$ is a hyperbolic pair in $V_i$ ($1 \leq i \leq k$) and $V_{k+1}$ is either 0 or has a basis $\{v_{k+1}\}$ or $\{v_{k+1}, v_{k+2}\}$. Matrices will be written with respect to the ordered basis $v_1, \ldots, v_l$ of $V$.

We first show that the subgroup $B$ of $G$ fixes a unique 1-space in $V$, which is generated by an isotropic vector (or singular vector if $G$ is an orthogonal group and $q$ is even). Consider $B$ acting on $V$. Since $U \leq B$ and $U$ is a $p$-group, $U$ fixes every vector in a nontrivial subspace of $V$ fixed by $B$. As $B = UH$ and $H$ is diagonalizable on $V$, $B$ fixes a 1-space $V_0$ of $V$. Suppose $G$ is not orthogonal with $q$ even. If $V_0$ is not isotropic, then $V = V_0 \perp V'_0$ and $U$ acts faithfully on $V'_0$. However this implies that $U$ is contained in a classical group of smaller dimension, which is impossible in view of $|U|$. So in this case $V_0$ is isotropic. Now suppose $G$ is orthogonal and $q$ is even. If $V_0$ is not singular then $V'_0$ is a nondegenerate orthogonal space of dimension less than $\dim V$. Also, $U$ acts faithfully on $V'_0$, as otherwise $G$ would contain a transvection, which is not the case. As before, order considerations yield a contradiction. Thus, $V_0$ is singular. We only need the uniqueness of $V_0$. Suppose that $B$ fixed the 1-space $V'_0$. Then $V'_0$ is isotropic (or singular) and so $V'_0 = V_0^g$ for some $g \in G$. Thus $B \leq N_G(V_0)$ and $B \leq N_G(V'_0) = N_G(V_0)^F$. The theory of parabolic subgroups implies that $g \in \text{stab}(V_0)$ and $V_0 = V'_0$. Since $B$ fixes a unique 1-space and since $H$ is diagonalizable on $V$, it follows that $\dim(C_V(U)) = 1$.

We may assume that $B \leq N_G(\langle u_1 \rangle) = Y$, so that $Y$ is a parabolic subgroup of $G$. Since $V = \langle u_1, v_1 \rangle \perp \langle u_1, v_1 \rangle^l$, $Y$ contains a subgroup $Y_0$ such that $Y_0$ is trivial on $\langle u_1, v_1 \rangle$ and induces on $\langle u_1, v_1 \rangle$ the derived group of the group of isometries of $\langle u_1, v_1 \rangle^l$. Let $Q = O_p(Y)$. Then since $Y$ acts irreducibly on the space $\langle u_1 \rangle^l/\langle u_1 \rangle$, $Q$ is trivial on
this space. Also, \( V/\langle v_1 \rangle^1 \) is 1-dimensional and \( \langle v_1 \rangle \) is 1-dimensional, so that \( (Y/Q)' \) is trivial on these spaces and, hence, faithful on \( \langle v_1 \rangle /\langle v_1 \rangle \). It follows that \( (Y/Q)' \approx Y_0 \).

Thus, by (2.2) we have \( Y = G_1 \).

We now claim that \( g \in G \) belongs to \( Q = Q_1 \) if and only if \( g \) has one of the following matrix forms. This fact is verified by checking that the matrices described in each case form a normal \( p \)-subgroup of \( G_1 \), with the property that no larger \( p \)-subgroup of \( G_1 \) acts trivially on \( \langle v_1 \rangle /\langle v_1 \rangle \).

(3.4) \( G \) symplectic.

\[
\begin{pmatrix}
1 & a_2 & \cdots & a_k \\
-a_2 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
-a_k & \cdots & 1 & 0 \\
a_{k+1} & \cdots & a_{l-1} & 1
\end{pmatrix}
\]

Here \( a_i + a_i = (a_{l-1}v_2 + \cdots + a_2v_{l-1}, a_{l-1}v_2 + \cdots + a_2v_{l-1}) \), and \( \bar{a} = a^q \).

(3.5) \( G \) unitary.

\[
\begin{pmatrix}
1 & 0 & \cdots & 0 \\
-a_2 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
-a_k & \cdots & 1 & 0 \\
-a_{l-1} & \cdots & a_{l-1} & 1
\end{pmatrix}
\]

(3.6) \( G \) orthogonal.

\[
\begin{pmatrix}
1 & 0 & \cdots & 0 \\
-a_2 & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
-a_{l-1} & \cdots & 1 & 0 \\
+a_1 & \cdots & a_{l-1} & 1
\end{pmatrix}
\]

Here \( a_i = -t(a_{i-1}v_2 + \cdots + a_2v_{l-1}) \), where \( t( ) \) is the quadratic form on \( V \).

If \( g \in Q_1 \) has one of the above forms, set \( v_g = a_{l-1}v_2 + \cdots + a_2v_{l-1} \). Then \( v_g \) satisfies the condition:

\[
(v_g)g = a_iv_1 + v_i + v_g \quad \text{(symplectic case)},
\]
\[(v_g)g = -\overline{a_g}v_1 + v_I + v_g \quad \text{(unitary case)}, \]
\[(v_g)g = a_gv_1 + v_I + v_g \quad \text{(orthogonal case)}.\]

In all cases, \(v_g\) is a vector belonging to \(V_2 \perp \cdots \perp V_{k+1}\), and for \(g \in Q_1\) and \(v \in V_2 \perp \cdots \perp V_{k+1}\),
\[(v)g = v - (v, v_g)v_1.\]

Using these facts we obtain, for all \(g, h \in Q_1\),
\[
[\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \\ (v_g, v_h) \end{pmatrix},
\]
\[
(3.7)
\]
where \((v_g, v_h)' = (v_h, v_g) - (v_g, v_h)\).

Consequently, \(Q_1\) is elementary abelian if \(V\) is orthogonal, or if \(V\) is symplectic and \(q\) is even. In the remaining cases, \(Q_1\) is special and has as center the group \(X\) of transvections in \(G\) with direction \(\langle v_1 \rangle\). By (3.7), if \(g \in Q_1 - Z(Q_1)\), then all elements of the coset \(gZ(Q_1)\) are conjugate in \(Q_1\).

Clearly \(C_G(V_1)\) induces a group containing the derived group of the isometry group of \(V_1 = V_2 \perp \cdots \perp V_{k+1}\). If \(*, C_G(V_1)\), then \(g'y \in Q_1\). We have
\[
(v_g)y^{-1}g'y = cy_1 + (v_g)y + v_1,
\]
where \(c\) is the coefficient of \(v_1\) in \((v_g)g\). In particular, \(v_y^{-1}g'y = (v_g)y\). The properties of the set of vectors \(\{v_g|g \in Q_1\}\) show that the action of \(C_G(V_1)\) on \(Q_1\) (if \(G\) is orthogonal) or on \(Q_1/X\) (if \(G\) is symplectic or unitary) is determined by the mappings \(v_g \mapsto v_gy, g \in Q_1, y \in C_G(V_1)\). Therefore, \(L_1\) acts on \(Q_1\) (in the orthogonal case) or on \(Q_1/X\) (in the symplectic or unitary cases) as a group of linear transformations on a vector space over \(F_q\), preserving a nondegenerate quadratic form, or a nonsingular alternating or Hermitian scalar product. Also \(L_1 \leq C_G(X)\).

Suppose that \(V\) is symplectic with \(q\) odd or that \(V\) is unitary. Then \(X = Q_1'\), and (3.7) shows that the commutator function induces a nondegenerate alternating form on \(Q_1/X\). The action of \(C_G(V_1)\) on \(Q_1\) shows that this form is preserved by \(L_1\).

Suppose that \(V\) is symplectic and \(q\) is even. Then \(Q_1\) is abelian, and we will show that \(L_1\) acts indecomposably on \(Q_1\). Let \(X_1\) be an \(L_1\)-invariant subgroup of \(Q_1\), not contained in \(X\). Let \(1 \neq g \in X_1\) be as in (3.4). As \(L_1\) is transitive on the nonzero vectors of \(Q_1/X \approx V_2 \perp \cdots \perp V_{k}\), every nonzero vector of \(V_2 \perp \cdots \perp V_{k}\) appears as \(v_h\) for some \(h \in X_1\). This construction produces \(q^{l-2} - 1\) elements of \(X_1\) all having the same entry \(a_l\). These elements, together with \(1\), do not form a group. It follows
that, if \( Q_1 \) is decomposable, then \( Q_1 = X \times X_1 \), with \( |X_1| = q^{\ell - 2} \), and the preceding argument gives a contradiction.

The rest of the proof involves the \((B, N)\) structure of \( G \). We begin with some remarks concerning the root systems. (Further discussion of these root systems can be found in (6.1)–(6.4).) The root of maximal height is as follows [8, pp. 252, 254, 256]:

\[
B_n: \alpha_1 + 2 \sum_{1 < i} \alpha_i.
\]

\[ (3.8) \]

\[
C_n: 2 \sum_{i < n} \alpha_i + \alpha_n.
\]

\[
D_n: \alpha_1 + 2 \sum_{1 < i < n - 1} \alpha_i + \alpha_{n-1} + \alpha_n.
\]

For type \( B_n \) and \( D_n \), this root is fixed by \( W_2 = \langle s_1, s_3, \ldots, s_n \rangle \), while for type \( C_n \) it is fixed by \( W_1 \). We now divide the discussion into three cases.

(1) \( G = SO^\ell(l, q) \), where \( q \) is odd if \( l \) is. Here \( \Delta \) has type \( B_n \) or \( D_n \). Define \( r \) by (3.8). By the commutator relations (2.1), \( C(U_r) \supseteq \langle U^w \mid w \in W_1 \rangle \supseteq Q_2 L_2 \), so \( N(U_r) \supseteq Q_2 L_2 H = G_2 \) by (2.2). Then \( N(U_r) = G_2 \) by the maximality of \( G_2 \), and clearly \( C(U_r)H = G_2 \).

Since \( U \cap L_1 \) is Sylow in \( L_1 \), from the action of \( L_1 \) on \( Q_1 \) it follows that the space of elements fixed by \( U \cap L_1 \) is an isotropic 1-space (singular, if \( q \) is even).

Since \( U_r < Q_1 \), it follows that \( U_r \) is in this 1-space, so since \( |U_r| = q \), it follows that \( U_r \) is isotropic (or singular).

(2) \( G = Sp(2n, q) \) or \( SU(2n, q) \). Here \( \Delta \) has type \( C_n \), and \( U_r \) is elementary abelian of order \( q \), where \( r \) is given in (3.8). Since \( W_1 \) fixes \( r \), the commutator relations (2.1) imply that \( C(U_r) \supseteq \langle U^w \mid w \in W_1 \rangle \supseteq Q_1 L_1 \). Then, as in (1), \( G_1 = N(U_r) = C(U_r)H \). The irreducibility of \( L_1 \) on \( Q_1/X \) shows that \( X = U_r \).

Since each root \( \neq \pm \alpha \), which involves \( \alpha_1 \) also involves \( \alpha_2, Q_2 = \langle U_\alpha \alpha > 0, \alpha \neq \alpha_1, \alpha \rangle \). Thus, \( Q_12 = Q_2 U_1 \). Moreover, \( Q_2 < Q_12 L_12 \).

The root \( s = r - \alpha_1 \) is the highest short root, and is fixed by \( W_1 \). The commutator relations (2.1) imply \( C(U_s) \supseteq \langle U_\alpha \mid \alpha > 0, \alpha \neq \alpha_1, w \in W_1 \rangle = Q_2 L_12 \). Then \( G_{12} = Q_2 L_12 U_1 H = C_{Q_12}(U_s) U_1 H \). Also, \( L_2 = L_{12} \langle U_1, U_{-1} \rangle \) with \( [L_{12}, U_1] = [L_{12}, U_{-1}] = 1 \). Since \( G_2 = Q_2 L_2 H \), and since \( H \) normalizes \( L_{12} \), we have \( Q_2 L_2 L_12 < G_2 \).

The group \( U_s U_r / U_r \leq Z(U/U_r) \). Also, \( s \) is short, so \( |U_s| = |U_1| = q \) for \( Sp(2n, q) \) and \( q^2 \) for \( SU(2n, q) \). As in (1), \( U_s U_r / U_r \) is an isotropic 1-space of \( Q_1 / U_r \).

(3) \( G = SU(2n + 1, q) \). This time \( \Delta \) has type \( BC_n \). With respect to the basis \( \alpha_1, \ldots, \alpha_n \) of \( B_n \), the root \( r = 2(\alpha_1 + \cdots + \alpha_n) \) is the root of maximal height in \( C_n \), where \( r/2 \) is a root. The root \( s = \alpha_1 + 2(\alpha_2 + \cdots + \alpha_n) = r - \alpha_1 \) is highest in \( B_n \). Here \( U_s \) and \( U_1 \) are conjugate under \( W \), as are \( U_r = U_{r/2} \) and \( U_{n} \). This implies that \( U_1 \) is elementary abelian of order \( q^2 \) and \( U_r \) is special of order \( q^3 \) with center of order \( q \).

The only roots \( \alpha \) not of length \( \sqrt{2} \) for which \( U_\alpha \leq Q_1 \) are \( r \) and \( r/2 \) [8, pp. 252,
Since \( Z(Q_1) = Q'_1 = X \) has order \( q \), we must have \( Z(U_r) = Z(Q_1) \).

As in (1), the space of fixed elements for \( U \cap L_1 \) in its action on \( Q_1/X \) is an isotropic 1-space. Since \( s = r - a_1 \), the commutator relations (2.1) yield \([U \cap L_1, U_r] = 1\). So again we find that \( U_r X/X \) is an isotropic 1-space. The remainder of (3.3)(v) can now be proved as in (2). This completes the proof of (3.1)–(3.3).

(3.9) Lemma. Let \( G \) and \( s \) be as in (3.2) or (3.3). Let \( \chi \) be an irreducible constituent of both \( 1^G_B \) and \( 1^G_{\xi(x)} \), where \( 1 \neq x \in U_r \). Then \( \chi \) is a constituent of \( 1^G_{G_{12}} \).

Proof. Set \( T = Q_2 L_{12} \). By (3.2) and (3.3), we know that \( T \leq C(x) \), \( T \subseteq G_2 \), and \( G_{12} = TU_1 H \). In particular, \( \chi \in 1^G_B \). Write

\[
1^G_T = (1^G_{G_2})^G = (1^G_{G_2} + \theta_1 + \cdots + \theta_k)^G,
\]

where the \( \theta_i \)'s are irreducible characters of \( G_2 \) having \( T \) in their kernels. We may assume that \( \chi \notin 1^G_{G_2} \) and, hence, that \( \chi \in \theta_i^G \) for some \( i \). Since \( \chi \in 1^G_B \), the Mackey Subgroup Theorem yields

\[
0 < (\theta_i^G, 1^G_B) = \sum_{G_2 w B} (\theta_i^{w^{-1}}, 1)_{G_2 \cap w B},
\]

where the sum is taken over the distinct \((G_2, B)\)-double cosets.

There is a double coset \( G_2 w B \) for which \((\theta_i^{w^{-1}}, 1)_{G_2 \cap w B} > 0\). We can consider \( w \) to be in \( W \). Since \( s \in W_2 \), we may assume that every minimal expression for \( w \) as a word in the \( s_i \)'s has the form \( w = s_{i_1} \cdots s_{i_l} \) with \( s_{i_1} \neq s_1 \). Then \((\alpha_1)w \) is a positive root, so \( G_2 \cap B \geq U_1 H \). Consequently,

\[
0 < (\theta_i^{w^{-1}}, 1)_{G_2 \cap B} \leq (\theta_i^{w^{-1}}, 1)_{U_1 H} = (\theta_i^{w^{-1}}, 1)_{U_1 H},
\]

so \((\theta_i, 1)_{U_1 H} > 0\). That is, \( 1_{U_1 H} \in (\theta_i)_{U_1 H} \). But \( T \) is in the kernel of \( \theta_i \), so \( 1_{U_1 H T} \in (\theta_i)_{U_1 H T} \), where \( G_{12} = U_1 H T \). Thus, \( \theta_i \in 1^G_{G_{12}} \), as required.

4. Properties of the exceptional groups. We next consider some general properties of the groups \( G = F_4(q), 2E_6(q), E_6(q), E_7(q), \) and \( E_8(q) \), having, respectively, Weyl groups of types \( F_4, F_4, E_6, E_7, \) and \( E_8 \).

Let \( r \) be the positive root of maximal height. The commutator relations (2.1) imply that \( U_r \leq Z(U) \). By [8, pp. 260, 265, 269, and 272], \( r \) is as follows.

\[
F_4: r = 2a_1 + 3a_2 + 4a_3 + 2a_4, \\
E_6: r = a_1 + 2a_2 + 3a_3 + 3a_4 + 2a_5 + a_6, \\
E_7: r = 2a_1 + 2a_2 + 3a_3 + 4a_4 + 3a_5 + 2a_6 + a_7, \\
E_8: r = 2a_1 + 3a_2 + 4a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8.
\]

(4.1)

(4.2) Proposition. (i) The stabilizer of \( r \) in \( W \) is \( W_i \), where \( i \) is given in Table 4. Also, \( G_i = N_G(U_r) \).

(ii) \((1^G_{G_i}, 1^G_{G_i}) = (1^W_{W_i}, 1^W_{W_i}) = 5\).
| $G$   | $|G : G_1|$ | $|G : G_2|$ | $\rho(1)$ | $\sigma(1)$ |
|-------|-------------|-------------|-----------|-----------|
| $PSO(2n + 1, q)$ | $\frac{q^{2n} - 1}{q - 1}$ | $\frac{(q^{2n} - 1)(q^{2n-2} - 1)}{(q - 1)(q^2 - 1)}$ | $\frac{q(q^n - 1)(q^{n-1} + 1)}{2(q - 1)}$ | $\frac{q(q^n + 1)(q^{n-2} - 1)}{2(q - 1)}$ |
| $PSp(2n, q)$ | $\frac{q^{2n} - 1}{q - 1}$ | $\frac{(q^{2n} - 1)(q^{2n-2} - 1)}{(q - 1)(q^2 - 1)}$ | $\frac{q(q^n - 1)(q^{n-1} + 1)}{2(q - 1)}$ | $\frac{q(q^n + 1)(q^{n-2} - 1)}{2(q - 1)}$ |
| $PSO^+(2n, q)$ | $\frac{(q^n - 1)(q^{n-1} + 1)}{q - 1}$ | $\frac{(q^n - 1)(q^{n-1} + 1)(q^{n-1} - 1)(q^{n-2} + 1)}{(q - 1)(q^2 - 1)}$ | $\frac{q(q^n - 1)(q^{n-2} + 1)}{q^2 - 1}$ | $\frac{q^2(q^n - 1)(q^{n-1} + 1)}{q^2 - 1}$ |
| $PSO^-(2n, q)$ | $\frac{(q^n + 1)(q^{n-1} - 1)}{q - 1}$ | $\frac{(q^n + 1)(q^{n-1} - 1)(q^{n-1} + 1)(q^{n-2} - 1)}{(q - 1)(q^2 - 1)}$ | $\frac{q^2(q^n - 1)(q^{n-1} + 1)}{q^2 - 1}$ | $\frac{q^2(q^n + 1)(q^{n-2} - 1)}{q^2 - 1}$ |
| $PSU(2n, q)$ | $\frac{(q^{2n} - 1)(q^{2n-1} + 1)}{q^2 - 1}$ | $\frac{(q^{2n} - 1)(q^{2n-1} + 1)(q^{2n-2} - 1)(q^{2n-3} + 1)}{(q + 1)(q^2 - 1)}$ | $\frac{q^2(q^{2n} - 1)(q^{2n-3} + 1)}{(q + 1)(q^2 - 1)}$ | $\frac{q^3(q^{2n-1} + 1)(q^{2n-2} - 1)}{(q + 1)(q^2 - 1)}$ |
| $PSU(2n + 1, q)$ | $\frac{(q^{2n+1} + 1)(q^{2n} - 1)}{q^2 - 1}$ | $\frac{(q^{2n+1} + 1)(q^{2n-1})(q^{2n-1} + 1)(q^{2n-2} - 1)}{(q^2 - 1)(q^4 - 1)}$ | $\frac{q^3(q^{2n-1} - 1)(q^{2n-1} + 1)}{(q + 1)(q^2 - 1)}$ | $\frac{q^2(q^{2n+1} + 1)(q^{2n-2} - 1)}{(q + 1)(q^2 - 1)}$ |
(iii) $1_{W_i}^W$ is multiplicity-free, and the degrees of its irreducible constituents are given in Table 4. The reflection character of $W$ is a constituent of $1_{W_i}^W$.

Table 4

| $G$       | $i$ | $|G:G_i|$ | Degrees in $1_{W_i}^W$ | Degree $\rho(1)$ of reflection character |
|-----------|-----|----------|------------------------|------------------------------------------|
| $F_4(q)$  | 1   | (q^4 + 1)$\frac{q^{12} - 1}{q - 1}$ | 1, 2, 9, 4, 8           | $\frac{1}{2}q(q^3 + 1)^2(q^4 + 1)$        |
| $2E_6(q)$ | 1   | (q^4 + 1)$\frac{q^9 + 1 - q^{12} - 1}{q^3 + 1 - q - 1}$ | 1, 2, 9, 4, 8           | $q^2(q^4 + 1)(q^6 + 1)\frac{q^5 + 1}{q + 1}$ |
| $E_6(q)$  | 2   | (q^4 + 1)$\frac{q^9 - 1 - q^{12} - 1}{q^3 - 1}$ | 1, 15, 20, 6, 30        | $q(q^4 + 1)\frac{q^9 - 1}{q^3 - 1}$         |
| $E_7(q)$  | 1   | $\frac{q^{14} - 1 - q^{12} - 1 - q^{18} - 1}{q^4 - 1 - q^6 - 1}$ | 1, 27, 35, 7, 56        | $q(q^6 + 1)\frac{q^{14} - 1}{q^2 + 1}$       |
| $E_8(q)$  | 8   | (q^{10} + 1)$\frac{q^{24} - 1 - q^{30} - 1}{q^6 - 1 - q}$ | 1, 35, 84, 8, 112       | $q(q^{10} + 1)\frac{q^{24} - 1}{q^6 - 1}$     |

Proof. It is easy to check that $r$ is fixed by $W_i$, so $G_i = \langle U_i, H \rangle \subseteq N_G(U_i)$. Thus, $G_i = N_G(U_i)$ by the maximality of $G_i$. Moreover, if $\langle r \rangle W = r$, then $\langle U_i \rangle W = U_i$, so $w \in G_i$ and, hence, $w \in W_i$ by the uniqueness of the Bruhat decomposition. This proves (i).

To prove (ii), we must calculate the number of orbits of $W_i$ on $(r)W$ (see (2.7) and (2.8)). By (2.4) (or using [8, pp. 260, 264, 268, and 272]), for each integer $m$, $O_m = \{ \alpha \in (r)W | \alpha \text{ has } m \text{ as coefficient of } \alpha \}$ is either empty or an orbit of $W_i$. Again by [8], $O_0, O_1, O_{-1}, O_2, \text{ and } O_{-2}$ are the orbits of $W_i$. This proves (ii). In particular, $1_{W_i}^W$ is multiplicity-free.

To prove (iii), let $w_0$ be the element of $W$ of greatest length. Again using [8], we find that $w_0$ normalizes $W_i$; in fact, $w_0 \in Z(W)$ for $W$ of type $F_4$, $E_7$, or $E_8$. We will consider $W_i = W_i(w_0)$.

Since $w_0$ sends positive roots to negative roots and $(\alpha_i)w_0 = -\alpha_i$, $w_0$ fixes $O_0$ and interchanges both $O_1$ and $O_{-1}$, and $O_2$ and $O_{-2}$. Consequently, $W$ acts as a rank 3 permutation group on $\{ (\alpha_i - \alpha_j) \alpha \in (r)W \}$, the stabilizer of $\langle r, -r \rangle$ being $\tilde{W}_i$.

Since $1_{W_i}^W = 1_{\tilde{W}_i}^W + \lambda$, with $\lambda$ a linear character, we have $1_{W_i}^W = 1_{\tilde{W}_i}^W + \lambda^W$. Here, $1_{W_i}^W - 1_{\tilde{W}_i}^W$ is the sum of 2 irreducible characters, so by (ii), $\lambda^W$ is also the sum of 2 irreducible characters.

Let $V$ be the natural module for the reflection representation of $W$, and let $\tau$ be the corresponding reflection character. Then $\alpha_1, \ldots, \alpha_n$ can be regarded as a basis for $V$. Set $V_i = \langle \alpha_i | i \neq i \rangle$. Then $W_i$ stabilizes $V_i$ and is trivial on $V/V_i$; that is, $1_{W_i}$ appears as a constituent of the character of $W_i$ on $V$. Thus, $\tau$ appears in $1_{W_i}^W$ with positive multiplicity (and, hence, multiplicity 1).
If \( \tau \in \mathcal{W} \), then \( \mathfrak{l}(w_0) \in \tau(\mathfrak{l}(w_0)) \). However, if \( W \) is not of type \( E_6 \), then \( w_0 \) is stabilizes \( V_1 = V_2 \) and is \(-1\) on \( V/ V_2 \) [8, p. 261]. In any case, \( V_1 \) is the natural module for the reflection representation of \( W \), so \( \widetilde{\mathfrak{w}}_1 \) is irreducible on \( V_1 \). In particular, \( \widetilde{\mathfrak{w}}_1 \) fixes no vector of \( V \), so \( \tau \notin \mathcal{W} \).

It follows that \( \tau \in \lambda \), so the degrees of the irreducible constituents of \( \lambda \) are \( \tau(1) \) and \( |W : \mathfrak{w}_1| - \tau(1) \). The degrees of the three irreducible constituents of \( \mathcal{W}_1 \) can be found by using the results of Frame [39, Chapter 5] or Higman [21], or by guessing and elimination. The results are given in Table 4.

In Table 4 we have also listed the index \( |G : G_1| \) and degree of the reflection character \( \rho \) of \( G \) (see (5.4)), which will be needed later. We will also need to use another parabolic subgroup later, when \( G \) is \( F_4(q) \), \( E_6(q) \), or \( E_7(q) \).

(4.3) Proposition. (i) Let \( W \) have type \( F_4 \). Then \( \mathcal{W}_4 \) decomposes into five irreducible characters of degrees 1, 2, 9, 4, and 8. Of these, the ones also in \( \mathcal{W}_1 \) have degrees 1, 4, and 9.

(ii) Let \( G = E_6(q) \). Then \( \mathcal{W}_6 \) is the sum of three irreducible characters of degrees 1, 6, and 20, all of which occur in \( \mathcal{W}_2 \). Also, \( |G : G_6| = (q^9 - 1)(q - 1)^{-1} \cdot (q^{12} - 1)(q^4 - 1)^{-1} \).

(iii) Let \( G = E_7(q) \). Then \( \mathcal{W}_7 \) decomposes into four irreducible characters, of degrees 1, 27, 7, and 21, of which only the first three appear in \( \mathcal{W}_1 \). Also, \( |G : G_7| = (q^7 + 1)(q^{14} + 1)(q - 1)^{-1} \).

Proof. In (i), (ii), and (iii), let \( j = 4, 6, \) and 7, respectively. Then \( (\mathcal{W}_4, \mathcal{W}_6) = 5, 3, \) and 4, respectively. For (ii) and (iii) this is proved in [23]. For (i) it can be deduced by applying the graph automorphism of \( W \) to \( W_1 \); alternatively, we could proceed as in (4.2), replacing \( r \) by \( s = \alpha_4 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 \). The indices \( |G : G_j| \) are easy to compute.

We next claim that \((\mathcal{W}_4, \mathcal{W}_6) = 3 \). To prove this, we must find the number of orbits of \( W_j \) on \( (r) W_j \). This is easy to do, using the roots given in [8] and the action of the reflections on each root.

This proves (ii), since the reflection character of \( W \) appears in \( \mathcal{W}_6 \). To find the degrees in (iii), introduce \( \mathfrak{w}_j = W_j(w_0) \) as in the proof of (4.2). This time, \( \mathcal{W}_j \) is the sum of just two characters, of degrees 1 and 27. Comparison with Table 4 completes the proof of (iii).

It remains only to show that for \( W \) of type \( F_4 \), \( \mathcal{W}_4 \) and \( \mathcal{W}_4 \) have in common an irreducible character of degree 9; we already know by (4.2) that they have \( \mathfrak{w}_4 \) and the reflection character in common. We will show that the third common character \( \varphi \) cannot have degree 2 or 8.

Suppose \( \varphi(1) = 8 \). Set \( \mathfrak{w}_4 = W_4(w_0) \). The proof of (4.2) shows that \((\mathcal{W}_4, \mathcal{W}_4) = 1 \). Then \( W = \mathfrak{w}_4 \). Since \( \mathfrak{w}_4 \cap \mathfrak{w}_4 \) contains \( W_4(w_0) \) of order 16, \( |W| \) divides \((2^5 \cdot 3)/2^4 \), which is not the case.

Finally, suppose \( \varphi(1) = 2 \). Then \( \varphi|W_4 - 1 W_4 \) and \( \varphi|W_4 - 1 W_4 \) are linear. Consequently, the reflections \( s_2, s_3, \) and \( s_4 \) commute mod \( \ker \varphi \), which is absurd. This proves (4.3).
The remainder of this section will be devoted to the study of the structure of parabolic subgroups of $G$.

(4.4) Proposition. Let $G = E_6(q), E_7(q), \text{or } E_8(q)$, and let $r$ and $i$ be as before (see (4.1) and Table 4).

(i) $Q_i$ is a special group with center $U_r$, and has order $q^{21}, q^{33}, \text{or } q^{57}$, respectively.

(ii) $G_i = N(U_r) = C(U_r)H$ and $L_i \leq C(U_r)$, where $L_i/Z(L_i) \approx A_5(q), D_6(q), \text{or } E_7(q)$, respectively.

(iii) $Q_i/U_r$ can be turned into an $F_q$-space such that the commutator function induces a nondegenerate alternating form on $Q_i/U_r$. Moreover, $L_i$ acts on $Q_i/U_r$ as a group of $F_q$-linear transformations preserving this form.

Proof. Again let $Q_i$ consist of those roots with $i$th coefficient $1$. Then $Q_i = \langle U_r, U_s \mid s \in \mathcal{O}_i \rangle$ [8, pp. 260–270]. Let $s, t \in \mathcal{O}_i$. Then, since the Dynkin diagram of $G$ is simply-laced, the commutator relations (2.1) show that $[U_s, U_t] = 1$ if and only if $s + t$ is not a root. Moreover, if $s + t$ is a root, then $s + t = r$.

Conversely, if $s \in \mathcal{O}_1$, we claim that $r - s \in \mathcal{O}_1$. For, by (4.1) and the definition of $i$ in Table 4, $r - \alpha_i = (r)x_i \in \mathcal{O}_1$. Since $\mathcal{O}_1$ is an orbit of $W_i$, we can write $s = (\alpha_i)w$ with $w \in W_i$. It follows that $r - s = (r - \alpha_i)w \in \mathcal{O}_1$.

Thus, $Q_i$ is the central product of the groups $\langle U_s, U_{r-s} \rangle = U_sU_rU_{r-s}$, each of which is special of order $q^3$ with center $U_r$. Hence, $Q_i$ is special. Its order is easily found using (2.2), as is the structure of $L_i$. Also, $L_i$ centralizes $U_r$, so $C(U_r) \supseteq Q_iL_i$. Then $N(U_r) \supseteq Q_iL_iH = G_i$, and, hence, $G_i = N(U_r) = C(U_r)H$ by the maximality of $G_i$.

It remains to prove (4.4)(iii). Let $H$ consist of all the elements $h(\chi)$, with $\chi$ a character of the additive group generated by the roots into $F_q^*$. Then $H \supseteq H$, and $L_iH$ and $Q_iL_iH$ are groups. Let $H_0 = \{h(\chi) \in H | \chi(\alpha_j) = 1 \text{ for all } j \neq i \}$. Then $|H_0| = q - 1$, and $H_0$ centralizes $L_i$ while acting on $Q_i$. Moreover, if $h(\chi) \in H_0$, then $U_i(a)h(\chi) = U_i(\chi(\alpha_i)a)$ for all $s \in \mathcal{O}_1$ and $a \in F_q$. Consequently, $H_0$ acts fixed-point-freely on $Q_i/U_r$.

If $0 \neq a \in F_q$, let $h_a \in H_0$ be the unique element for which $h_a = h(\chi) \in H_0$ and $\chi(\alpha_i) = a$. Then $Q_i/U_r$ becomes an $F_q$-space as follows: for $v \in Q_i/U_r$, define $av = y^h_aU_r$. Since $L_i$ centralizes $H_0$, it acts as a group of $F_q$-transformations on this vector space. Finally, $U_r$ can be regarded as a field via the correspondence $t \mapsto U_r(t)$. From the commutator relations (2.1), it follows that the commutator function is a nondegenerate alternating form on the $F_q$-space, preserved by $L_i$. This completes the proof of (4.4).

(4.5) Proposition. Let $G = F_4(q)$.

(i) $|Q_1| = q^{15}$, and $L_1/Z(L_1) \approx PSp(6, q)$. If $q$ is odd, then $Q_1$ is special with center $U_r$ (cf. (4.1)) of order $q$; $G_1$ acts irreducibly on $Q_1/U_r$. If $q$ is even, then $Q_1 = LS$ with $[L, S] = 1, L \cap S = U_r, L \text{ special with center } U_r, \text{ and } S \text{ an elementary abelian normal subgroup of } G_1 \text{ of order } q^7$; moreover, $G_1$ acts irreducibly on $U_r, S/U_r$, and $Q_1/S$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(ii) \(|Q_4| = q^{15}\) and \(L_4 \cong SO(7, q)'\). \(G_4\) has a normal elementary abelian subgroup \(R_4\) of order \(q^7\) such that \(U_s < R_4 < Q_4\), where \(s = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4\). \(G_4\) acts irreducibly on \(Q_4/R_4\).

(iii) If \(q\) is odd, then \(L_4\) acts on \(R_4\) as a group of \(F_q\)-transformations preserving a nondegenerate symmetric form. The isotropic 1-spaces of \(R_4\) are conjugates of root groups \(U_\alpha\) with \(\alpha\) a long root.

(iv) If \(q\) is even, then \(U_s \leq G_4\). \(L_4\) acts on \(R_4\) as a group of \(F_q\)-transformations preserving a quadratic form for which the radical of \(R_4\) is \(U_s\). The singular 1-spaces of \(R_4\) are conjugates of groups \(U_\alpha\) with \(\alpha\) a long root.

(v) \(G_4 = N(U_s) = C(U_s)H\). If \(q\) is even, \(G_4 = N(U_s) = C(U_s)H\).

(4.6) Proposition. Let \(G = 2E_6(q)\).

(i) \(\beta_1\) is special of order \(q^{21}\) with center \(U_\beta\) of order \(q\). \(G_1\) acts irreducibly on \(Q_1/U_\beta\). Moreover, \(G_1 = N(U_\beta) = C(U_\beta)H\).

(ii) \(|Q_4| = q^{24}\) and \(L_4 \cong SO^{-}(8, q)'\). \(G_4\) has a normal elementary abelian subgroup \(R_4\) of order \(q^8\) such that \(U_s < R_4 < Q_4\), where \(s = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4\). \(G_4\) acts irreducibly on \(Q_4/R_4\).

(iii) \(L_4\) acts on \(R_4\) as a group of \(F_q\)-transformations preserving a quadratic form. The isotropic 1-spaces (or singular, if \(q\) is even) are conjugates of root groups \(U_\alpha\) with \(\alpha\) a long root.

Proofs. Let \(G = F_4(q)\) or \(2E_6(q)\), so \(W\) is of type \(F_4\). Then \(W\) has two orbits on \(\Delta\): the long and short roots. Here \(\alpha_2\) and \(r\) are long while \(\alpha_3\) and \(s\) are short. The action of \(W\) is determined by the following equations.

\[
(a_j)s_j = -a_j \quad \text{and} \quad (a_j)s_k = a_j \quad \text{for} \quad |j - k| > 1,
\]

\[
\begin{align*}
(a_2)s_1 &= \alpha_1 + \alpha_2, \quad (a_3)s_4 = \alpha_3 + \alpha_4, \\
(a_1)s_2 &= \alpha_1 + \alpha_2, \quad (a_3)s_2 = \alpha_2 + \alpha_3, \\
(a_2)s_3 &= \alpha_2 + 2\alpha_3, \quad \text{and} \quad (a_4)s_3 = \alpha_3 + \alpha_4.
\end{align*}
\]

(4.7)

From this information it is easy to determine all roots. In particular, let \(L_m^I\) (and \(S_m^I\)) be the set of long (or short) roots for which \(m\) is the coefficient of \(a_i\). Then

\[
L_1^I = \{\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + 2\alpha_3, \alpha_1 + 2\alpha_2 + 2\alpha_3, \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4\},
\]

\[
S_1^I = \{\alpha_1 + \alpha_2 + \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_2 + 2\alpha_3 + \alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4\},
\]

and \(Q_1 = \langle U_\alpha | \alpha \in \{r\} \cup L_1^I \cup S_1^I \rangle\). Moreover, \(W_1 = \langle s_1, s_2, s_3 \rangle\) is transitive on both \(L_1^I\) and \(S_1^I\) by (2.4). It follows that root groups \(U_\alpha, U_\beta \leq Q_1\) are conjugate under \(W_1\) if and only if \(\alpha\) and \(\beta\) are roots of the same length.

Before proceeding further, we note the following facts.
Lemma. Let $\alpha$ and $\beta$ be positive roots in $\Delta$.

(i) If $\alpha + \beta$ is not a root, then $[U_\alpha, U_\beta] = 1$.

(ii) If $\alpha$ and $\beta$ are long, and $\alpha + \beta$ is a root, then $\alpha + \beta$ is long. Suppose $\alpha, \beta,$ and $\alpha + \beta$ are all long or all short. Then $[U_\alpha, U_\beta] = U_{\alpha + \beta}$ whenever $1 \not\in U_\alpha$.

(iii) Suppose $\alpha$ is short, $\beta$ is long, and $\alpha + \beta$ is a root. Then $\alpha + \beta$ is short, $2\alpha + \beta$ is long, $[U_\alpha, U_\beta] < U_{\alpha + \beta}U_{2\alpha + \beta}$, and $[U_\alpha, U_\beta] \neq U_{2\alpha + \beta}$. Moreover, $[g, U_\beta] = U_{\alpha + \beta}$ whenever $1 \not\in U_\beta$.

(iv) Suppose $\alpha$ and $\beta$ are short and $\alpha + \beta$ is a long root. If $G = F_4(q)$ with $q$ even, then $[U_\alpha, U_\beta] = 1$. In all other cases, $[U_\alpha, U_\beta] = U_{\alpha + \beta}$, $(U_\alpha, U_\beta)$ is special with center $U_{\alpha + \beta}$, and $[g, U_\beta] = U_{\alpha + \beta}$ whenever $1 \not\in U_\beta$.

Proof. This can be proved as follows. By [10], we can write $\alpha = \alpha_1$ and $\beta = m_1\alpha_1' + m_2\alpha_2'$, where $\alpha_1'$ and $\alpha_2'$ are roots generating a root system of rank 2 and $m_1, m_2 \in \mathbb{Z}$. Now (4.8) can be checked from the structure of the rank 2 subgroup $<U_{\alpha_1'}, U_{\alpha_2'}> = T$, where $T/Z(T) \approx \text{PSp}(3, q), \text{PSp}(4, q), \text{or} \text{PSU}(4, q)$.

We now return to the proof of (4.5) and (4.6). By [8, p. 272], $r$ is the only root for which $\alpha$ has coefficient 2. Thus, for $\alpha, \beta \in \Delta = \Delta_1 \cup \Delta_2$, $\alpha + \beta$ is a root if and only if $\alpha + \beta = r$. Also, $r - \alpha_1 \in \Delta_1$ and $r - (\alpha_1 + \alpha_2 + \alpha_3) \in \Delta_1$. Consequently, the transitivity of $W_1$ on $\Delta_1$ and $\Delta_2$ implies that $r - \alpha \in \Delta_1$ if $\alpha \in \Delta_1$ and $r - \alpha \in \Delta_2$ if $\alpha \in \Delta_2$. Now (4.8) implies that, except when $G = F_4(q)$ with $q$ even, $Q_1$ is the central product of the special groups $<U_\alpha, U_{r-a}> = U_\alpha U_{r-a}$, $\alpha \in \Delta_1 \cup \Delta_2$, each having center $U_r$, so $Q_1$ is special and $Z(Q_1) = U_r$. Set $L = <U_\alpha | \alpha \in \Delta_1 \cup \{r\}>$ and $S = <U_\beta | \alpha \in \Delta_1 \cup \{r\}>$. When $G = F_4(q)$ with $q$ even, (4.8) implies that $Q_1 = LS$ with $[L, S] = 1, L \cap S = U_r$, $S$ elementary abelian, and $L$ special with center $U_r$. In any case, $|Q_1|$ is determined by (2.2).

When $G = F_4(q)$ with $q$ even, $S \leq G_1$. For $W_1$ permutes the groups $U_\alpha, \alpha \in \Delta_1$. Also, $H$ normalizes $S$. Thus, we need only check that $U$ normalizes $S$. Consider $U_\alpha \prec S$ and $U_\beta$ with $\beta \in \Delta^+$. If $\beta$ is short then $[U_\alpha, U_\beta] \leq S$ by (4.8)(ii) and (iv).

If $\beta$ involves $\alpha_1$, we have already seen that $[U_\alpha, U_\beta] = 1$. Suppose $\beta$ is long and does not involve $\alpha_1$. By (4.8)(iii), $\alpha + \beta \in \Delta_1$, while $2\alpha + \beta$ is a root with first coefficient 2. Then $2\alpha + \beta = r$, and hence $[U_\alpha, U_\beta] \leq U_{\alpha + \beta}U_{2\alpha + \beta} \leq S$. Thus, $S \leq G_1$ in this case.

Since $r$ is the root of maximal height, $U_r \preceq Z(U)$. Moreover, $W_1$ fixes $r$ and $H$ normalizes $U_r$, so $C(U_r) \supseteq \langle U, W_1 \rangle = Q_1 L_1$ and $N(U_r) \supseteq Q_1 L_1 H = G_1$. By the maximality of $G_1$, we have $G_1 = N(U_r) = C(U_r)H$. If $G = F_4(q)$ with $q$ even, then the graph automorphism of $G$ interchanges the roots $r$ and $s$ and the parabolic subgroups $G_1$ and $G_4$. Thus, in this case we have $G_4 = N(U_r) = C(U_r)H$. This proves (4.5)(v) and the last part of (4.6)(ii).

The rest of (4.5)(i) and (4.6)(i) is either contained in the following lemma or is obtained by very similar methods.

Lemma. If $q$ is odd or $G$ is not $F_4(q)$, then $G_1$ acts irreducibly on $Q_1/U_r$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. Suppose that $M$ is a proper $G_j$-submodule of $V = Q_j/U_j$. Let bars denote images in $V$. Choose $\alpha \in L^1_1 \cup S^1_1$, and suppose that $\bar{\alpha} \cap M \neq 1$. Since $H$ acts irreducibly on $\bar{U}_\alpha$, $\bar{U}_\alpha \leq M$. Thus, $\bar{U}_\alpha \leq M$ for all $\alpha \in L^1_1$, or for all $\alpha \in S^1_1$, but not both as $M \neq V$. Suppose $\alpha \in S^1_1$. Then $\alpha + \beta \in L^1_1$ for some short root $\beta$, where $U_\beta \leq G_j$, and then $M \supseteq [\bar{U}_\alpha, U_\beta] = \bar{U}_{\alpha+\beta}$ by (4.8)(iv). We must thus have $\alpha \in L^1_1$. Then there is a short root $\beta$ such that $\alpha + \beta \in S^1_1$. By (4.8)(iii), $\alpha + 2\beta = r$. Also, $U_\beta \leq G_j$, so by (4.8)(iii) we have $[\bar{U}_\alpha, U_\beta] \leq M \cap \bar{U}_{\alpha+\beta} = M \cap \bar{U}_{\alpha+\beta}$ and $[\bar{U}_\alpha, U_\beta] \neq 1$. Thus, $M \cap \bar{U}_{\alpha+\beta} \neq 1$ for a short root $\alpha + \beta$, and this is impossible.

Thus, $\bar{U}_\alpha \cap M = 1$ for all $\alpha \in L^1_1 \cup S^1_1$. The rest of the proof depends on the following "separation" properties, each of which is easily proved by inspection using the transitivity of $W_1$ on $L_1^1$, $S_1^1$, and $L_0^1 = \{\pm \alpha_2, \pm (\alpha_2 + 2\alpha_3), \pm (\alpha_2 + 2\alpha_3 + 2\alpha_4)\}$:

(a) if $\alpha \neq \beta$ and $\alpha, \beta \in S_1^1$, there is a long root $\lambda \in L_0^1$ such that $\alpha + \lambda \in L_1^1$ and $\beta + \lambda$ is not a root; (b) if $\lambda \in L_0^1$, there is a unique root $\lambda^* \in S_1^1$ such that $\lambda + \lambda^*$ is a root; and (c) if $\alpha \in L_1^1$ and $\beta \in S_1^1$, there is a long root $\lambda \in L_0^1$ such that $\alpha + \lambda \in L_1^1$ and $\beta + \lambda$ is not a root.

These are used as follows. Note that $U_\lambda \leq G_j$ for all $\lambda \in L_0^1$. Take $v \neq 1$ in $M$, and let $\Sigma(v)$ be minimal among those subsets $\Sigma$ of $L_1^1 \cup S_1^1$ such that $v \in \Pi_{\alpha \in \Sigma} \bar{U}_\alpha$. Then choose $v$ with $|\Sigma(v)|$ minimal; we know this number is $> 1$. Let $\alpha, \beta \in \Sigma(v)$ with $\alpha \neq \beta$. Then, interchanging $\alpha$ and $\beta$ if necessary, (a), (b), and (c) imply the existence of a long root $\lambda \in L_0^1$ such that $\alpha + \lambda$ is a root in $L_1^1 \cup S_1^1$ having the same length as $\alpha$, while $\beta + \lambda$ is not a root. By (4.8), we can find $g \in U_\lambda$ such that $1 \neq [g, v] \in M$ and $|\Sigma([g, v])| < |\Sigma(v)|$. This contradiction proves the lemma.

We now turn to $G_4$. We will consider the following sets of roots.

$L_2^4 = \{\alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4, \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4\}$,

$A_1 = \{\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3, \alpha_1 + \alpha_2 + 2\alpha_3, \alpha_1 + 2\alpha_2 + 2\alpha_3\}$.

Set $R_4 = \langle U_\alpha | \alpha \in L_2^4 \cup \{s\} \rangle$, where $L_2^4 \cup \{s\}$ consists of all roots with $\alpha_4$-coordinate 2. The commutator relations (2.1) imply that $R_4$ is an elementary abelian normal subgroup of $G_4$. Then $G_4$ acts on $Q_4/R_4$ and $R_4$. Using the methods of (4.9) it is not difficult to see that $G_4$ acts irreducibly on $Q_4/R_4$. Also, $|U_1| = |U_2| = q$, while $|U_4| = |U_2| = q$ if $G = F_4(q)$ and $|U_4| = |U_2| = q^2$ if $G = 2E_6(q)$. Thus, $|R_4| = q^7$ if $G = F_4(q)$ and $|R_4| = q^8$ if $G = 2E_6(q)$.

It remains only to determine that the action of $L_4$ on $R_4$ is as in (4.5) or (4.6), and that $L_4 \simeq SO(7, q)'$ or $SO^-(8, q)'$. From the Dynkin diagram we know that $L_4$ is a central extension of $SO(7, q)'$ or $SO^-(8, q)'$ (see (2.2) and Table 2). Thus, it suffices to show that $R_4$ can be regarded as an $F_q$-space having a form of the appropriate type preserved by $L_4$.

First note that $A_1$ consists of all roots in a system of type $B_3$ having first coordinate 1. Let $X = \langle U_\alpha | \alpha \in A_1 \rangle$. We apply (3.1) to the group $L_4$. The group $X$
is elementary abelian and has the structure of an $F_q$-space. Moreover, this space has 

a nondegenerate quadratic form preserved by $L_{14}$. The radical of $X$ is 0 unless $q$ is 
even and dim($X$) is odd; that is, when $G = F_q(q)$, with $q$ even, in which case rad($X$) = 

$U_{a}$, where $a = a_1 + a_2 + a_3$. In any case, the isotropic (or singular, if $q$ is even) 

1-spaces of $X$ are the conjugates of the root groups $U_{a}$ with $a$ a long root.

Set $w = s_4s_3s_2s_3s_4$. Then

$$(A_1)^w = \{a_1 + 2a_2 + 2a_3 + a_4, a_1 + 2a_2 + 2a_3 + 2a_4, a_1 + 2a_2 + 2a_3 + 4a_4, s\},$$

(4.10) $$(A_1)^w = \{a_1 + 2a_2 + 2a_3 + a_4, a_1 + 2a_2 + 2a_3 + 2a_4, a_1 + 2a_2 + 2a_3 + 4a_4, s\}.$$ 

Also, $(a_2)^w = a_2$ and $(a_3)^w = a_3$, so $w$ centralizes $L_{14}$. Consequently, $L_{14}$ acts on 

$X^w = \langle (A_1)^w \rangle$ as it does on $X$.

By (4.10), $(A_1)^w \cup (A_1)^w s_1 = L_{2}^4 \cup \{s\}$, so $R_4 = X^w X^{w s_1}$. In fact, $R_4 = 

X^w \times Y$ with $Y = U_{a_1 + a_2 + a_3 + 2a_4}$. Since $a_2 + 2a_3 + 2a_4$ is the only member of 

$L_{2}^4 \cup \{s\}$ not involving $a_1$, (4.8)(i) implies that $[L_{14}, Y] = 1$. Conjugating by $s_1$, we 

find that $R_4 = X^{w s_1} Y^{s_1}$ with $[L_{14}^1, Y^{s_1}] = 1$. By definition, $L_{14} = \langle U_2, U_3, U_{-2}, 

U_{-3} \rangle$, so $L_{14}^1 = \langle U_{a_1 + a_2}, U_3, U_{(a_1 + a_2)}, U_{-3} \rangle$. Since $[U_{a_1 + a_2}, U_{-2}] = U_1$, it 

follows that $L_4 = \langle L_{14}, L_{14}^1 \rangle$. We will determine the action of $L_4$ on $R_4$ by using 

the known actions of $L_{14}$ and $L_{14}^1 = L_{14}^{w s_1}$.

First we switch to additive notation: write $V = R_4$, $V_1 = (X)^w$, and $V_2 = Y$, so 

$V = V_1 \oplus V_2$. We know that $V_1$ is an $F_q$-space, so each $a \in F_q$ determines a scalar 
multiplication $v \mapsto av$ on $V_1$. There is also a scalar action on $(V_1)^s_1$. We have $V = 

(V_1)^s_1 \oplus (V_2)^s_1$, and $(V_1)^s_1 = V_2 \oplus V_2'$, where $V_2' = (V_1)^s_1 \cap V_1$. We thus have 
two scalar actions on $V_2'$, one determined by $V_1$ and the others by $(V_1)^s_1$. Here, 

$V_2' = U_2 \oplus U_{a_1 + 2a_2 + 2a_3 + 2a_4} \oplus U_{a_1 + 2a_2 + 4a_3 + 2a_4}$. 

Also, the commutator relations imply that 

$$[U_{+1}, U_{-1}] = [U_{+1}, U_{a_1 + 2a_2 + 2a_3 + 2a_4}] = [U_{+1}, U_{a_1 + 2a_2 + 4a_3 + 2a_4}] = 1.$$ 

Thus, $(U_{+1}, U_{-1})$ centralizes $V_2'$, and consequently, $s_1$ centralizes $V_2' = V_1 \cap (V_1)^s_1$. 

It follows that the scalar action on $(V_1)^s_1$ obtained from that on $V_1$ agrees on the 

overlap of the two spaces, and consequently, $V = V_1 + (V_1)^s_1$ becomes an $F_q$-space. 

We know that $L_{14}$ acts on $V_1$, while inducing the identity on $V_2$, and a similar statement 

holds for $L_{14}^1$. Thus, $L_1 = \langle L_{14}, L_{14}^1 \rangle$ acts on $V$ as a group of $F_q$-linear 

transformations.

Consider the action of $L_{14}^1 \approx SO(5, q')$ or $SO^*(6, q')$ on the space $(V_1)^s_1$. 

Clearly $L_{124} = \langle U_3, U_{-2} \rangle = L_{14}^1$. Here $L_{14}^1$ is contained in a proper parabolic 

subgroup of $L_{14}$, and since $a_2$ is long, it follows as in (3.1) that $L_{124}$ stabilizes an 

isotropic (or singular) 1-space $(v) \not\in$ rad($V_1)^s_1$). (Actually, rad($V_1)^s_1$) is 0 except 

when $G = F_4(q)$ with $q$ even, in which case it is a 1-space.) Moreover, $L_{124}$ induces
SO(3, q)' or SO^~(4, q)' on \langle \omega \rangle / \langle \omega \rangle and acts irreducibly on this space, or \( G = F_4(q) \) with \( q \) even and \( L_{124} \) acts irreducibly on \( \langle \omega \rangle / \langle \omega \rangle + \text{rad}((V_1)_s) \), inducing \( Sp(2, q) \) there. Now \( L_{14} \) is trivial on \( V_2 \), so \( L_{124} \leq L_{14}^2 \) is trivial on the subspace \( V_2 \) of \((V_1)_s\). Thus, if \( \text{rad}((V_1)_s) = 0 \), then \( V_2 \) must be a hyperbolic plane. If \( \text{rad}((V_1)_s) \neq 0 \), then by (3.1) we have \( \text{rad}((V_1)_s) = U_{s_1} + U_{s_2} + U_{s_3} = U_s \leq V_2 \); once again it follows that \( V_2 \) is a hyperbolic plane. In either case, since \( L_{124}^2 \) fixes \( V' \) we have \( (V_1)_s = V_2 \perp V' \).

Similarly, \( V_1 \) is the usual module for \( L_{14}^4 \), and we can write \( V_1 = V_2 \perp V_2' \) for a hyperbolic plane \( V_2' = (V_2)_s^{-1} \). We can now induce a quadratic form on \( V \) as follows.

The decomposition \( V = V_2 \oplus V_2' \oplus V_2 \) will be orthogonal. The subspaces \( V_2 \) and \( V_2' \) will be hyperbolic planes, on which the quadratic forms are determined by \( L_{14} \) and \( L_{14}^2 \), respectively. The form on \( V \) restricts to \( V_1 \) and \( (V_1)_s \) in the obvious way. This is well defined. Indeed, as before, \( s_1 \) is trivial on \( V_2 = V_1 \cap (V_1)_s \), so the forms on \( V_1 \) and \( (V_1)_s \) agree on their intersection \( V_2' \).

Finally, \( L_{14}^4 \) is trivial on \( V_2' \) and \( L_{14} \) is trivial on \( V_2^* \). Thus, \( L_4 = \langle L_{14}^2, L_{14}^4 \rangle \) preserves the form. Moreover, it is clear that the form is nondegenerate and the radical is trivial unless \( G = F_4(q) \) with \( q \) even. In the latter case \( \text{rad}(V) = \text{rad}((V_1)_s) = U_s \).

Since a vector in \( V_1 \) is isotropic (or singular) in \( V_1 \) if and only if it is in \( V \), we can apply (3.1) to complete the proof of the propositions.

(4.11) **Lemma.** Let \( G = E_8(q) \) and let \( \chi \neq 1_G \) be an irreducible character of \( G \). Then \( \chi(1) \geq q^{28}(q - 1) \).

**Proof.** Let \( Q = Q_8 \), and consider \( \chi|Q \). By (4.4) \( Q \) is special of order \( q^{57} \), \( |U| = |Z(Q)| = q \), and if \( |Z(Q) : T| = p \), then \( Q/T \) is extraspecial of order \( q^6p \). Let \( \varphi \) be a nonlinear irreducible constituent of \( \chi|Q \), and set \( T = Z(Q) \cap \ker \varphi \). Then \( |Z(Q) : T| = p \) and \( \varphi \) is faithful on \( Q/T \). Thus, \( \varphi(1) = q^{28} \). Also, \( \varphi \) is determined by \( \varphi(Z(Q)) \). Since \( H \) is transitive on \( U_r^* = Z(Q)^* \), \( \varphi^h \in \chi|Q \) for each \( h \in H \), \( \chi(1) \geq q^{28}(q - 1) \), as claimed.

5. **The constituents of \( 1_G^* \).** The following terminology will be used throughout §§5–7.

(5.1) **Definition.** Fix a type of Chevalley group, of normal or twisted type, of rank \( n \geq 3 \), whose Dynkin diagram is in Table 1. Let \( S = \{G(q)|q \text{ is a prime power}\} \) be the set of all Chevalley groups of the given type; all have the same Coxeter system \( (W, R) \), where \( R = \{s_1, \ldots, s_n\} \) is as in §2. Here, \( q \) is related to \( G(q) \) in such a way that the following statements hold. (A more general situation is studied in [5], [12], and [19].) Let \( B(q) \) be a Borel subgroup of \( G(q) \). Then there are positive integers \( c_1, \ldots, c_n \) such that

(i) \( c_i = c_j \) if \( s_i \) and \( s_j \) are conjugate in \( W \);
(ii) \( |B(q) : B(q) \cap B(q)^a| = q^{c_1} \);
(iii) \( |U| = q^{c_1} \); and
(iv) all \( c_i \) are 1 for groups of normal type, the \( c_i \)'s for the classical groups are given in Table 5, and for \( 2E_6(q), c_1 = c_2 = 1, c_3 = c_4 = 2 \).
Groups of rank $n \leq 2$ will be handled separately.

<table>
<thead>
<tr>
<th>Type of Group</th>
<th>$c_1 = \cdots = c_{n-1}$</th>
<th>$c_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2A_{2n}(q)$</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>$2A_{2n-1}(q)$</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$B_n(q)$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$C_n(q)$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$D_n(q)$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$2D_{n+1}(q)$</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

(5.2) **Proposition** [5], [12]. Let $S$ be as in (5.1). Then, corresponding to each irreducible character $\psi$ of $W$, there is a polynomial $d_\psi(i) \in \mathbb{Q}[t]$, called the generic degree associated with $\psi$, having the following properties.

For each prime power $q$, there is a bijection $\psi \mapsto \xi_{\psi,q}$ between the irreducible characters $\psi$ of $W$ and the irreducible constituents $\xi_{\psi,q}$ of $1_{G(q)}$, such that

$$d_\psi(q) = \xi_{\psi,q}(1), \quad d_\psi(1) = \psi(1),$$

and

$$(\psi, 1^W_j) = (\xi_{\psi,q}, 1_{G(q)}^\mathbb{Q})$$

for each subset $J$ of $\{1, \ldots, n\}$.

(5.3) **Lemma.** Let $h(t) = \sum \psi(1)d_\psi(t)$, where the sum is taken over the distinct irreducible characters of $W$. Then for all prime powers $q$, $h(q) = |G(q) : B(q)|$.

**Proof.** By (5.2), $1_{G(q)}^\mathbb{Q} = \sum \psi(1)\xi_{\psi,q}$. Evaluating both sides at 1 yields the result.

(5.4) **Proposition** [12]. Let $S$ be as in (5.1) and (5.2). Let $\varphi$ denote the character of the usual reflection representation of $W$. Then $\xi_{\varphi,q} = \rho$ is called the reflection character of $G(q)$. The degree of $\rho$ is given in Tables 3 and 4. Moreover, $(\rho, 1_{G(q)}^\mathbb{Q}) = |J|$ for each $J \subset \{1, \ldots, n\}$.

We remark that groups of rank 2 also have reflection characters $\rho$, whose degrees are given in (7.26). We also note that the degrees $\rho(1)$ for $E_6(q)$ and $^3D_4(q)$ are stated incorrectly in [12].

$\Phi_j(t)$ will denote the $j$th cyclotomic polynomial.

(5.5) **Proposition.** Let $S$ be as in (5.1) and (5.2). Fix an irreducible character $\psi \neq 1^W$ of $W$, and set $f(i) = d_\psi(i)$. Then the following statements hold.

(i) $f(i) = \alpha^k f^{#}(i)$, where $0 < \alpha \in \mathbb{Q}$, $1 \leq k \in \mathbb{Z}$, and $f^{#}(i)$ is a product of cyclotomic polynomials other than $t - 1$; in particular, $f^{#}(0) = 1$ and $f^{#}(i)$ is monic.

(ii) Write $|G(q) : B(q)| = g(q)$, so $g(i) \in \mathbb{Z}[t]$ is a product of cyclotomic poly-
nomials other than \( t - 1 \). Then

\[ f^\#(t), g(t), z(t) \prod_{i=1}^n [(f^\#(i) - 1)(t - 1)^{-1}], \]

where \( z(t) = 1 \), except that \( z(t) = (t^2 - 1) / (t^3 - 1) \), when \( G = \text{PSU}(2n + 1, q) \). In particular, if \( G \) is of normal type, then \( f^\#(t), g(t) \).

(iii) Write \( \alpha = a/b \), with \( 1 < a, b \in \mathbb{Z} \) and \( (a, b) = 1 \). Then \( (a/b) f^\#(1) = f(1)|W|, a|W|, b|f^\#(1) \), and \( b|g(1)z(1) \prod_{i=1}^n c_i \). In particular, \( b|g(1) \) for groups of normal type.

(iv) If \( p > 1 \) is a prime, then \( p^{k+1} | b \).

(v) Let \( q = p^j \), where \( p \) is a prime and \( j \geq 1 \). Then \( p^n \nmid f(q) \) if and only if \( q = p, p|W| \), and \( p^{k}|b| \).

**Proof.** By (5.2), we can write \( f(t) = \alpha t^k f^\#(t) \), with \( \alpha \in \mathbb{Q}, k \geq 0 \), and \( f^\#(0) = 1 \). For each prime power \( q \), \( f(q)|G(q)| \), where \( |G(q)| = q^n g(q) z(q) \prod_{i=1}^n (q^{ci} - 1) \), for some positive integer \( N \). Consequently, \( f^\#(t)|g(t)z(t) \prod_{i=1}^n (t^{ci} - 1) \). Then \( f^\#(t) \) is a product of cyclotomic polynomials. Since \( \psi(1) = \alpha f^\#(1) \neq 0 \), \( t - 1 \) does not appear in the factorization of \( f^\#(t) \). Since \( \Phi_j(1) > 0 \) for all \( j > 1, f^\#(1) > 0 \) and, hence, \( \alpha > 0 \).

In order to prove that \( k \geq 1 \), we first note that \( h(t) = \sum \psi(1) d_\psi(t) \) is, by (5.3), a polynomial such that \( h(0) = 1 \). Therefore \( h(t) - 1 = \sum_{\psi \neq 1} \psi(1) d_\psi(t) \), and since each \( d_\psi(t) = \alpha_\psi t^k f^\#(t) \), with \( \alpha_\psi > 0 \), and \( f^\#(0) = 1 \), we have, by evaluating both sides at \( t = 0 \), the result that \( k_\psi > 0 \) for every \( \psi \neq 1 \). This completes the proof of (i) and (ii), since all \( c_i = 1 \) for groups of normal type.

Clearly \( (a/b) f^\#(1) = f(1) = \psi(1)|W|, a|W|, \) and \( b|f^\#(1) \). By (ii), \( b|g(1)z(1) \prod_{i=1}^n c_i \). This proves (iii).

To prove (iv), suppose \( p^{k+1} | b \). Here \( f(p) = (a/b)p^{k} f^\#(p) \). Since \( f(p) \) and \( f^\#(p) \) are integers and \( f^\#(p) \equiv 1 \) (mod \( p \)) by (i), this is impossible.

Finally, suppose \( q = p^j \) with \( p \) a prime, where \( p \nmid f(q) \). Then \( p^n \nmid (a/b) q^kf^\#(q) \), so \( q^k | b \). By (vi), \( p = q, \) so \( p^n \nmid b \). Moreover, \( b|g(1)z(1) \prod_{i=1}^n c_i = |W|z(1) \prod_{i=1}^n c_i \). Thus, either \( p|W, p|c_i \) for some \( c_i < 2, \) or \( p|2 \). But \( 2|W, \) so \( p|W \) in any case. Conversely, if \( q = p, p|W, \) and \( p^n \nmid b, \) then \( f(p) = (a/b)p^k f^\#(p) \) is not divisible by \( p \).

**Remark.** The fact that \( k \geq 1 \) in (i) is Corollary B' of Green [19]; the proof we have given is slightly different from his. Theorem (5.5) also provides the following additional information.

(5.6) **Theorem.** Let \( G \) be a Chevalley group of rank \( n \geq 3 \). Associate a power \( q \) of a prime \( p \) with \( G \) as in (5.1). Let \( B \) be a Borel subgroup of \( G \). Then every irreducible constituent of \( t^q_B - 1 \) has degree divisible by \( p \), except possibly when \( q = p \) is a prime dividing \( |W| \).

**Proof.** (5.5)(v).

More precise information can be proved in some special cases:

(5.7) **Theorem.** Let \( G \) be a Chevalley group of rank \( n \geq 1 \) defined over a field of characteristic \( p \).
(i) If \( n \leq 2 \) and \( G \) is not \( \text{Sp}(4, 2), \text{G}_2(2), \text{G}_2(3), \) or \( \text{F}_4(2) \), then each nonprincipal irreducible constituent of \( 1^G_B \) has degree divisible by \( p \).

(ii) Suppose \( n > 3 \) and \( G \) is neither \( \text{Sp}(2n, 2), \text{PSO}(2n + 1, 2)', \) nor \( \text{F}_4(2) \). Define \( i \) as follows: \( i = 1 \) or \( 2 \) if \( G \) is a classical group; \( i = 1 \) or \( 4 \) if \( G \) is \( \text{F}_4(q) \); \( i = 1 \) if \( G \) is \( \text{E}_6(q) \); \( i = 1, 2 \) or \( 6 \) if \( G \) is \( \text{E}_7(q) \); \( i = 1 \) or \( 7 \) if \( G \) is \( \text{E}_8(q) \). Then each nonprincipal constituent of \( 1^G_G \) has degree divisible by \( p \).

This theorem and the next one will be basic to the proof of the Main Theorem. The proof is long, and will be given in \( \S \S 6, 7 \). We remark that a straightforward modification of the proof yields the conclusion of (ii) if \( i = 4 \) and \( G = \text{E}_6(q) \). For \( n = 2 \), the degrees of all the irreducible constituents of \( 1^G_B \) are listed in (7.26).

We also remark that, by (2.9), once (5.7) is known for a Chevalley group \( G \), it is known for any group \( G^+ \) satisfying \( G \leq G^+ \leq G^* \), where \( G^* \) is defined in (2.6).

(5.8) Theorem. Let \( G \neq \text{Sp}(2n, 2) \) be a classical group of \((B, N)\)-rank \( n > 3 \), defined over a field of characteristic \( p \). Then each nonprincipal constituent of \( 1^G_{G_{12}} \) has degree divisible by \( p \).

Here, \( G_{12} \) is defined as in \( \S 2 \). The proof of (5.8) is postponed until \( \S 8 \).

In one case of (5.6), a complete result is already known:

(5.9) Lemma. If \( G \) has type \( A_n(q) \), then each constituent \( \chi \) of \( 1^G_B - 1^G_G \) has degree divisible by \( q \).

Proof. According to [33], \( \chi \) can be written \( \chi = \sum a_J 1^G_{G_J} \) with \( a_J \in \mathbb{Z} \), where the sum is over all \( J \subseteq \{1, \ldots, n\} \). Then also \( \chi = \sum a_J (1^G_{G_J} - 1^G_G) \), where \( q \) divides the degree of \( 1^G_{G_J} - 1^G_G \). Thus, \( q | \chi(1) \).

The following technical lemma will be needed in \( \S 7 \).

(5.10) Lemma. Let \( S \) be as in (5.1). Fix \( J \subseteq \{1, \ldots, n\} \), and consider the parabolic subgroup \( P(q) = G(q)_J \) of \( G(q) \). Let \( f_0(t) = 1, f_1(t), \ldots, f_s(t) \) be the (not necessarily distinct) polynomials determined, via (5.2), by \( 1^G_{P(q)} \). Thus

\[ |G(q) : P(q)| = 1 + \sum_{j=1}^{s} f_j(q). \]

For \( j > 1 \), write \( f_j(t) = a_j t^k f_j^*(t) \) as in (5.5)(i), \( d_j = \deg f_j \), and \( d = \max_{j \geq 1} d_j \). Assume that \( d_s = d \), and write \( k = k_s \). Then

\[ |G(q) : P(q)|(q^k - 1) = (q^{d+k} - 1) + \sum_{j=1}^{s-1} f_j(q)(q^{d+k-j} - 1). \]

Proof. \( |G(q) : P(q)| = h(t) \), where \( h(t) \in \mathbb{Z}[t] \). Then \( h \) and the \( f_j^* \) are products of cyclotomic polynomials other than \( t - 1 \). Since \( f_j(t) \) has highest term \( a_j x^{d_j} \) with \( a_j > 0 \), we have \( \deg h = d \). Thus, \( h(1/t) = h(t)/t^d \). Also, \( f_j^*(1/t) = f_j^*(t)|t^{d_j-k_j} \), so \( f_j(1/t) = f_j(t)|t^{d_j+k_j} \). Consequently,
\[ h(t)^k = h(1/t)^{d+k} = \left(1 + \sum_{j=1}^{s} f_j(1/t)\right)^{d+k} = r^{d+k} + \sum_{j=1}^{s} f_j(t)^{d+k-d-kj}. \]

Since \( d + k - d_j - k_j = 0 \), subtraction of \( h(t) \) from this last relation yields the desired result.

We remark that it is conceivable that \( d + k - d_j - k_j < 0 \) for some subscripts \( j \).

We also note that further information is obtained by replacing \( q \) by \( t \) in the conclusion of (5.10), and then differentiating at \( t = 1 \); this will be done in §7.

6. The degrees of certain characters of the classical groups. In this section we shall prove Theorem (5.7)(ii) for the classical groups having Coxeter systems \((W, R)\) of types \( B_n, C_n, BC_n, \) and \( D_n, \) for \( n \geq 4. \) For groups of type \( A_n, \) the result is already known because of (5.9). The groups of types \( B_n, C_n, \) and \( BC_n \) for \( n = 2 \) and \( 3 \) will be treated in §7.

Let \( E_n \) be Euclidean space of dimension \( n, \) and let \( e_1, \ldots, e_n \) be an orthonormal basis. By [8], fundamental systems of roots of types \( B_n, C_n, \) and \( D_n \) are given as follows.

\begin{align*}
B_n: & \quad \alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_3, \ldots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_n; \\
C_n: & \quad \alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_3, \ldots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = 2e_n; \\
D_n: & \quad \alpha_1 = e_1 - e_2, \alpha_2 = e_2 - e_n, \ldots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_{n-1} + e_n.
\end{align*}

Letting \( R = \{s_1, \ldots, s_n\} \) denote a distinguished set of generators of a Coxeter system of type \( B_n, C_n, \) or \( D_n, \) we can identify \( s_1, \ldots, s_n \) with the following linear transformations of \( E_n. \)

\begin{align*}
B_n, C_n, and BC_n: & \quad \text{If } j < n, (e_j)s_j = e_{j+1}, (e_{j+1}s_j = e_j, (e_is_i = e_i, i \neq j, j + 1; (e_n)s_n = -e_n, (e_js_j = e_j, j < n.}
\\
D_n: & \quad \text{If } j < n, (e_j)s_j = e_{j+1}, (e_{j+1}s_j = e_j, (e_is_i = e_i, i \neq j, j + 1; (e_n)s_n = -e_{n-1}, (e_{n-1}s_n = -e_n, (e_js_j = e_j, j \neq n - 1, n.}
\end{align*}

The group \( W \) can be viewed as a transitive permutation group on the set \( \{\pm e_1, \ldots, \pm e_n\}, \) which we shall denote by \( \{\pm 1, \ldots, \pm n\}. \)

(6.3) **Lemma.** Let \( (W, R) \) be a Coxeter system of type \( B_n, C_n, BC_n, \) or \( D_n, \) for \( n \geq 4, \) with \( R = \{s_1, \ldots, s_n\} \) as in (6.2).

(a) \( W_1 = \langle s_2, \ldots, s_n \rangle \) is the stabilizer of \( \{1\}, \) when \( W \) is viewed as a permutation group on the set \( \{\pm 1, \ldots, \pm n\}. \) The double coset space \( W_1 \backslash W/W_1 \) has 3 double
cosets, corresponding to the orbits of \( W_1 \) on the set \( \{\pm 1, \ldots, \pm n\} \).

(b) \( W_2 = \langle s_1, s_3, \ldots, s_n \rangle \) is the stabilizer of the pair \( \{1, 2\} \), when \( W \) is viewed as a transitive permutation group on the set of \( 2n(n-1) \) unordered pairs \( \{\pm i, \pm j\}, \ i \neq j \). The double coset space \( W_2 \backslash W/W_2 \) contains 6 double cosets, corresponding to the orbits of \( W_2 \) on the set of unordered pairs \( \{\pm i, \pm j\}, \ i \neq j \).

**Proof.** The proof of (a) is immediate, and is omitted. For (b), one first checks that \( W_2 \) is exactly the stabilizer of \( \{1, 2\} \) because \( |W_2| = 2n(n-1) \). It is then easy to verify that there are exactly 6 orbits, with representatives \( \{1, 2\}, \{1, 3\}, \{-1, 2\}, \{3, 4\}, \{-1, 3\}, \) and \( \{-1, -2\} \).

(6.4) **Lemma.** Let \( G \) be a classical group having a Coxeter system of type \( B_n, C_n, BC_n \) or \( D_n \), with \( n \geq 4 \). Then \( l_G \) is multiplicity-free and contains \( l_{G_1} \). Moreover, \( (l_{G_i}^1, l_{G_2}^1) = 3 \) and \( (l_{G_2}^2, l_{G_2}^2) = 6 \).

**Proof.** By (2.8), \( (l_{G_i}^1, l_{G_j}^1) = (l_{G_i}^1, l_{G_j}^1) \) for all \( i \) and \( j \). By (6.3), \( (l_{W_1}^W, l_{W_1}^W) = 3 \) and \( (l_{W_2}^W, l_{W_2}^W) = 6 \). Finally, since the unordered pairs \( \{\pm i, \pm j\} \) correspond to the right cosets \( W_2w \), the orbits of \( W_1 \) on this set correspond to the double cosets \( W_2wW_1 \). Since there are 3 orbits, we have \( (l_{W_1}^W, l_{W_1}^W) = 3 \). All the statements in the lemma follow from these remarks.

(6.5) **Proposition.** If \( G \) has a Coxeter system \((W, R)\) of type \( B_n \), with \( n \geq 4 \), then (5.7)(ii) holds.

**Proof.** We begin with a closer examination of the double coset space \( W_2 \backslash W/W_2 \). By (6.3), this space can be identified with the \( W_2 \)-orbits on the set of unordered pairs \( \{\pm i, \pm j\} \). The following table lists a representative of each orbit, the size of the orbit, and an element of \( W \) of minimal length which carries \( \{1, 2\} \) to an element of the orbit. The latter elements are the unique elements of minimal length belonging to the various double cosets, and we shall index the double cosets by these representatives.

<table>
<thead>
<tr>
<th>Orbit Representative</th>
<th>Size of Orbit</th>
<th>Double Coset Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>{1, 2}</td>
<td>1</td>
<td>( w_0^* = 1 )</td>
</tr>
<tr>
<td>{1, 3}</td>
<td>4(n-2)</td>
<td>( w_1^* = s_2 )</td>
</tr>
<tr>
<td>{-1, 2}</td>
<td>2</td>
<td>( w_2^* = s_2 \cdots s_n )</td>
</tr>
<tr>
<td>{3, 4}</td>
<td>2(n-2)(n-3)</td>
<td>( w_3^* = s_2s_3s_2 )</td>
</tr>
<tr>
<td>{-1, 3}</td>
<td>4(n-2)</td>
<td>( w_4^* = s_2 \cdots s_{n-1}s_2s_{n-1} \cdots s_2 )</td>
</tr>
<tr>
<td>{-1, -2}</td>
<td>1</td>
<td>( w_5^* = s_2 \cdots s_n \cdots s_2s_2s_2 \cdots s_n \cdots s_2 )</td>
</tr>
</tbody>
</table>

Let \( \xi_0, \ldots, \xi_5 \) be the standard basis elements of the Hecke algebra \( H(G, G_2) \), in the sense of [13]. Then

\[
\xi_i = \frac{1}{|G_2|} \sum_{x \in G_2 w_i^* G_2} x, \quad 0 \leq i \leq 5.
\]
Note that $\xi_0$ is the identity element of $H(G, G_2)$. Let $L_{\xi_i}$ denote the left multiplication by $\xi_i$ on the space $H(G, G_2)$. We note that $H(G, G_2)$ is commutative since $I_{G_2}$ is multiplicity-free (by (6.4)). We shall compute the matrix of the left multiplication $L_{\xi_1}$ with respect to the basis $\xi_0, \ldots, \xi_5$, and determine the characteristic roots of this matrix (which will all occur with multiplicity one). This will lead to a proof of (6.5).

(6.7) Lemma. The matrix $M$ of the left multiplication $L_{\xi_1}$ with respect to the basis $\xi_0, \xi_1, \ldots, \xi_5$ is given by

$$M = \begin{pmatrix}
0 & x(x+1)\eta & 0 & 0 & 0 & 0 \\
1 & \lambda + \mu x^2 & \mu x^3 & \nu x^2 & 0 & 0 \\
0 & \eta & (x-1)\eta & 0 & \eta x^2 & 0 \\
0 & (x+1)^2 & 0 & 0 & \nu(x+1)^2 & 0 \\
0 & 1 & x & \mu x & \xi & \nu x^2 \\
0 & 0 & 0 & 0 & \eta(x+1) & \eta(x^2-1)
\end{pmatrix},$$

where $x = q^e_1 = q^e_2 = \cdots = q^{e_n-1}$, and $y = q^{e_n}$, and

$$\lambda = x^2 + x - 1, \quad \xi = \frac{1}{x-1} ((2x^2-1)(x^{2n-6}y-1) + \lambda x^{n-3}(x-y)), \quad \mu = \frac{(x^{n-3} - 1)(1 + x^{n-4}y)}{x-1}, \quad \eta = \frac{(x^{n-2} - 1)(1 + x^{n-3}y)}{x-1}, \quad \nu = x^{2n-6}y, \quad \theta = \frac{(x+1)(x^{2n-6}y - x^{n-2}y + x^{n-1} - \lambda)}{x-1}.$$

(The index parameters $c_j$ are given in Table 5, §5.)

Proof. We have, by [13],

$$\xi_1 \xi_i = \sum_{k=0}^5 b_{1ik} \xi_k$$

where

$$b_{1ik} = |G_2|^{-1} |G_2 w_i^* G_2 \cap w_k^* G_2 w_i^* G_2|$$

$$= |G_2|^{-1} |w_k^* G_2 w_i^* G_2 \cap G_2 w_i^* G_2|$$

$$= |G_2|^{-1} |G_2 w_i^* G_2 w_k^* \cap G_2 w_i^* G_2|,$$

using the fact that $w_j^*$ is an involution for $j = 0, 1, \ldots, 5$. Thus, $b_{1ik}$ is just the number of left cosets of $G_2$ that are contained in both $G_2 w_i^* G_2 w_k^*$ and $G_2 w_i^* G_2$. Also, $M$ is just the matrix $(b_{1ik})$. We begin the computation of $b_{1ik}$ by finding a set
of $G_2$-coset representatives in $G_2w_1G_2$. We have

$$W_2s_2W_2 = \left( \bigcup_{i=1}^{2(n-2)} W_2w_1i \right) \cup \left( \bigcup_{j=1}^{2(n-2)} W_2w_1j \right),$$

where

$$w_{1,1} = s_2, \quad w'_{1,1} = s_2s_1,$$

$$w_{1,2} = s_2s_3, \quad w'_{1,2} = s_2s_1s_3,$$

$$\vdots$$

$$w_{1,2(n-2)} = s_2 \cdots s_{n-1}s_n \cdots s_3, \quad w'_{1,2(n-2)} = s_2s_1 \cdots s_{n-1}s_n \cdots s_3.$$

Moreover, the above unions are all disjoint and the elements $w_{1,i}$ and $w'_{1,j}$, $1 \leq i, j \leq 2(n-2)$, are easily seen to be the unique elements of minimal length in the cosets containing them. Then by standard arguments for groups with BN-pairs (see [8]),

$$G_2s_2G_2 = \left( \bigcup_{i=1}^{2(n-2)} BW_2w_1iB \right) \cup \left( \bigcup_{j=1}^{2(n-2)} BW_2w_1jB \right)$$

where the unions are all disjoint. Moreover, using the root structure in $G$ (see [30]), we have

$$G_2s_2U = G_2s_2U_2,$$

$$G_2s_2s_3U = G_2s_2s_3U_2^3U_3$$

and

$$G_2s_2s_1U = G_2s_2s_1U_1^3U_1$$

$$G_2s_2s_1 \cdots s_{n-1}s_n \cdots s_3U = G_2s_2s_1 \cdots s_{n-1}s_n \cdots s_3U_2^{s_3s_{n-3}s_2} \cdots U_4^3U_3.$$

Since $|U_1| = \cdots = |U_{n-1}| = x$ and $|U_n| = y$, we conclude from the uniqueness of expression in the Bruhat decomposition that

- $G_2s_2U$ contains $x$ left $G_2$ cosets,
- $G_2s_2s_3U$ contains $x^2$ left $G_2$ cosets,
- $\cdots$
- $G_2s_2 \cdots s_{n-1}s_n \cdots s_3U$ contains $x^{2n-5}y$ left $G_2$ cosets,
- $G_2s_2s_1U$ contains $x^2$ left $G_2$ cosets,
- $\cdots$
- $G_2s_2s_1 \cdots s_{n-1}s_n \cdots s_3$ contains $x^{2n-4}y$ left $G_2$ cosets.

In particular, $G_2w_1^4G_2$ contains
\[(x + x^2 + \cdots + x^{n-2} + x^{n-2}y + \cdots + x^{2n-5}y) + (x^2 + \cdots + x^{n-3} + x^{n-3}y + \cdots + x^{2n-4}y) = x(x + 1)\eta\]

left \(G_2\)-cosets, when \(\eta\) is given in the statement of (6.7).

We shall now give, in tabular form, the distribution of the \(G_2\)-cosets in \(G_2w_iG_2w_i^*\). (Zeros are omitted in the tables, except in the totals.) Determination of the double coset containing a given \(w \in \mathcal{W}\) is made by applying \(w\) to \(\{e_1, e_2\}\) and finding the orbit to which \(\{(e_1)w, (e_2)w\}\) belongs. Determination of whether \(l(ws_i) \geq l(w)\), for example, is made by computing \((\alpha_i)w^{-1}\), using the fact that

\[l(ws_i) > l(w) \quad \text{if and only if} \quad (\alpha_i)w^{-1} > 0.\]

This information is used in combination with

\[wBs_i \subseteq BwB \cup Bws_iB, \quad \text{and} \quad wBs_i \subseteq Bws_iB\]

if \(l(ws_i) \geq l(w)\). In computations with root systems we shall use the notation \(S_\alpha\)
for the linear map \(x \rightarrow x - 2(x, \alpha)\alpha/(\alpha, \alpha)\), where \(\alpha \in E_n\). After each case some remarks will be made on some of the less obvious parts of the calculations.

<table>
<thead>
<tr>
<th>(G_2w_iG_2w_i^*)</th>
<th>(w_0^*)</th>
<th>(w_1^*)</th>
<th>(w_2^*)</th>
<th>(w_3^*)</th>
<th>(w_4^*)</th>
<th>(w_5^*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(G_2w_iG_2w_i^*)</td>
<td>0</td>
<td>(x(x + 1)\eta)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(G_2w_iG_2w_{i1})</td>
<td>(w_0^*)</td>
<td>(w_1^*)</td>
<td>(w_2^*)</td>
<td>(w_3^*)</td>
<td>(w_4^*)</td>
<td>(w_5^*)</td>
</tr>
<tr>
<td>(G_2w_{1, 2}Uw_1^*)</td>
<td>1</td>
<td>(x - 1)</td>
<td>(x^2)</td>
<td>(x^{2n-6}y)</td>
<td>(x^{2n-5}y)</td>
<td>(x^2)</td>
</tr>
<tr>
<td>(G_2w_{1, 2}Uw_1^*)</td>
<td>(x^2)</td>
<td>(x^3)</td>
<td>(x^{2n-5})</td>
<td>(x^{2n-4}y)</td>
<td>(x^2)</td>
<td>(x^3)</td>
</tr>
<tr>
<td>(G_2w_{1, 2}Bw_1^*)</td>
<td>(x^2)</td>
<td>(x^{2n-5})</td>
<td>(x^{2n-4}y)</td>
<td>(x^3)</td>
<td>(x^2)</td>
<td>(x^{2n-5})</td>
</tr>
<tr>
<td>Totals</td>
<td>1</td>
<td>(\lambda + \mu x^2)</td>
<td>(xv)</td>
<td>(\mu x^3)</td>
<td>(x^2v)</td>
<td>0</td>
</tr>
</tbody>
</table>

**Remarks.** \(G_2w_{11}Bw_1^* = G_2s_2U_2s_2 \subseteq G_2 \cup G_2s_2U_2^*\), since \(s_2U_2s_2 = \{1\} \cup s_2U_2^*s_2\) and \(s_2U_2^*s_2 \subseteq G_2s_2U_2\).
\[
\begin{array}{cccccc}
G_2w^*_1G_2w^*_2 & w_0^* & w_1^* & w_2^* & w_3^* & w_4^* & w_5^* \\
G_2w_{1,1}Uw_2^* & 1 & x & -1 & & & \\
G_2w_{1,2}Uw_2^* & x & x(x-1) & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
G_2w_{1,2n-4}Uw_2^* & x^{2n-6}y & x^{2n-6}y(x-1) & & & & \\
G_2w_{1,1}'Uw_2^* & & & & x^2 & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
G_2w_{1,2n-4}'Uw_2^* & & & & x^{2n-4}y & & \\
\hline
\text{Totals} & 0 & \eta & (x-1)\eta & 0 & x^2\eta & 0 \\
\end{array}
\]

**Remarks.** \(w_2^* = S_{e_2}.\)

\(G_2w_{1,1}Uw_2^* = G_2s_2U_2w_2^* = G_2s_2U_2s_2(s_3w_2^*) = G_2s_2w_2^* \cup G_2w_2^*U_2U_2w_2^*,\)

and \((\alpha_2)w_2^* = (\alpha_2)S_{e_2} < 0,\) giving 1 coset in \(G_2w^*_1G_2\) and \(x - 1\) cosets in \(G_2w^*_2G_2.\)

\(G_2w_{1,2}Uw_2^* = G_2s_2s_3U_2U_2w_2^* = (G_2s_2U_2w_2^*)U_3w_3^*,\)

and the first computation can be applied to all \(G_2w_{1,i}Uw_2^*, \ 1 \leq i \leq 2n - 4.\) Also,

\(G_2w_{1,i}'Uw_2^* \subset G_2w^*_2G_2, \ 1 \leq i \leq 2n - 4.\)
### 2-TRANSITIVE PERMUTATION REPRESENTATIONS

<table>
<thead>
<tr>
<th>$G_2 w_1^* U w_4^*$</th>
<th>$w_0^*$</th>
<th>$w_1^*$</th>
<th>$w_2^*$</th>
<th>$w_3^*$</th>
<th>$w_4^*$</th>
<th>$w_5^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_2 w_{11} U w_4^*$</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$x - 1$</td>
</tr>
<tr>
<td>$G_2 w_{1,2} U w_4^*$</td>
<td></td>
<td></td>
<td>$x$</td>
<td></td>
<td>$x(x - 1)$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,2n-5} U w_4^*$</td>
<td></td>
<td></td>
<td>$x^{2n-7} y$</td>
<td></td>
<td>$x^{2n-7} y(x - 1)$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,2n-4} U w_4^*$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$x^{2n-6} y$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,2n-4} U w_4^*$</td>
<td></td>
<td></td>
<td>$x$</td>
<td></td>
<td>$x(x - 1)$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,2n-4} U w_4^*$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$x^3$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,n-4} U w_4^*$</td>
<td></td>
<td></td>
<td>$x^{2n-6} y$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>1</td>
<td>$x$</td>
<td>$x^\mu$</td>
<td>$\xi$</td>
<td>$x^{2+\nu}$</td>
</tr>
</tbody>
</table>

**Remarks.** $w_w^* = S_{\epsilon_1 - \epsilon_3} S_{\epsilon_2}$:

- For $G_2 w_{11} U w_4^*$, $(a_2) w_4^* < 0$.
- For $G_2 w_{1,2} U w_4^*$, $(a_3) w_4^* > 0$, $(a_2) s_3 w_4^* < 0$.
- For $G_2 w_{1,3} U w_4^*$, $(a_4) w_4^* > 0$, $(a_3) s_4 w_4^* > 0$, $(a_2) s_3 s_4 w_4^* < 0$.
- For $G_2 w_{1,2n-5} U w_4^*$, $(a_4) w_4^* > 0$, $(a_5) s_4 w_4^* > 0$, \ldots
- $(a_3) s_4 \ldots s_n \cdots s_4 w_4^* > 0$,
- $(a_2) s_3 \cdots s_n \cdots s_3 s_4^* < 0$.
- For $G_2 w_{1,2n-4} U w_4^*$, $(a_2) s_2 \cdots s_n \cdots s_3 w_4^* > 0$.

<table>
<thead>
<tr>
<th>$G_2 w_1^* U w_5^*$</th>
<th>$w_0^*$</th>
<th>$w_1^*$</th>
<th>$w_2^*$</th>
<th>$w_3^*$</th>
<th>$w_4^*$</th>
<th>$w_5^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_2 w_{11} U w_5^*$</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$x - 1$</td>
</tr>
<tr>
<td>$G_2 w_{1,2} U w_5^*$</td>
<td></td>
<td></td>
<td>$x$</td>
<td></td>
<td>$x(x - 1)$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,2n-5} U w_5^*$</td>
<td></td>
<td></td>
<td>$x^{2n-6} y$</td>
<td></td>
<td>$x^{2n-6} y(x - 1)$</td>
<td></td>
</tr>
<tr>
<td>$G_2 w_{1,2n-4} U w_5^*$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$x^{2n-6} y$</td>
<td></td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$0$</td>
<td>$(x + 1) \eta$</td>
<td>$(x^2 - 1) \eta$</td>
</tr>
</tbody>
</table>
Remarks. \( w_s^g = S_{e_2 + e_1} \).
This completes the proof of (6.7).

(6.8) Lemma. The characteristic roots of \( M \) are:

\[
\begin{align*}
\theta_0 &= x(x + 1)(1 + x^{n-3}y)(x^{n-2} - 1)(x - 1)^{-1}, \\
\theta_1 &= (x^{n-2}y + \lambda)(x^{n-2} - 1)(x - 1)^{-1}, \\
\theta_2 &= (x^{n-1} - \lambda)(1 + x^{n-3}y)(x - 1)^{-1}, \\
\theta_3 &= -(x + 1)(1 + x^{n-3}y), \\
\theta_4 &= (x + 1)(x^{n-2} - 1), \\
\theta_5 &= -(x + 1 + x^{n-3}(y - x)).
\end{align*}
\]

The proof of (6.8) was done by machine computation. The program was written by Professor T. Beyer of the University of Oregon Computer Science Department.

Since \( \xi_1 \) has 6 distinct characteristic roots, it follows that the Hecke algebra \( H(G, G_2) \) is generated by \( \xi_1 \). Recall that \( \xi_0 = |G_2|^{-1} \sum_{\alpha \in G_2} \alpha \) is the identity in \( H(G, G_2) \), \( V = CG\xi_0 \) is a \( (CG, H(G, G_2)) \) bimodule, and \( V \) regarded as a left \( CG \)-module affords the permutation representation \( 1_{G_2}^{G_2} \). The next result is known [21], but is presented here in a slightly different form.

(6.9) Lemma. Let \( A \) be the matrix of right multiplication by \( \xi_1 \) on \( V \).

(i) The minimal polynomials of \( A \) and \( M \) are the same, and coincide with the characteristic polynomial \( p(t) \) of \( M \).

(ii) \( 1_{G_2}^{G_2} \) has exactly 6 irreducible constituents \( \xi_{0,q}, \xi_{1,q}, \ldots, \xi_{5,q} \), which are afforded by the subspaces of \( V \) belonging to the characteristic roots \( \theta_0, \ldots, \theta_5 \) of \( A \). The degree of \( \xi_{i,q} \) is the multiplicity of \( \theta_i \) as a characteristic root of \( A \).

(iii) For \( 0 \leq i \leq 5 \), let \( p(t) = p(t)/(t - \theta_i) \). Then the degree of \( \xi_{i,q} \) is given by \( \xi_{i,q}(1) = p(\theta_i)^{-1}(\text{trace } p(A)) \).

Proof. Since the \( 6 \times 6 \) matrix \( M \) has 6 different characteristic roots, we know that the characteristic and minimal polynomials of \( M \) coincide. Since \( \beta \rightarrow L_\beta \) is a faithful representation of the algebra \( H(G, G_2) \), we have \( p(\xi_1) = 0 \) in \( H(G, G_2) \). Also, \( \xi_1 \rightarrow A \) induces a matrix representation of \( H(G, G_2) \), therefore \( p(A) = 0 \). On the other hand, \( H(G, G_2) \) is a subspace of \( V \), and is invariant under right multiplication by \( \xi_1 \). Therefore, if, for some polynomial \( f(t) \), \( f(A) = 0 \), we have \( f(R_{\xi_1}) = 0 \), where \( R_{\xi_1} \) is the right multiplication by \( \xi_1 \) in \( H(G, G_2) \), then \( f(\xi_1) = 0 \). Therefore \( p(t) \mid f(t) \), and we have shown that \( p(t) \) is also the minimal polynomial of \( A \).

Since \( H(G, G_2) \) is isomorphic to the centralizer ring \( \text{Hom}_{CG}(V, V) \), \( V \) has 6 irreducible \( CG \)-submodules, each appearing with multiplicity one. On the other hand, \( V \) is the direct sum of the six subspaces belonging to the characteristic roots of \( A \), and these are \( CG \)-submodules of \( V \). It follows that the irreducible \( CG \)-components of \( 1_{G_2}^{G_2} \) are afforded by the subspaces belonging to the characteristic roots of \( A \), and that the
dimensions of these subspaces are the multiplicities of the characteristic roots of $A$.

Part (iii) follows from part (ii) and a result of Feit and Higman [16, Lemma (3.4)], since $p(t)$ has simple roots. This completes the proof of the lemma.

The next lemma is also known [21, Theorem (5.2)]. We include a proof since our situation is slightly different.

(6.10) **Lemma.** Let $A$ be the matrix of the right multiplication by $\xi_1$ on $V$ and let $s \geq 0$ be an integer. Then $\text{trace } A^s = |G : G_2| \eta_{s0}$, where $\eta_{s0}$ is defined by $\xi_1 = \sum_{i=0}^s \eta_{si} \xi_i$.

**Proof.** If $\xi$ is an element of $H(G, G_2)$, write $(\xi)_R$ for the right multiplication by $\xi$ on $V$. We then have

$$\text{trace}(A^s) = \text{trace}((\xi_1)^s)_R = \sum_{i=0}^s \eta_{si} \text{trace}(\xi_i)_R.$$ 

Moreover, $\text{trace}(\epsilon_0)_R = \dim V = |G : G_2|$. It suffices to show that $\text{trace}(\xi_i)_R = 0$ for $i \geq 0$. Let $G_2 \omega^*_i G_2 = \bigcup_{j} g_j \omega^*_i G_2$ (disjoint), for $i = 0, \ldots, 5$. Then the elements $\{g_j \omega^*_i \xi_0\}_{i,j}$ form a basis for $V$. For $t = 0, \ldots, 5$ we have

$$g_{ji} \omega^*_i \xi_0 \xi_t = \sum_{l,k} a_{ji, lk} g_{lk} \omega^*_l \xi_0,$$

with nonnegative rational coefficients $a_{ji, lk}$. If for some $t \neq 0$, $a_{ji, li} \neq 0$, then multiplying (6.11) on the left by $(g_j \omega^*_i)^{-1}$ yields

$$\xi_t = a_{ji, li} \xi_0 + \sum_{h,l} b_{lh} g_{lh} \omega^*_l \xi_0,$$

with $b_{lh} \geq 0$. This is impossible, so the lemma is proved.

We are now ready to finish the proof of Proposition (6.5). Let $M$ be the matrix in (6.7), with $x$ and $y$ viewed as indeterminates. Let $c_1, \ldots, c_{n-1}, c_n$ be a system of index parameters associated with a system of groups with $BN$-pairs of type $B_n$ (see (5.1)). The possibilities for the $c_i$'s are given in Table 5.

(6.12) **Lemma.** Let

$$F(x, y) = (x^n - 1)(x^{n-1} - 1)(x^{n-2} - 1)(x^n - 1)(x^{n-2}y + 1)/(x - 1)^2(x + 1),$$

for $n \geq 4$. For $G = G(q) \in S$, and $q^{c_1} = \cdots = q^{c_n-1} = x, q^{c_n} = y$, we have $|G : G_2| = F(q^{c_1}, q^{c_n})$.

**Proof.** Table 3.

By (6.7) there exist polynomials $\eta_{ij}(x, y) \in Z[x, y]$ such that $\xi_i^s = \sum_{j=0}^s \eta_{ij}(q^{c_1}, q^{c_n}) \xi_j$, as in (6.10). Define $T_i(x, y) = F(x, y) \eta_{i0}(x, y)$, for $s \geq 0$. Then $T_i(x, y) \in Z[x, y]$, and $T_i(q^{c_1}, q^{c_n}) = \text{trace } A^i, s \geq 0$.

Let $t$ be an indeterminate, and fix $i \in \{0, \ldots, 5\}$. Write $p_f(x, y, t) = p(t)(t - \theta)^{-1}$, where $p(t)$ is the characteristic polynomial of $M$. We then have

$$p_f(x, y, t) = \prod_{j \neq i} (t - \theta_j) = \sum_{k=0}^4 h_k(x, y)t^k,$$

with $h_k(x, y) \in Z[x, y]$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(6.13) \textbf{Lemma.} Let
\[ K(x, y) = F(x, y) \left( \sum_{k=0}^{4} h_k(x, y) n_{k, 0}(x, y) \right). \]

Then
\[ K(q^{e_1}, q^{e_n}) = \text{trace } p_i(q^{e_1}, q^{e_n}, A). \]

\textbf{Proof.} The result is immediate from (6.10) and (6.12).

(6.14) \textbf{Proposition.} Let \( t \) be an indeterminate, and let
\[ \delta_i(t) = \prod_{i \neq i} (\theta_i(t^{e_1}, t^{e_n}) - \theta_i(t^{e_1}, t^{e_n})), \]
and
\[ d_i(t) = K(t^{e_1}, t^{e_n})/\delta_i(t). \]

Then \( d_i(q) = \xi_{i, q}(1) \) for all \( q \).

\textbf{Proof.} Immediate from (6.9)(iii) and (6.13).

Thus, \( d_i(t) \) is the generic degree of the characters \( \xi_{i, q}, 0 \leq i \leq 5 \) (cf. (5.2)).

Now suppose \( q \) is a power of the prime \( p \). We have to show that \( p \) divides \( \xi_{i, q}(1) \) except possibly when \( c_1 = c_n \) and \( q = 2 \).

Using (6.8), direct computation (which is omitted) shows that \( \delta_i(t) \in \mathbb{Z}[t] \), and that \( \pm \delta_i(t) \) is monic except in the following cases:

(a) \( \delta_i(t) = \pm 2\delta_i(t) \), with \( \delta_i(t) \) monic, \( i = 1, 2, \) if \( c_1 = c_n \);
(b) \( \delta_4(t) = 2\delta_4(t), \delta_5(t) = 2\delta_5(t) \), with \( \delta_i(t) \) monic, if \( c_1 = 1, c_n = 2 \).

Using the fact that \( d_i(t) \in Q[t] \), and that \( K(t^{e_1}, t^{e_2}) \in \mathbb{Z}[t] \), it follows that \( d_i(t) \in \mathbb{Z}[t] \) if \( \delta_i(t) \) is monic, and \( d_i(t) = \frac{1}{2} d_i(t) \), with \( d_i(t) \in \mathbb{Z}[t] \) in case \( \delta_i(t) = 2\delta_i(t) \) with \( \delta_i(t) \) monic. Now we apply (5.3) to conclude that \( q \) (and, hence, \( p \)) divides \( d_i(t) \) if \( d_i(t) \in \mathbb{Z}[t] \), and that \( p \) divides \( d_i(t) \) in all cases except possibly when \( q = p = 2 \) and one of the situations (a) or (b) above prevails. Case (a) is a genuine exception, and is provided for in the statement of the theorem.

It remains to show when \( q = p = 2 \), and \( c_1 = \cdots = c_{n-1} = 1, c_n = 2 \), that \( d_4(t) \) and \( d_5(t) \) are both even. In this case, \( G = \text{PSO}^{-2n}(2n + 2, 2). \) Assume one or both of \( d_4(2), d_5(2) \) is odd. The odd degrees must be associated with characters in \( 1G_2 - 1G_1 \) because of the formulas of the degrees in \( 1G_1 \) given in Table 3. The sum of the generic degrees of the characters in \( 1G_2 - 1G_1 \) is, by Table 3,
\[ f(t) = (t^{n+1} + 1)(t^{2n} - 1)(t^n - 1)(t - 1)^{-1}(t^2 - 1)^{-1} - (t^{n+1} + 1)(t^n - 1)(t - 1)^{-1}. \]

Since \( f(t) \) has leading term equal to \( t^2 \), it follows from (5.5) that \( t^2 \) divides the generic degrees of the characters in \( 1G_2 - 1G_1 \). If \( d(t) \) is a generic degree for which \( d(2) \) is odd, we have \( t^2 d(t) \), and \( 2d(t) \in \mathbb{Z}[t] \). These imply that \( d(2) \) is even, a contradiction, and Proposition (6.5) is proved.
(6.15) Proposition. If G has a Coxeter system \((W, R)\) of type \(C_n\) or \(BC_n\) with \(n \geq 4\), then (5.7)(ii) holds.

Proof. We begin by considering a system \((W', R')\) of type \(B_n\). Then, as in (6.1), we can choose an orthonormal basis \(e_1, \ldots, e_n\) of \(E_n\) so that the roots in \(\Delta'\) are \(\pm e_i, 1 \leq i \leq n, \) and \(\pm (e_i \pm e_j)\), for \(1 \leq i < j \leq n\). For a fundamental system we take \(\alpha_1' = e_1 - e_2, \ldots, \alpha_{n-1}' = e_{n-1} - e_n, \) and \(\alpha_n' = e_n\).

Now let \(\Delta\) be the set of roots consisting of \(\pm 2e_i, 1 \leq i \leq n, \) and \(\pm (e_i \pm e_j)\), for \(1 \leq i < j \leq n\). Then \(\Delta\) is a system of type \(C_n\), and as a base we may take \(\alpha_1 = e_1 - e_2, \ldots, \alpha_{n-1} = e_{n-1} - e_n\) and \(\alpha_n = 2e_n\). There is an obvious bijection from \(\Delta'\) to \(\Delta\) sending \(\alpha_i'\) to \(\alpha_i\) for each \(i\). Also, for \(i = 1, \ldots, n\), the fundamental reflection \(s_i'\) is actually identical to \(s_i\). Thus, \((W', R') = (W, R)\). In particular, \(W' = W\) and \(W'_2 = W_2\).

It follows that all calculations and results used in the proof of (6.2) continue to hold if \(G = G(q)\) has Coxeter system \((W, R)\) of type \(C_n\). We find that \(p\) divides the degree of each nonprincipal irreducible constituent of \(\text{lg}\) except when \(c_1 = \cdots = c_n-1 = c_n = 1\) and \(q = 2\), where \(G = C_n(2) \cong \text{Sp}(2n, 2)\). Thus, (5.7)(ii) holds for type \(C_n\).

If \(G\) has Coxeter system \((W, R)\) of type \(BC_n\), then the above remarks show once again that (5.7)(ii) holds for \(G\).

(6.16) Proposition. Let \(G\) have a Coxeter system \((W, R)\) of type \(D_n\), with \(n \geq 4\). Then (5.7)(ii) holds.

Proof. We proceed as in the proof of (6.5). Let \(\{\alpha_1, \ldots, \alpha_n\}\) be a fundamental system of roots of type \(D_n\), expressed in terms of an orthonormal basis \(e_1, \ldots, e_n\) of \(E_n\) according to (6.1). The fundamental reflections \(s_1, \ldots, s_n\) are given in (6.2). The notation is chosen so that the first \(n - 1\) generators are the same as the first \(n - 1\) generators of the Coxeter system of type \(B_n\) considered in the proof of (6.5). The group \(W\) acts as a permutation group on \(\{\pm 1, \ldots, \pm n\}\) as in (6.3), and is a subgroup of index 2 in a Coxeter group of type \(B_n\).

By (6.3), \(W\) acts as a permutation group on the set of unordered pairs \(\{\pm i, \pm j\}\), \(i \neq j\), in such a way that \(W_2\) is the stabilizer of \(\{1, 2\}\), and the orbits of the set of pairs relative to the action of \(W_2\) correspond to the \((W_2, W_2)\)-double cosets in \(W\). By (6.3) there are 6 orbits. The following table is the analogue of (6.6).

<table>
<thead>
<tr>
<th>Orbit Representative</th>
<th>Size of Orbit</th>
<th>Double Coset Representatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>{1, 2}</td>
<td>1</td>
<td>(w_0^* ) = 1</td>
</tr>
<tr>
<td>{1, 3}</td>
<td>(4(n - 2))</td>
<td>(w_1^* = s_2)</td>
</tr>
<tr>
<td>{-1, 2}</td>
<td>2</td>
<td>(w_2^* = s_2 \cdots s_{n-2} s_{n-1} s_n s_{n-2} \cdots)</td>
</tr>
<tr>
<td>{3, 5}</td>
<td>(2(n - 2)(n - 3))</td>
<td>(w_3^* = s_2 s_3 s_5 s_2)</td>
</tr>
<tr>
<td>{-1, 3}</td>
<td>(4(n - 2))</td>
<td>(w_4^* = s_2 \cdots s_{n-2} s_1 s_{n-1} s_n s_{n-2} \cdots)</td>
</tr>
<tr>
<td>{-1, -2}</td>
<td>1</td>
<td>(w_5^* = w_2^* w_1^* w_2^*)</td>
</tr>
</tbody>
</table>
Proceeding as in the case of $B_n$, we let $\xi_0, \xi_1, \ldots, \xi_5$ denote the standard basis elements of the Hecke algebra $H(G, G_2)$, and proceed to calculate the matrix of the left multiplication $L_{\xi_1}$.

(6.18) **Lemma.** The matrix $M'$ of the left multiplication $L_{\xi_1}$ with respect to the basis $\xi_0, \xi_1, \ldots, \xi_5$ is

$$
M' = 
\begin{pmatrix}
0 & x(x + 1)\eta' & 0 & 0 & 0 & 0 \\
1 & \lambda + \mu'x^2 & xv' & \mu'x^3 & \nu'x^2 & 0 \\
0 & \eta' & (x - 1)\eta' & 0 & \eta'x^2 & 0 \\
0 & (x + 1)^2 & 0 & \theta' & \nu'(x + 1)^2 & 0 \\
0 & 1 & x & \mu'x & \xi' & \nu'x^2 \\
0 & 0 & 0 & 0 & \eta'(x + 1) & \eta'(x^2 - 1)
\end{pmatrix}
$$

where

$$
x = q, \quad \xi' = \frac{1}{x - 1} [(2x^2 - 1)(x^2n-6 - 1) + \lambda x^{n-3}(x - 1)],
$$

$$
\lambda = x^2 + x - 1, \quad \eta' = \frac{(x^{n-2} - 1)(1 + x^{n-3})}{x - 1},
$$

$$
\mu' = \frac{(x^{n-3} - 1)(1 + x^{n-4})}{x - 1}, \quad \theta' = \frac{(x + 1)(x^{2n-6} - x^{n-2} + x^{n-1} - \lambda)}{x - 1},
$$

$$
\nu' = x^{2n-6}.
$$

**Proof.** As in the case of $B_n$, we begin by finding a set of shortest $W_2$-coset representatives in $W_2W_1^*W_2$. Using the same notation as in the case of $B_n$, we have

$$
W_2s_2W_2 = \left( \bigcup_{l=1}^{2n-4} W_2w_{1l} \right) \cup \left( \bigcup_{l=1}^{2n-4} W_2w'_{1l} \right) \quad \text{(disjoint)},
$$

where

$$
w_{1,1} = s_2,
$$

$$
w_{1,2} = s_2s_3,
$$

$$
\vdots
$$

$$
w_{1,n-2} = s_2 \cdots s_{n-1},
$$

$$
w_{1,n-1} = s_2 \cdots s_{n-2}s_n,
$$

$$
w_{1,n} = s_2 \cdots s_{n-2}s_{n-1}s_n,
$$

$$
w_{1,n+1} = s_2 \cdots s_ns_{n-2},
$$

$$
\vdots
$$

$$
w_{1,2n-4} = s_2 \cdots s_{n}s_{n-2} \cdots s_3,
$$

and
As in the case of $B_n$, this is verified by checking that the elements of \{w_{1j}\} and \{w'_{1j}\}, when applied to \{1, 2\}, give all the elements in the $W_2$-orbit of \{1, 3\}. Note that $w_{1,n-2}$ and $w_{1,n-1}$ have the same length as words in \{s_1, \ldots, s_n\}.

Following the procedure we used in the case of $B_n$, we find the entries in $M'$ by calculating the distribution of left $G_2$-cosets in $G_2w_1G_2w_1^*$ in the different $(G_2, G_2)$-double cosets. The first step is to find $G_2$-coset representatives in $G_2w_1G_2$. This is done using the root structure in $G_2$, and the formulas $G_2s_2U = G_2s_2U_1$, $G_2s_2G_2 = G_2s_2s_3U = G_2s_2s_3U_2^3$, etc. The following tables give the required information.

\begin{table}
\begin{tabular}{|c|c|c|c|c|c|c|c|c|}
\hline
$G_2w_1G_2w_1^*$ & $w_0^*$ & $w_1^*$ & $w_2^*$ & $w_3^*$ & $w_4^*$ & $w_5^*$ \\
\hline
$G_2w_1G_2w_1^*$ & $w_0^*$ & $x$ & $w_1^*$ & $w_2^*$ & $w_3^*$ & $w_4^*$ & $w_5^*$ \\
$G_2w_1G_2w_1^*$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{n-2}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{n-2}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{2n-5}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{2n-4}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{n-5}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{n-6}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{n-4}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
\hline
Totals & $0$ & $x(x + 1)\eta'$ & $0$ & $0$ & $0$ & $0$ & $0$
\end{tabular}
\end{table}

\begin{table}
\begin{tabular}{|c|c|c|c|c|c|c|c|c|}
\hline
$G_2w_1G_2w_1^*$ & $w_0^*$ & $w_1^*$ & $w_2^*$ & $w_3^*$ & $w_4^*$ & $w_5^*$ \\
\hline
$G_2w_1G_2w_1^*$ & $1$ & $x - 1$ & $w_2^*$ & $w_3^*$ & $w_4^*$ & $w_5^*$ \\
$G_2w_1G_2w_1^*$ & $x^2$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{2n-6}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{2n-5}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^2$ & $x^3$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{2n-5}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
$G_2w_1G_2w_1^*$ & $x^{2n-4}$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ & $\ldots$ \\
\hline
Totals & $1$ & $\lambda + \mu x^2$ & $x\nu'$ & $\mu x^3$ & $x^2\nu'$ & $0$
\end{tabular}
\end{table}
Remark. In checking these results, it is useful to know that $w_2^*$ has the following expression as a product of two commuting reflections:

$$w_2^* = S_{(\alpha_n)s_{n-2}} \cdots S_{(\alpha_{n-1})s_{n-2}} = S_{x_2+\epsilon_n} S_{x_2-\epsilon_n}.$$
**Remark.** In this case, it is helpful to express \( w_4^* \) as a product of three commuting reflections:

\[
 w_4^* = S_{e_2 + e_n} S_{e_2 - e_n} S_{e_1 - e_3}.
\]

**Remark.** As in the case of \( B_n \), this time \( w_5^* = S_{e_1 + e_2} \).

These computations prove Lemma (6.18).

(6.19) **Lemma.** \(|G : G_2| = (q^{2n-2} - 1)(q^n - 1)(q^{n-2} + 1)/(q^2 - 1)(q + 1)\).

**Proof.** Table 3.

We are now in a position to complete the proof of (6.16). We proceed as in the
case of $B_n$. We note that the matrix $M'$ is obtained from the matrix $M$ by setting $y = 1$. Consequently, setting $y = 1$ in (6.8) gives the roots of $M'$. Thus, using (6.19), we have a formula for the degrees of the irreducible constituents in $1G_{G_2}$, as in (6.14).

Let $\delta_i(t, 1) = \Pi_{\alpha_j \neq \alpha_i} (\theta_j(t, 1) - \delta_j(t, 1))$. A direct computation, which we omit, shows that $\delta_i(t, 1) \in Z[t]$, and that $\pm \delta_i(t)$ is monic except in the following cases: $\delta_i(t, 1) = \pm 2\delta_i(t)$, with $\delta_i(t)$ monic, in case $i = 3$ and $i = 5$. As in the $B_n$ case, we conclude that the generic degrees $d_i(t)$ are in $Z[t]$ if $\delta_i(t, 1)$ is monic, and $d_i(t) = \frac{1}{2} d_i(t)$, with $d_i(t) \in Z[t]$ in case $i = 3$ or $i = 5$. Apply (5.3) to conclude that $q$, and hence $p$, divides $d_i(q)$ in case $d_i(t) \in Z[t]$, and that $p$ divides $d_i(q)$ in all cases except possibly when $q = p = 2$ and $i = 3$ or 5.

It remains to prove that when $q = p = 2$, neither of the degrees $d_3(2)$ nor $d_5(2)$ can be odd. This follows in exactly the same way as at the corresponding point at the end of the proof of (6.5). This completes the proof of Proposition (6.16).

7. Proof of Theorem (5.7): Conclusion. The remaining cases of (5.7) will be handled separately. Except for the treatment of $2F_4(q)$ in (7.26), we will not use the intersection matrix approach of §6. Instead, we will primarily use an ad hoc method based on the algebraic properties of the polynomials discussed in §5. If $h(t) \in Q[t]$ and $h(t) = a_k t^k + a_{k+1} t^{k+1} + \cdots + a_t t^t$, where $k \leq l$ and $a_i \in Q$, we will say that $h(t)$ leads with $a_k t^k$ and has highest term $a_t t^t$.

(7.1) Proposition. If $G = E_6(q)$, then Theorem (5.7) holds.

Proof. By (5.4), $1G_{G_1}$ contains the reflection character $\rho$. By (4.3)(ii) and Table 4, $1G_{G_1} - 1G$ is the sum of $\rho$ and an irreducible character, both of which have degrees divisible by $q$. In view of the symmetry between $G_1$ and $G_6$, we now need only consider $1G_{G_2}$. By (4.3)(ii), $1G_{G_2} \supseteq 1G_{G_1}$.

Suppose some irreducible constituent of $1G_{G_2} - 1G$ has degree not divisible by $p$. Then, by (5.6), $q = 2, 3,$ or 5. Also, by (4.3)(ii), Table 4, and (5.2), one of the two irreducible constituents of $1G_{G_2} - 1G_{G_1}$ has degree not divisible by $p$, and we can write

\[
\frac{f_1(t)}{f_1(1)} + \frac{f_2(t)}{f_2(1)} = (t^4 + 1)(t^9 - 1)(t^9 - 1)^{-1}(t^{12} - 1)(t^{3} - 1)^{-1}
\]

(7.2)

\[
- (t^9 - 1)(t^9 - 1)^{-1}(t^{12} - 1)(t^{4} - 1)^{-1},
\]

where $f_i(t) \in Q[t], f_i(1) = 15$ and $f_2(1) = 30$. Since some $f_i(t)$ is not monic, and since the right side of (7.2) leads with $t^3$, we can write $f_1(t) = (a/c)t^3f_1^{\text{cycl}}(t)$ and $f_2(t) = (b/d)t^2f_2^{\text{cycl}}/(t)$, as in (5.5), where $(a/c) + (b/d) = 1$ and $(a, c) = (b, d) = 1$. Then $c = d$ and $a + b = c$. Also, $|W| = 2^7 3^4 5$ and $3^2 |c|$ imply that $q = 2$ or 3 (see (5.5)(v)).

The right side of (7.2) is divisible by $\Phi_3(t)$, where $\Phi_3(t) = 5$. Also, $5 | f_1(1)$ and $5 | f_2(1)$, while $5$ cannot divide both $a$ and $b$. As $f_1^{\text{cycl}}(t)$ is a product of cyclotomic polynomials by (5.5)(i), $\Phi_3(t)$ divides one and, hence, both $f_i(t)$'s. As $5^2 \nmid f_1^{\text{cycl}}(t)$, $5 \nmid a, b$. Also, $5^2 \nmid |W|$, so $\Phi_3(t)^2 \nmid f_1^{\text{cycl}}(t)$. Since $5 | f_1(1)$, it follows that $5 \nmid c$.

We now have: $a + b = c; (a, b) = 1; 5 \nmid a, b, c; q^3 |c; and a, b, c | |W|$. Since these conditions cannot be satisfied, this is a contradiction.
In each of the cases $2E_6(q)$, $E_7(q)$, $E_8(q)$, and $F_4(q)$, we shall use the following notation. The representation $1_{G_f}$ is the sum of $1$, $\zeta_{q,f}$ (the reflection character; see (5.4)) and three other characters of $G$. Accordingly, we apply (5.5) and write

$$f_1(t) + f_2(t) + f_3(t) = h(t) - 1 - d(t),$$

where $h(t) \in \mathbb{Z}[t]$ is the polynomial such that $h(q) = [G(q): G_{q,f}(q)]$, and $f_j(t) \in \mathbb{Q}[t]$ for $j = 1, 2, 3$ are the generic degrees of the three other characters of $G$ in $1_{G_f}$. Let $\varphi_1, \varphi_2, \varphi_3$ be the irreducible degrees of the three other characters of $G$ in $1_{G_f}$. Let $\varphi_1(t) = d_1(t)$, $\varphi_2(t) = d_2(t)$, $\varphi_3(t) = d_3(t)$, and set $k = k_3$.

(7.4) Lemma. Let $G = 2E_6(q), E_7(q), E_8(q), \text{ or } F_4(q)$, and let $h(t) = \sum \varphi(j)(\mathbb{Z}[t])$ as in (5.3). The leading term of $h(t) - 1 - d(t)$, where $\varphi$ is the reflection character, is, respectively, $2t$, $2t^2$, $3t^2$, and $t$. In each case this term is $\varphi_j(t)^{\alpha_j}$ for some $j = 1, 2$ or 3. If $G$ is $2E_6(q), E_7(q)$ or $E_8(q)$, then $f(t)$ is monic. If $G = F_4(q)$, then $\alpha_j = \frac{1}{2}$.

Proof. We use the formula for $|G(q)|$ and Table 4 to check the first statement. Next apply Table 4, and note that the right side of (7.3) leads with $t$, $t^2$, $\frac{1}{2}t$, respectively. Consequently, this term has the form $\alpha_j t^{\alpha_j}$, $(\alpha_j + 1)\alpha_j$ or $(\alpha_1 + \alpha_2 + \alpha_3)^{\alpha_1}$, respectively. Therefore $1 = \alpha_j, \alpha_j + \alpha_i$ or $\alpha_1 + \alpha_2 + \alpha_3$ if $G = 2E_6(q), E_7(q)$, or $E_8(q)$, and $\frac{1}{2} = \alpha_j, \alpha_j + \alpha_i$ or $\alpha_1 + \alpha_2 + \alpha_3$ if $G = F_4(q)$.

The set of numbers $\{\varphi_1(1), \varphi_2(1), \varphi_3(1)\}$ is, respectively, $\{2, 8, 9\}$, $\{27, 35, 56\}$, $\{35, 84, 112\}$ or $\{2, 8, 9\}$ (see Table 4). The coefficient of the leading term of $h(t) - 1 - d(t)$ is at least $\varphi(j)d(t)$, where $\varphi$ is the reflection character, is, respectively, $2t$, $2t^2$, $3t^2$, and $t$. The only possibilities are as follows: $\alpha_j = 1$ and $\varphi_1(1) = 2, 27, \text{ or } 35$, respectively, if $G = 2E_6(q), E_7(q)$ or $E_8(q)$; and $\alpha_j = \frac{1}{2}$ and $\varphi_1(1) = 2$ if $G = F_4(q)$. This completes the proof of (7.4).

Next apply (5.10) to (7.3) to obtain

$$f_1(t)(d^{d+k-d_1-b_1} - 1) + f_2(t)(d^{d+k-d_2-b_2} - 1)$$

$$= h(t)(t^{k} - 1) - (d^{d+k} - 1) - d(t)(d^{d+k} - 1)$$

where $a = \deg(d(t))$ and $b^b$ is the highest power of $t$ dividing $d(t)$. Differentiating (7.5) and setting $t = 1$ yields

$$f_1(1)(d + k - d_1 - b_1) + f_2(1)(d + k - d_2 - b_2)$$

$$= h(1)(d + k - \varphi(1)(d + k - a - b)).$$

(7.7) Proposition. If $G = 2E_6(q)$, then Theorem (5.7) holds.

Proof. Assume the result is false. By Table 4, $q|\varphi(1)$, and so $p \nmid f_i(t)$ for some $i = 1, 2, 3$. For $i$ chosen as in (7.4), we have $i \neq j$.

In this case the right side of (7.3) leads with $t$ and has highest term $t^{21}$. Then $d = 21$. From Table 4 we have $a = 16, b = 2$. Then (7.6) becomes

$$f_1(1)(21 + 2 - 1) + f_2(1)(21 + 2 - 1) = 19k - 33.$$
By Table 4, \(\{f_1(1), f_2(1), f_3(1)\} = \{2, 8, 9\}\), and by (7.4), \(f_1(1) = 2\) and \(f_3(t)\) is monic. We claim that for \(s = 1, 2\) or 3, \(f_s(1) = 9\) implies \(k_s \geq 3\). By (4.3)(i) and (5.2) the constituent of \(1^G_{G_4^*}\) with generic degree \(f_s(t)\) also appears in \(1^G_{G_4}\). Writing down the analogue of (7.3) for \(1^G_{G_4^*}\) we obtain an equation in which the right-hand side leads with \(t^3\). By (5.5)(i), \(t^3 | f_3(t)\), and \(k_s \geq 3\), as required.

If \(k = 1\), then \(f_1(t) + f_2(t) = k(t) - 1 - d_1(t) - f_3(t)\), and the right side is in \(Z[t]\) since \(k(t) = 1\) \(d_1(t)\) leads with \(t\). Thus \(k_1 = k_2 \geq 3\) and \(d_1 = d_2 < 21\). By (7.4) we have \(f_3(1) = 2\). Then (7.8) reads \((21 + 1 - d_1 - k_1)(17) = 19 - 33\), which is impossible.

Therefore \(k > 1\), and we may assume \(k_1 = 1, f_1(t)\) is monic, and \(f_1(1) = 2\). Then \(k_2 = k_3 \geq 3\). Write \(f_2(t) = (a/c)t^k f_2^*(t)\) and \(f_3(t) = (b/d)t^k f_3^*(t)\), according to (5.5). As the highest term on the right side of (7.3) is \(t^{21}\), we have \(d_1 < 21\) and \((a/c) + (b/d) = 1\). Thus \(c = d\) and \(a + b = c\). By (5.5), \(d^k | c\); \(a\) and \(b\) divide \(|\mathcal{W}|\); and \(c | |\mathcal{W}|^2\). Since \((a, b) = 1\) and \(k \geq 3\), these conditions are impossible, and the proof of Proposition (7.7) is completed.

(7.9) Proposition. If \(G = E_7(q)\), then Theorem (5.7) holds.

Proof. Assume the result is false. We proceed as in the case of \(2F_4(q)\). By Table 4, \(q\phi(l)\), so \(p \nmid f_j(q)\) for \(i = 1, 2\) or 3. With \(j\) as in (7.4), \(f_j(1) = 27\) and \(f_j(t)\) is monic.

In this case, the right side of (7.3) leads with \(t^2\) and has highest term \(t^{33}\). Thus \(d = d_3 = 33\) and by Table 4, \(a = 17\) and \(b = 1\). Then (7.6) reads

\[
(7.10) \quad f_1(1)(33 + k - d_1 - k_1) + f_2(1)(33 + k - d_2 - k_2) = 118k - 138.
\]

If \(k = 2\), then \(f_3(t)\) is monic, and as in the case of \(2F_4(q)\), we have \(k_1 = k_2\) and \(d_1 = d_2\). Then (7.10) reads \((35 + 56)(38 - d_1 - k_1) = 236 - 138\), which is impossible.

Consequently, \(k > 2\), and we may assume that \(k_1 = 2\), and that \(f_1(t)\) is monic. Then \(d_1 < 33, k_2 = k_3 \geq 3\), and \(d_2 = d_3\). Write \(f_2(t) = (a/c)t^k f_2^*(t)\) and \(f_3(t) = (b/d)t^k f_3^*(t)\) as in (5.5). Then since the highest term on the right side of (7.3) is \(t^{36}\), we have \((a/c) + (b/d) = 1\), so \(c = d\) and \(a + b = c\). Moreover \(q^k | c\) by (5.5), \(a\) and \(b\) divide \(|\mathcal{W}|\), and \(c | |\mathcal{W}|^2\). We may assume that \(f_2(1) = 35\) and \(f_3(1) = 56\).

(7.11) Lemma. Each nonprincipal irreducible constituent of \(1^G_{G_7}\) has degree divisible by \(q\). Moreover, \(1^W_{\tau(1)} = 1 + \varphi + \varphi_1 + \tau\), where \(\varphi\) is the reflection character and \(\tau(t)\) is monic.

Proof. By (4.3)(iii), \(1^W_{\tau(1)} \) decomposes as in the statement of (7.11), and \(\tau(1) = 21\). It suffices to show that \(\tau(t)\) is monic. From (5.2) and (4.3) we obtain

\[
(7.12) \quad d_4(t) + f_4(t) = (t^5 + 1)(t^9 + 1)(t^{14} - 1)(t - 1) - t(t^6 + 1)(t^{14} - 1)(t^5 + 1) - t(t^6 - 1).
\]

Since \(f_4(t)\) is monic, \(d_4(t) \in Z[t]\). The right side of (7.12) is monic of degree 27, so if \(d_4(t)\) is not monic, \(\deg(d_4(t)) < 27\) and \(d_4 - 27\). Apply (5.10) to (7.12) to obtain...
\[ d_4(t)(t^{29} - v - 1) = (t^5 + 1)(t^9 + 1)(t^{14} - 1)(t - 1)^{-1}(t^2 - 1) - (t^{29} - 1) \]
(7.13)
\[- t(t^6 + 1)(t^{14} - 1)(t^2 + 1)^{-1}(t^2 - 1)^{-1}(t^{29} - 17 - 1) - 1)\]
where \( u = \deg(d_4(t)) \) and \( t^v \) is the highest power of \( t \) dividing \( d_4(t) \). Differentiate (7.13), and evaluate at \( t = 1 \), to obtain
\[ 21(29 - u - u) = 6, \]
which is impossible. This completes the proof of (7.11).

We now complete the proof of (7.9) by obtaining properties of \( a, b \) and \( c \) that lead to a contradiction. Since \( a | \phi_2(1) \) and \( b | \phi_3(1) \), we have \( 3 \nmid a, b; 2 \nmid a, \) and \( 5 \nmid b \). The possibilities for \( q \) are 2, 3, 5, 7, and we have \( q | \phi(1) \), and \( f_2^\#(1) | \mathcal{W} \), by (5.5). Since \( 5^2 \nmid | \mathcal{W} | \) and \( 7^2 \nmid | \mathcal{W} | \), it follows that \( q = 2 \) or \( 3 \). Finally, neither 5 nor 7 divide \( c \), otherwise \( 5^2 \) or \( 7^2 \) divide \( f_3^\#(1) \) or \( f_2^\#(1) \), respectively, which is impossible.

By (7.11), \( d_4(t) \) is monic. Since \( d_4(t) \) has to be a multiple of 7, a check of the cyclotomic polynomials in the formula for the order of \( E_6(q) \) shows that \( \Phi_7(t) | d_4(t) \). Subtracting (7.12) and (7.3), we find that \( \Phi_7(t)|f_2(t) + f_3(t) \). Since 7 cannot divide both of \( a \) and \( b \) (since \( a + b = c \)) we conclude that \( \Phi_7(t) \) divides one and hence both of \( f_2(t) \) and \( f_3(t) \). Since \( 7^2 \nmid | \mathcal{W} | \), this shows that \( 7 \nmid a \) and \( 7 \nmid b \). It is now easy to check that there are no possible solutions for \( a, b, \) or \( c \). This completes the proof of (7.9).

(7.15) PROPOSITION. If \( G = E_6(q) \), then Theorem (5.7) holds.

PROOF. Assume once more that the result is false. By Table 4, \( q | \rho(1) \), so \( p \nmid f_i(q) \) for some \( i = 1, 2, 3 \). With \( j \) as in (7.4), \( f_j(1) = 35 \), and \( f_j(t) \) is monic.

The right side of (7.3) has highest term \( t^{57} \), so that \( d = d_3 = 57 \). By Table 4, \( a = 29 \) and \( b = 1 \). Thus (7.5) reads
\[ f_1(1)(57 + k - d_1 - k_1) + f_2(1)(57 + k - d_2 - k_2) = 21(11k - 13). \]
(7.16)
The right side of (7.3) leads with \( t^2 \). Then each \( k_i \geq 2 \), and some \( k_i = 2 \). We assert that \( k > 2 \). If not, then \( k = 2, f_2(t) = f_3(t) \) is monic, and \( f_3(1) = 35 \). Moreover \( d_1 < 57 \) and \( d_2 < 57 \). As in the previous cases, two \( k_i \)'s and two \( d_i \)'s must be equal. It follows that \( k_1 = k_2 \) and \( d_1 = d_2 \). Now (7.16) reads
\[ (84 + 112)(57 + 2 - d_1 - k_1) = (21)9, \]
which is impossible. Thus \( k > 2 \).

We may now order the \( f_i(t) \)'s so that \( k_1 = 2 \); then \( f_1(t) \) is monic and \( k_2 \) and \( k_3 > 2 \). If \( f_3(t) \in \mathbb{Z}[r] \), then \( f_2(t) \) also belongs to \( \mathbb{Z}[r] \), which is not the case. Therefore \( f_3(t) \notin \mathbb{Z}[r] \), and this time \( d_2 = d_3 \) and \( k_2 = k_3 \).

Put \( \alpha_2 = a/c_2, \alpha_3 = b/c'c \) as in (5.5). Then \( (a/c) + (b/c') = 1 \) so \( a + b = c = c' \).

By (5.5), \( q | \phi(1) \), where \( k \geq 3 \). Also \( (a, b) = 1 \), and we may assume that \( f_2(1) = 84 \) and \( f_3(1) = 112 \). Thus \( 5 \nmid a, 5 \nmid b, 3^2 \nmid a, 3 \nmid b, 2^3 \nmid a, \) and \( 5^5 \nmid b \).

We claim that \( 7 \nmid a, b \). Since \( f_1(t) \) is monic, the argument used in the proof of (7.9) shows that \( \Phi_7(t)|f_1(t) \). so by (7.3) and Table 4, we have \( \Phi_7(t)|f_2(t) + f_3(t) \). As
7|f_i(1) and 7^2 \nmid f_i(1) for i = 1, 2, 3, it follows that \Phi_i(t) divides one, and, hence, both of f_2(t) and f_3(t). Thus, 7 \nmid a, b.

As q^3|c, q = 2 or 3. Suppose q = 3. Then 3^3|c, while c = a + b < 1 + 16 which is impossible. Thus q = 2, and both a and b are odd. But this leads to an impossible diophantine equation. This completes the proof of (7.15).

(7.18) Proposition. Let G = F_4(q). Then the f_i(t)'s can be numbered so that the following statements hold.

(i) \deg f_3(t) = 15.
(ii) 9 \leq \deg f_1(t) \leq 15, 8 \leq \deg f_2(t) \leq 15.
(iii) f_1(t) = (\frac{a}{b})f_1^#(t), f_1^#(t) \in \mathbb{Z}[t], f_1^#(0) = 1, f_1(1) = 2. In particular, f_1(2) is odd, and 3|f_1(3).
(iv) \mathfrak{f}_1|f_2(t), f_3(t).
(v) 2|f_2(2), f_3(2), and 3|f_2(3), f_3(3).
(vi) Theorem (5.7) holds for F_4(q), q > 2.

Proof. By (7.4), if f_2(1) = 2, then f_2(t) = (\frac{a}{b})f_2^#(t). Since the right side of (7.3) leads with (7.4) if i \neq j, then k_i \geq 2.

Reorder the f_i(t)'s so that i = 1. Then (iiii) holds. The highest term on the right side of (7.3) is t^{15}, so for some i > 1, d_i = 15. We may assume i = 3. Then (i), (iii), (iv) hold.

Suppose that f_2(2) or f_3(2) is odd. Using (7.3), with t = 2, and noting that f_1(2) is odd, it follows that both f_2(2) and f_3(2) are odd. Write \alpha_2 = (a/b), \alpha_3 = c/d, with (a, b) = (c, d) = 1. Then by (5.5), 2^k|b, c and k > 2. If d_2 < 15, then from (7.3), it follows that \alpha_3 = 1 or \frac{a}{b}, a contradiction. Thus d_2 = d_3 = 15, and \alpha_2 + \alpha_3 = 1 or \frac{a}{b}. This implies that k = 2, and k_2 = 2. Now (7.6) reads f_1(1)(15 + 2d_1 - 1) = 11, which is impossible as f_1(1) = 8 or 9.

Similarly, if f_2(3) or f_3(3) is not divisible by 3, then the corresponding denominator of \alpha_i is divisible by 9. From (7.3) it follows that 3 divides neither f_2(3) nor f_3(3). As above, k_2 = k, d_2 = d_3 = 15. Since 27 \nmid \mathfrak{f}_1, k = 2. This leads to the same contradiction as before.

This proves (v) and, hence, also (5.7) for 1^G_{G_1}. We must also prove (5.7) for 1^G_{G_4}. Let q be even. Then G has an outer automorphism interchanging G_1 and G_4. Thus, the degrees of the irreducible constituents of 1^G_{G_1} and 1^G_{G_4} agree for all even q. By (5.2), the correspondence generic degrees agree. Hence, for all q, the degrees of the irreducible constituents of 1^G_{G_1} and 1^G_{G_4} agree. Since (5.7) is known for 1^G_{G_1}, it must hold for 1^G_{G_4}. This proves (vi).

It remains only to prove (ii). We will show that f_i(q) \nmid q^7(q - 1) for each i and all odd primes q. Once this is known, it follows that d_i \geq 8 and also d_1 \geq 9 as \alpha_1 = \frac{a}{b}. We already know that d_1 \leq 15 and d_2 \leq 15.

Consequently, consider G = F_4(q) with q an odd prime. By (4.5), Q_1 is extra-special of order q^{15} with center U_1. Let \chi be a nonprincipal irreducible constituent of 1^G_B of degree f_i(q). Then \chi is faithful, so there is an irreducible constituent \theta of \chi|G_1 with U_1 \nsubseteq \ker \theta. Applying Clifford's theorem, we obtain \theta|Q_1 =

}{

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
\[ a(\xi_1 + \cdots + \xi_0), \text{ where } a \in \mathbb{Z} \text{ and the } \xi_i's \text{ are distinct conjugate irreducible characters of } Q_1. \] Then \[ \xi_i|U_r = \xi_i(1)\varphi_i \text{ for a nonprincipal linear character } \varphi_i \text{ of } U_r. \] Moreover, one and, hence, all \( \xi_i's \) are faithful, so since \( Q_1 \) is extraspecial we must have \( \xi_i(1) = q^7. \)

Since \( H \) is transitive on the \( q - 1 \) nonprincipal characters of \( U_r \), each such character appears as a \( \varphi_i \). Thus, \( \chi(1) \gg (q - 1)q^7 \), as required.

We remark that a much more detailed analysis similar to the above can be used to show that, for all \( i = 1, 2, 3 \) and all \( q = 2^a \), \( f_i(q) \gg q^6(q^3 - 1)(q - 1) \). From this it follows that \( d_1 \gg 11 \) and \( d_2 \gg 10 \).

We next prove Theorem (5.7) in case \( G \) is a classical group having \( (B, N) \)-rank 3 (except for \( PSO^+(6, q) \approx PSL(4, q) \), which has already been handled in (5.9)).

(7.19) **Proposition.** If \( G \) is \( PSp(6, q) \) with \( q > 2 \), \( PSO(7, q)' \) with \( q \) odd, \( PSO^-(8, q)' \), \( PSU(6, q) \), or \( PSU(7, q) \), then Theorem (5.7) holds.

**Proof.** \( 1G_G - 1G - \rho \) is irreducible, where \( \rho \) is the reflection character. Since \( |G : G_1| \equiv 1 \pmod{q} \), Table 3 shows that \( \rho \) and this character have degrees divisible by \( p \).

It is easy to check, as in §6, that \( 1G_G \geq 1G_G - 1G_G \) and \( 1G_G - 1G_G \) is the sum of two irreducible characters. Let \( f_1(t) \) and \( f_2(t) \) be the corresponding generic degrees (see (5.2)). Then

\[ f_1(q) + f_2(q) = |G : G_2| - |G : G_1|. \]

Thus, \( f_1(t) + f_2(t) \) leads with \( t^2 \) for \( PSp(6, q) \) and \( PSO(7, q)' \), \( t^3 \) for \( PSU(6, q) \) and \( PSO^-(8, q)' \), and \( t^5 \) for \( PSU(7, q) \). Since \(|W| = 48\), by (5.5)(v) we may assume that \( q = 2 \), so \( G \) is \( PSU(6, q) \) or \( PSO^-(8, q)' \).

In these cases, if (7.19) is false we are led, as in (7.1), to an equation of the form \( a + b = c \) with \( 8 \mid c \) and \( a, b \) odd divisors of 48. There is obviously no solution.

(7.21) **Lemma.** If \( G \) is \( Sp(2n, 2) \), \( n \gg 3 \), then each irreducible constituent of \( 1G_G - 1G_G \) has even degree.

**Proof.** If \( n \gg 4 \), the lemma is proved exactly as at the very end of the proof of (6.5).

Let \( n = 3 \), and deny (7.21). By (7.24), \( f_1(t) + f_2(t) \) leads with \( t^2 \), and we again have an equation \( a + b = c \) with \( 4 \mid c \), \( 8 \mid c \), \( (a, c) = 1 \), and \( a, b, c \mid |W| = 48 \). We may thus assume that \( 3 \mid b \) and \( 3 \nmid a \). As in §4, it is easy to check that \( f_1(1) = f_2(1) = 3 \), so \( \Phi_3(t) = f_1(t) \) by (5.5)(ii). But \( \Phi_3(t) \) divides the right side of (7.20). Consequently, \( \Phi_3(t) = f_2(t) \). Since \( 3b, 3 \Phi_3(1) = 9 \) divides \( f_2(1) \), which is a contradiction.

We remark that the degrees of the constituents of \( 1G_G - 1G_G \) can be found in [3] when \( G = Sp(2n, 2), n \gg 4 \).

(7.22) **Proposition.** Theorem (5.7)(i) holds when \( n = 2 \). More precisely, the degrees of the irreducible constituents of \( 1G_G \) are as follows; moreover, in each list, the second degree is that of the reflection character, while the third and fourth characters occur with multiplicity one in \( 1G_G \) for precisely one \( i \).

(i) For \( Sp(4, q) \): \( 1, \frac{1}{2}q(q + 1)^2, \frac{1}{2}q(q^2 + 1), \frac{1}{2}q(q^2 + 1), q^4 \).
(i) For $\text{PSU}(4, q)$: $1, q^2(q^2 + 1), q^3(q^2 - q + 1), q(q^2 - q + 1), q^6$.

(ii) For $\text{PSU}(5, q)$: $1, q^2(q^2 + 1)(q^2 - q + 1), q^3(q^5 + 1)(q + 1), q^4(q^5 + 1)(q + 1), q^{10}$.

(iii) For $\text{PSU}(6, q)$: $1, q^3(q^2 - 1)(q^2 - q + 1), q^2(q^4 + q^2 + 1), (1/3)q^3(q^4 - q^2 + 1), q^6$.

(iv) For $G_2(q)$: $1, (1/6)(q + 1)^2(q^2 + q + 1), (1/3)(q(q^4 + q^2 + 1), (1/2)(q + 1)(q^3 + 1), q^6$.

(v) For $3D_4(q)$: $1, q^2(q^3 + 1)^2, q^3(q^4 - q^2 + 1), q^4 - q^2 + 1), \frac{1}{2}q^3(q + 1)^2(q^4 - q^2 + 1), q^{12}$.

(vi) For $2F_4(q)$: $1, q^2(q^2 - 1)(q^3 + q^2 + 1)(q^2 + 1)(q + 1)(q^2 + 1), q^6$.

Proof. (i)–(v) are proved as in the proof of [32, Theorem D] using information in [32]. (We note, however, that the value of $\rho(1)$ for $3D_4(q)$ is incorrectly stated on [12, p. 111].) We will outline the proof for $G = 2F_4(q)$. Here $W$ is dihedral of order 16, has 4 irreducible characters of degree 1, and 3 of degree 2. By (5.2), $\text{IG}_i$ has 7 irreducible constituents, 4 appearing with multiplicity 1, and 3 with multiplicity 2. The degrees of the former are found on p. 115 of [12], while one of the latter is the reflection character. This leaves two characters. Each of these appears in $\text{IG}_i$ for $i = 1$ and 2; of the characters occurring in $\text{IG}_i$ with multiplicity 1, each of the ones discussed in [12, §10] appears in $\text{IG}_i$ for precisely one $i$.

Thus, consider $\text{IG}_i$. We may take the index parameters to be $c_1 = 1$, $c_2 = 2$. If $W = \langle s_1, s_2 \rangle$ as in §2, let $\xi_{s_2}$ be the corresponding element of the Hecke algebra $H(G, \text{IG}_i)$. Then, with respect to the standard basis $\xi_1, \xi_{s_2}, \xi_{s_2^2}, \xi_{s_2^3}, \xi_{s_2}(s_1s_2)^2, \xi_{s_2}(s_1s_2)^3$, right multiplication by $\xi_{s_2}$ has the following matrix.

$$M = \begin{pmatrix}
0 & q^2(q + 1) & 0 & 0 & 0 \\
1 & q^2 - 1 & q^3 & 0 & 0 \\
0 & 1 & q^2 - 1 & q^3 & 0 \\
0 & 0 & 1 & q^2 - 1 & q^3 \\
0 & 0 & 0 & q + 1 & (q^2 - 1)(q + 1)
\end{pmatrix}.$$ 

Here $M$ has characteristic roots $q^2(q + 1), -(q + 1), q^2 - 1, q^2 \pm \sqrt{2q} - 1$. Now the proof can be completed as in (6.1)(ii).

8. Proof of Theorem (5.8). Replace $G$ by the corresponding linear group $G = \text{Sp}(2n, q)$, $SO^{+}(l, q^2)$, or $SU(l, q)$, and let $V$ be the underlying vector space for the usual representation of $G$. Then $G_1$ is the stabilizer of an isotropic 1-space (or singular 1-space, for orthogonal groups of characteristic 2), $G_2$ is the stabilizer of an isotropic (or singular) 2-space, and $G_{12}$ is the stabilizer of an incident isotropic (or singular) 1- and 2-space.
For most of this section, we will assume the existence of isotropic (or singular) 4-spaces; the remaining cases will be discussed at the end of the section. The following inner products are then readily computed.

\[(1^G_{G_1}, 1^G_{G_1}) = 3,\quad (1^G_{G_2}, 1^G_{G_2}) = 6,\quad (1^G_{G_{12}}, 1^G_{G_{12}}) = 17;\]
\[(1^G_{G_1}, 1^G_{G_2}) = 3,\quad (1^G_{G_1}, 1^G_{G_{12}}) = 5,\quad (1^G_{G_2}, 1^G_{G_{12}}) = 9.\]

Those inner products not involving \(G_{12}\) were already given in (6.4). The remaining inner products are not difficult to check using the geometry. Let \(V_1\) be an isotropic (or singular) 1-space of \(V\) contained in an isotropic (or singular) 2-space \(V_2\) of \(V\). Suppose \(G_{12}\) stabilizes \(V_1\) and \(V_2\). Then to find \((1^G_{G_{12}, G_{12}})\) it suffices to find the number of orbits of \(G_{12}\) on the pairs \((A_1, A_2)\), where \(A_i\) is an isotropic (or singular) 1-space of \(V\) and \(A_1 < A_2\). Given \((A_1, A_2)\) and \((A'_1, A'_2)\), consider the subspaces \(V_2 + A_2\) and \(V_2 + A'_2\). If these are isometric by an isometry \(\tau\) such that \(V'_1 = V_1, V'_2 = V_2, A'_1 = A_1,\) and \(A'_2 = A_2\), then Witt's theorem guarantees that \((A_1, A_2)\) and \((A'_1, A'_2)\) are in the same orbit of \(G_{12}\). Using these facts, one can list the 17 orbits of \(G_{12}\). The other inner products are computed similarly.

Write
\[1^G_{G_1} = 1^G_G + \rho + \chi_1 \quad \text{and} \quad 1^G_{G_2} = 1^G_G + \rho + \chi_1 + \chi_2 + \chi_3 + \chi_4.\]

where \(\rho\) is the reflection character and \(\chi_1, \chi_2, \chi_3, \) and \(\chi_4\) are distinct and irreducible. By (5.4), \((\rho, 1^G_{G_{12}}) = 2\), so by (8.1), \((\chi_1, 1^G_{G_{12}}) = 2\). Then (8.1) shows that we can choose notation so that
\[1^G_{G_{12}} = 1^G_G + 2\rho + 2\chi_1 + 2\chi_3 + \chi_4 + \chi_6.\]

where \(1^G_G, \rho, \chi_1, \chi_3, \chi_4, \chi_5, \) and \(\chi_6\) are distinct irreducible characters of \(G\).

Clearly \(G_1\) induces a classical group on \(V_1/V_1\), with \(G_{12}\) corresponding to the stabilizer of an isotropic 1-space. Thus, \(1^G_{G_{12}} = 1^G_G + \sigma_1 + \sigma_2\) with \(\sigma_1\) and \(\sigma_2\) distinct nonprincipal irreducible characters. Then
\[\sigma_1^G + \sigma_2^G = (1^G_{G_{12}} - 1^G_G)^G = \rho + \chi_1 + 2\chi_2 + \chi_3 + \chi_4 + \chi_5 + \chi_6.\]

We will decompose the characters \(\sigma_1^G\) and \(\sigma_2^G\).

By the Mackey subgroup theorem,
\[\left(\sigma_1^G, \sigma_2^G\right) = \sum_{G_1 \in G, w \in G_1} \left(\sigma_1^{G_1}, \sigma_2^{G_1}\right) G_1^w G_1\]

where the sum ranges over the double cosets of \(G_1\) in \(G\). We can choose \(w \in \mathcal{W}\) with \(V_1 = V_1 w < V_2\), so \(G_1^w \cap G_1 < G_{12}\). Since \(\sigma_1|G_{12}\) and \(\sigma_2|G_{12}\) both contain \(1^G_{G_{12}}\), it follows that \((\sigma_1^G, \sigma_2^G) > 1\). Consequently, by (8.2) both \(\sigma_1^G\) and \(\sigma_2^G\) contain \(\chi_2\).

The same calculations show that, for \(i = 1, 2\),
\[\left(1^G_{G_1}, \sigma_i^G\right) > \left(1^G_{G_1} G_1^w, \sigma_i\right) G_1^w G_1 > 1\]

(Where \(w\) is as above). We can thus number the \(\sigma_i\)'s so that \(\rho < \sigma_1\) and \(\chi_1 < \sigma_2\).
We next consider \((l_{G_2}, o_{l_{G_2}}')\). There are three \((G_2, G_1)\)-double cosets: \(G_2 G_1\), \(G_2 x G_1\), and \(G_2 y G_1\). \(V_1 + (V_2) x\) is an isotropic (or singular) 3-space and \((V_1, V_2) y \neq 0\). Then \(G_2^y \cap G_1\) fixes \(V_1\) and \((V_2) x\). Since \(V_1 + (V_2) x\) is an isotropic (or singular) 3-space, it follows that \(G_2^y \cap G_1\) is conjugate in \(G_1\) to a subgroup of \(G_{13}\). Note that \(o_1\) and \(o_2\) are constituents of \(l_{G_1}^1\), just as \(x_1\) and \(x_2\) are constituents of \(l_{G_2}^2\). Thus, \((1_{G_2}^y \cap G_1, o_1)_{G_2^y \cap G_1} \geq 1\) for \(i = 1, 2\). Also, \(G_2^y \cap G_1\) fixes \(V_1\) and \((V_2) y\), and hence also the isotropic (or singular) 2-space \(V_1 + (V_1) y\), so it is conjugate in \(G_1\) to a subgroup of \(G_{12}\). As before, we find that, for \(i = 1, 2\),

\[
(1_{G_2}^y, o_{l_{G_2}}') = (1, o_1)_{G_2 \cap G_1} + (1, o_2)_{G_2^y \cap G_1} + (1, o_2)_{G_2^y \cap G_1} \geq 3.
\]

We can thus number the \(x_i\)'s so that \(o_1 \geq \rho + x_2 + x_3\) and \(G_2^y \geq x_1 + x_2 + x_4\).

Finally, consider \((1_{G_{12}}^1, o_{l_{G_{12}}}})\). The \((G_1, G_{12})\)-double cosets are \(G_{12} G_1, G_{12} x G_1, G_{12} y G_1, G_{12} w G_1\), and \(G_{12} z G_1\), where

(i) \((V_2) x = V_2\) and \((V_1) x \neq V_1\),

(ii) \(V_1 \nsubseteq (V_2) y\) and \((V_1, V_2) y = 0\),

(iii) \(V_1 \nsubseteq (V_2) w\) and \(rad(V_1 + (V_2) w) = (V_1) w\), and

(iv) \(V_1 \nsubseteq (V_2) z\) and \(rad(V_1 + (V_2) z)\) is a 1-space (of \((V_2) z\)) other than \((V_1) w\).

Then \(G_{12} \cap G_1\) fixes the orthogonal 1-spaces \(V_1\) and \((V_1) x\), so \(G_{12} \cap G_1\) is conjugate in \(G_1\) to a subgroup of \(G_{12}\). Similarly, \(G_{12} \cap G_1\) and \(G_{12} \cap G_1\) are conjugate in \(G_1\) to subgroups of \(G_{12}\). Since \(G_{12} \cap G_1\) fixes the isotropic (or singular) subspaces \(V_1, V_1 + (V_1) y, V_1 + (V_2) y\), it is conjugate in \(G_1\) to a subgroup of \(G_{123}\). Considering the group induced by \(G_1\) on \(V_1 / V_1\), we find that \(o_1\) occurs with multiplicity 2 in \(l_{G_{123}}^1\) just as \(x_1\) and \(x_2\) occur with multiplicity 2 in \(l_{G_{12}}^1\). (In fact, all that was needed for this was \((l_{G_1}^1, l_{G_1}^1) = 5\), and this holds so long as isotropic or singular 3-spaces exist.) Consequently,

\[
(1_{G_{12}}^1, o_{l_{G_{12}}}) \geq 4(1, o_1)_{G_{12}} + (1, o_1)_{G_{12}} \geq 6.
\]

We can thus number the \(x_i\)'s so that

\[
x_1 = \rho + x_2 + x_3 + x_5 \quad \text{and} \quad x_2 = x_1 + x_2 + x_4 + x_6.
\]

By \((5.7)\), \(p\) divides \(\rho(1), x_1(1)\) for \(i = 1, 2, 3, 4, o_1(1)\) and \(o_2(1)\). Consequently, by \((8.3)\) we have \(p|x_5(1), x_6(1)\), as required.

It remains to consider the cases where \(V\) has no isotropic (or singular) 4-space. In the case of \((B, N)\)-rank = 2, \((5.7)\) applies. Thus, we need only consider the case of \((B, N)\)-rank 3, where \(G\) is \(Sp(6, q), SU(6, q), SU(7, q)\), or \(SO^{-}(8, q)'\). Here the computations are very similar to the above, so we just sketch the proof.

The relevant inner products are as follows.

\[
(1_{G_1}^1, 1_{G_2}^1) = 3, \quad (1_{G_2}^1, 1_{G_2}^1) = 5, \quad (1_{G_1^3}^1, 1_{G_1^3}^1) = 6;
\]

\[
(1_{G_1}^1, 1_{G_2}^1) = 5, \quad (1_{G_1}^1, 1_{G_1^3}^1) = 5, \quad (1_{G_2}^1, 1_{G_2}^1) = 8.
\]
This time

\[ 1_{G_1}^G = 1_G + \rho + x_1, \quad 1_{G_2}^G = 1_G + \rho + x_1 + x_2 + x_3, \]

and

\[ 1_{G_{12}}^G = 1_G + 2\rho + 2x_1 + 2x_2 + x_3 + x_4 + x_5, \]

with \( 1_G, \rho, \) and the \( x_i \)'s distinct irreducible characters of \( G \). Define \( \sigma_1 \) and \( \sigma_2 \) as before. Then \( (1_{G_1}^G, 0^G) \geq 1, \) so \( x_2 \in 0_1^G, 0_2^G \). Also, \( (1_{G_1}^G, 0_i^G) \geq 1 \) for \( i = 1, 2 \), so we may assume that \( 0_1^G \supset \rho + x_2 \) and \( 0_2^G \supset x_1 + x_2 \).

Since \( G_1 \) induces a group on \( V_1/V_2 \) having a rank \( (B, N) \)-pair, \( 1_{G_{13}}^G \) contains just one of \( \sigma_1, \sigma_2 \), namely, the reflection character of \( G_1 \). Let \( \sigma_1 \in 1_{G_{13}}^G \) and let \( \sigma_i \neq \sigma_j \). As before, we find that \( (1_{G_{12}}^G, 0_i^G) \geq 3, (1_{G_2}^G, 0_j^G) \geq 2, (1_{G_{12}}^G, 0_i^G) \geq 6, \) and \( (1_{G_{12}}^G, 0_i^G) \geq 5 \). If \( \sigma_i = \sigma_j \) we can renumber so that \( 0_1^G = \rho + x_2 + x_3 + x_4 \) and \( 0_2^G = x_1 + x_2 + x_5 \). If \( \sigma_i = \sigma_2 \), then we renumber so that \( 0_1^G = \rho + x_2 + x_3 \) and \( 0_2^G = x_1 + x_2 + x_4 + x_5 \). In either case we obtain the desired divisibility, completing the proof of (5.8).

PART II. 2-TRANSITIVE REPRESENTATIONS

9. Counting lemmas. The proof of the Main Theorem depends on two elementary counting lemmas.

Let \( G \) be a transitive permutation group on a finite set \( \Omega \), with corresponding permutation character \( \theta \). Let \( \alpha \in \Omega \). Set \( m = |\Omega| = \theta(1) \).

(9.1) **Lemma.** Let \( P \triangleleft G \) be transitive on \( \Omega \), and let \( 1 \neq Q < P \). Suppose \( Q \) intersects \( 1 \) \( G \)-conjugacy classes \( \Sigma_1, \ldots, \Sigma_l \) of nontrivial elements, let \( x_1, \ldots, x_l \) be a system of representatives for these sets, and let \( c_i = |\Sigma_i \cap Q| \). Then

\[ m(|Q \alpha| - 1) = \sum_{i=1}^{l} c_i \theta(x_i). \]

**Proof.** Each orbit of \( Q \) has size \( |Q : Q \alpha| \), while \( Q \) has \( \theta(1) = |Q|^{-1} \sum_{x \in Q} \theta(x) \) orbits. Consequently,

\[ m = |Q : Q \alpha| \cdot \frac{1}{|Q|} \left( m + \sum_{\alpha \neq x \in Q} \theta(x) \right). \]

Simplification yields the lemma.

(9.2) **Lemma.** Suppose \( G \) is 2-transitive on \( \Omega \). If \( \alpha \in G \), then \( m - 1|G : C_G(x)|(\theta(x) - 1) \). In particular, if \( \theta(x) = 0 \) then \( m - 1|G : C_G(x)| \) is an algebraic integer.

**Proof.** Since \( \theta - 1_G \) is irreducible, \( |G : C_G(x)|(\theta(x) - 1)/(\theta(1) - 1) \) is an algebraic integer.

(Remark. In fact, if \( \alpha \neq \beta \), there are \( |G : C_G(x)|(m - \theta(x))/m(m - 1) \) conjugates of \( x \) mapping \( \alpha \) to \( \beta \). This follows from an easy counting argument.)

10. Initial reductions. Let \( G \) be a Chevalley group and \( G < G^* < Aut(G) \). Suppose \( G^* \) has a faithful 2-transitive permutation representation on a finite set \( \Omega \),
and let \( \alpha \in \Omega \). Set \( m = |\Omega| \). Let \( \theta^* \) be the permutation character of \( G^* \) on \( \Omega \), so \( \theta^*(1) = m \). Set \( \theta = \theta^*|G \). Let \( W, R, n \) and \( p \) be as in \( \S 2 \).

If \( g \in G^* \), let \( \Omega(g) \) denote its set of fixed points. Recall that a subgroup of \( G^* \) is semiregular if only the identity fixes a point.

Clearly, \( G \) is transitive on \( \Omega \), so \( |G:G_\alpha| = m \).

(10.1) Lemma. \( G_\alpha \) is maximal in \( G \).

Proof. [40, 10.4 or 12.3].

(10.2) Lemma. If \( n = 1 \), the Main Theorem holds.

Proof. First suppose that \( (\theta, 1_B^G) > 1 \). Since \( \chi = \theta^* - 1_G^* \) is irreducible, by Clifford's theorem \( \chi|G \) is the sum of irreducible characters of the same degree. But \( (\chi|G, 1_B^G) = 0 \), so \( p|\chi(1) \). Thus, \( p \nmid m \), so \( G^* \) contains a Sylow \( p \)-subgroup of \( G^* \).

By (2.3) and (10.1), \( G^* \) is a Borel subgroup of \( G^* \).

Suppose next that \( (\theta, 1_B^G) = 1 \), so \( G = G_\alpha B \). From the lists of maximal subgroups in [6], [20], [26], [37], [38], [39], it is straightforward to check that the only possibilities are those listed in the Main Theorem.

From now on we will assume \( n \geq 2 \).

(10.3) Lemma. Let \( G^+ \) and \( B^+ \) be as in (2.6). If \( B^+ \) is transitive on \( \Omega \), then \( G \) is as in cases (vii) or (viii) of the Main Theorem.

Proof. If \( B^+ \) is transitive then \( G^+ = B^+(G^+) \). From (2.10) it then follows that \( G \) is as in the Main Theorem.

From now on we will assume that \( B^+ \) is intransitive.

(10.4) Lemma. \( m \) is not a power of \( p \).

Proof. Otherwise, as \( G \) is transitive, \( G = G_\alpha U \). Thus, \( U \) is transitive, whereas we are assuming \( B^+ \) to be intransitive.

(10.5) Lemma. \( \theta \) is a constituent of \( 1_B^G \), \( (\theta, \theta) \) divides \( 6 \), each irreducible constituent of \( \theta \) is \( G^+ \)-invariant, and \( G^* \) acts transitively on the nonprincipal irreducible constituents of \( \theta \).

Proof. By (2.6), \( |G^*:G^+| \mid 6 \). Set \( \chi = \theta^* - 1_G^* \) and \( \chi|G^+ = \xi_1 + \cdots + \xi_k \) with the \( \xi_i \) irreducible. Then \( k \mid 6 \) and the \( \xi_i \) are conjugate characters under the action of \( G^* = G^+ N(B^+) \) (by the Frattini argument). Since \( B^+ \) is intransitive, some and, hence, all \( \xi_i \)'s are constituents of \( 1_B^{G^+} \). By (2.9), each \( \xi_i \) remains irreducible when restricted to \( G \).

It remains to show that \( \theta \) is multiplicity-free. Since each \( \xi_i|G \) occurs with the same multiplicity \( e \), and since \( \theta(g) = 0 \) for some \( g \in G \), we must have \( \Sigma \xi_i(g) = -1/e \). Thus, \( e = 1 \).

(10.6) Lemma. If \( p \nmid m \), then \( G = A_n(q), G_\alpha \) is conjugate to \( G_1 \) or \( G_n \), and the Main Theorem holds.
Proof. Suppose $p \nmid m$. Then we may assume that $U \leq G_\alpha$. By (2.3) and (10.1), $G_\alpha$ is a maximal parabolic subgroup. Suppose $\theta - 1_G$ is irreducible. Then there are just two $(G_\alpha, G_\alpha)$-double cosets. Thus, $G$ is $A_n(q)$ and $G_\alpha = G_1$ or $G_n$.

Suppose that $G^* > G^+$. By the Frattini argument, $G^* = GN(B)$, so there is an element $x \in G^* - G^+$ such that $x$ normalizes $B$. However, since $G$ is transitive, $G^* = GG_\alpha = GN(G_\alpha)$, so we can find $y \in G$ with $xy \in N(G_\alpha)$. Since $G_\alpha = G_\alpha^x \supseteq B^y$, $y \in G_\alpha$ and $x \in N(G_\alpha)$. This is impossible as the graph automorphism of $G$ interchanges $G_1$ and $G_n$. Consequently $G^* = G^+$ and we are in case (i) of the Main Theorem.

Now suppose $\theta - 1_G$ is reducible. By (10.5), $G^* > G^+$ and there are 3, 4 or 7 $(G_\alpha, G_\alpha)$-double cosets; here, 4 or 7 can occur only for $G = D_4(q)$. Moreover $G^*/G^+$ induces a group of graph automorphisms of the Dynkin diagram. As in the previous paragraph we argue that $G_\alpha$ is a maximal parabolic subgroup, fixed by a nontrivial graph automorphism, for which there are 3, 4, or 7 double cosets. By (5.4), $\rho \in \theta$. Since all irreducible constituents of $\theta - 1_G$ are conjugate in $G^*$, by (5.4) each appears in $1_G^P$ for each maximal parabolic subgroup $P$ of $G$. Consequently, $G \nleq A_n(q)$.

If $G = E_6(q)$ or $D_6(q)$, we can choose $P$ so that $1_G^P - 1_G - \rho$ is irreducible. Consequently, $\theta = 1_G^P$ for such a $P$. But it is easy to check (using Tables 3 and 4) that $p(1) \neq 1_G^P(1) - 1 - p(1)$. This completes the proof of (10.6).

From now on we will assume that $p|m$.

Lemma. $p$ does not divide the degree of any irreducible constituent of $\theta - 1_G$, where $\theta - 1_G \subseteq 1_B^G$.

Proof. This is clear since $p|m$.

(10.8) Corollary. $G \nleq A_n(q)$.

Proof. (10.7) and (5.9).

(10.9) Corollary. If $n \geq 3$, then $q = p$ is prime, where $q$ is related to $G$ as in (5.1). If $n = 2$, then $G = Sp(4, 2)$, $G_2(2)$, $G_2(3)$, or $2F_4(2)$.

Proof. (5.6), (5.7)(i), and (10.7).

(10.10) Lemma. Assume $G$ is not $Sp(2n, 2)$, $F_4(2)$, $G_2(2)$, $G_2(3)$, or $2F_4(2)$.

(i) If $G$ is a classical group, $G_{12}$ is transitive on $\Omega$. In particular, $G_1$ and $G_2$ are transitive.

(ii) If $G$ is an exceptional group, $G_i$ is transitive (where $i$ is as in (4.2) and Table 4).

Proof. (10.5), (10.7), (5.7), and (5.8) show that $(\theta, 1_G^{G_{12}}) = 1$ for (i) and $(\theta, 1_G^{G_i}) = 1$ for (ii).

(10.11) Lemma. Let $G$ be as in (10.10). Let $U_r$ and $U_s$ be as in (3.1)–(3.3) or (4.4)–(4.6).

(i) If $G$ is $PSp(2n, q)$ or $PSU(l, q)$, then $Z(U_r)$ and $U_s$ are semiregular on $\Omega$.

(ii) If $G$ is $PSO^*(l, q)$, then $U_r$ is semiregular on $\Omega$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(iii) If \( G \) is exceptional, then \( U_r \) is semiregular on \( \Omega \).

**Proof.** Let \( X \) be any of the groups claimed to be semiregular. For \( 1 \neq x \in X \), we will show that \( C(x) \) is transitive on \( \Omega \). Once this is known, since \( C(x) \) acts on \( \Omega(x) \) we will have \( \Omega(x) = \varnothing \) or \( \Omega \), so since \( G^* \) is faithful on \( \Omega \) the desired semiregularity will follow.

We must thus show that \( (0, \varnothing) \) = 1. Suppose \( G \) is exceptional. By (4.4)–(4.6), \( N(U_r) = G_i \) and \( G_i = C_G(x)H \). For \( w \in W \), \( G_i w B = C_G(x) H w B = C_G(x) w B \), so there are equally many \( (G_i, B) \) and \((C_G(x), B)\)-double cosets. Then \( (1_{C_G(x)}, 1_B) = (1_{G_i}, 1_B) \), so (10.5) and (10.10)(i) imply that \( (1_{C(x)}, \theta) = 1 \).

Next suppose that \( G = \text{PSp}(2n, q) \) (with \( q \neq 2 \)), \( \text{PSU}(l, q) \), or \( \text{PSO}^+(l, q) \), and that \( X = U_r \). In the first two cases, let \( i = 1 \), and in the last, let \( i = 2 \). Then, by (3.1)–(3.3), \( G_i = N(X) = C(x)H \). Since \( G_i \) is transitive by (10.10), as above, so is \( C(x) \).

Finally, suppose \( G = \text{PSp}(2n, q) \) (with \( q \neq 2 \)) or \( \text{PSU}(l, q) \), and that \( X = U_s \).

By (3.9), each irreducible character common to \( 1_{B} \) and \( 1_{C(x)} \) is contained in \( 1_{C(x)} \). Thus, by (10.5) and (10.10), no irreducible constituent of \( \theta - 1_G \) is a constituent of \( 1_{C(x)} \), so that \( (1_{C(x)}, \theta) = 1 \) again.

(10.12) **Lemma.** Assume that the conclusions of (10.10) hold. Define \( i \) as follows: if \( G \) is exceptional, \( i \) is as in (4.2); if \( G \) is orthogonal, let \( i = 2 \); and if \( G \) is symplectic or unitary, let \( i = 1 \). Then \( m - 1 \mid |G : G_i(q - 1)| \).

**Proof.** Set \( X = Z(U_r) \). Then, by (3.1)–(3.3) and (4.4)–(4.6), \( |X| = q = p \), \( G_i = N(X) \), and \( G_i = N(X)H \). Since \( H \) is an abelian group acting irreducibly on \( X \), it induces a fixed-point-free group of automorphisms of \( X \). Thus, \( |G_i : C(X)| q - 1 \), so \( |G : C(X)| |G : G_i(q - 1)| \). The result now follows from (9.2) and the conclusions of (10.11).

(10.13) **Lemma.** Assume that the conclusion of (10.12) holds for \( G \), and that \( n \geq 3 \). Then \( q^k \nmid m \), where \( k \) is as follows.

(i) \( k = 2n - 1 \) if \( G = \text{Sp}(2n, q) \).

(ii) \( k = 2n - 1 \) if \( G = \text{PSO}(2n + 1, q) \) with \( q \) odd.

(iii) \( k = 2l - 2 \) if \( G = \text{PSO}^+(2l, q) \).

(iv) \( k = 2l - 3 \) if \( G = \text{PSU}(l, q) \).

(v) \( k = 7 \) if \( G = E_6(q) \).

(vi) \( k = 9 \) if \( G = E_{6}(q) \).

(vii) \( k = 11 \) if \( G = E_8(q) \).

(viii) \( k = 17 \) if \( G = E_{7}(q) \).

(ix) \( k = 29 \) if \( G = E_8(q) \).

**Remark.** The powers listed in (10.13) are not intended to be the best possible. They merely provide a goal in the following sections: in §§11, 12 we show that \( q^k \mid m \).

**Proof.** Since the proofs in the various cases all follow the same pattern, we will only give samples of the method, including the hardest situations. Suppose \( q^k \mid m \),
and write \( m = q^k x \). By (10.12) we can write \((m - 1) y = |G : G_i| (q - 1)\) with \( y \in \mathbb{Z} \). Thus, \((q^k x - 1) y = |G : G_i| (q - 1)\). Using the indices \(|G : G_i|\) as given in Tables 3 and 4, together with elementary number theory, we will obtain a contradiction. We illustrate with the three cases \( G = F_4(q) \), \( E_6(q) \), and \( PSp^+(2l, q) \).

1. \( G = F_4(q) \). Here \((q^7 x - 1) y = (q^4 + 1)(q^{12} - 1)\). Taking congruences mod \( q^7 \), we find that \( y = q^7 z + q^4 + 1 \) with \( 0 \leq z \in \mathbb{Z} \). Then
\[
(q^7 x - 1)(q^7 z + q^4 + 1) = (q^4 + 1)(q^{12} - 1).
\]
By (10.4), \( x \) is not a power of \( p \); thus \( z \neq 0 \) and \( x \neq q^3 \). Then \( x < q^3 \), as otherwise \((q^7 x - 1)(q^4 + 1) < (q^4 + 1)q^{12} \), which is impossible.

Since \( q^7 x - 1 \) and \((q^4 + 1)(q^{12} - 1)x \) implies that \( q^7 x - 1 (q^4 + 1)(q^5 - x) \), we can write \((q^4 + 1)(q^5 - x) = (q^7 x - 1) y \) with \( y \in \mathbb{Z} \). Rewrite this \( v + q^5 = (q^4 + 1)x + q^7 (x^2 - q^2) \). If \( x > q^2 \), then \( v + q^5 > (q^4 + 1)x + q^7 > q^7 \), so \( v > q^5 \) and \((q^4 + 1)(q^7 - x) > (q^7 x - 1)q^5 \), which is impossible. Also, since \( x \) is not a power of \( p \), \( xv \neq q^2 \), and hence
\[
(q^4 + 1)q^3 > (q^4 + 1)x = v + q^5 + q^7 (q^2 - xv) > q^5 + q^7,
\]
which is again impossible.

2. \( G = E_6(q) \). Here
\[
(q^{29} x - 1) y = (q^{10} + 1)(q^{24} - 1)(q^{30} - 1)/(q^6 - 1).
\]
Taking congruences mod \( q^{29} \), we can rewrite this
\[
(10.14) (q^{29} x - 1)(q^{29} z + (q^{10} + 1)(q^{24} - 1) - q^{34}) = (q^{10} + 1)(q^{24} - 1)(q^{30} - 1),
\]
where \( z \in \mathbb{Z} \). We first show that \( z > 0 \). For otherwise, \( z = 0 \) and
\[
q^{24} - q^{10} - 1 \equiv (q^{10} + 1)(q^{24} - 1)(q^{30} - 1).
\]
However, \( q^{24} - q^{10} - 1 \) is relatively prime to \( q^{10} + 1 \) and \( q^{24} - 1 \), so \( 1 \equiv q^{30} \equiv q^6 (q^{10} + 1) \) (mod \( q^{24} - q^{10} - 1 \)), which is clearly false. Thus, \( z \geq 1 \), and (10.14) yields \( z q^{10} \). Multiplying the right side of (10.14) by \(-q^5 x^2\) and taking congruences mod \( q^{29} x - 1 \), we find that \( q^{29} x - 1 (q^{10} + 1)(1 + q^5 x)(q - x) \). Then \( x > q \) (since \( x \neq q \) by (10.4)), and hence \( q^{29} x - 1 \leq (q^{10} + 1)q^5 x^2 - 1 \). It follows that \( q^{29} \leq (q^{10} + 1)q^5 x \leq (q^{10} + 1)q^{15} \), which is impossible.

3. \( G = PSp^+(2l, q) \). Here
\[
(q^{2l-2} x - 1) y = (q^l \pm 1)(q^{l-1} \pm 1)(q^{l-1} x + 1)(q^{l-2} - 1)/ (q^2 - 1).\]
Taking congruences mod \( q^{2l-2} \), we find that \( y(q^2 - 1) = q^{2l-2} z \neq q^l \pm q^{l-2} - 1 \) with \( z \in \mathbb{Z} \). Then \( z \equiv 1 \) (mod \( q^2 - 1 \)), so that \( z \geq 1 \). By (10.4), \( x > 1 \). Thus,
\[
(q^{2l-2} x - 1)(q^{2l-2} z \neq q^l \pm q^{l-2} - 1) \leq (q^{2l-2} - 1)(q^l \pm 1)(q^{l-2} x \neq 1),
\]
which is impossible.

11. The classical groups. The proof of the Main Theorem will be completed in \$\S\S 11–13. In this section we assume that \( G \) is a classical group and \( W \) has rank \( \geq 3 \). Frequent use will be made of \$3. Recall that \( q \) is a prime by (10.9).
(11.1) Lemma. \( G \neq \text{PSp}(2n, q), q > 2. \)

**Proof.** Suppose \( G = \text{PSp}(2n, q) \) with \( q \) an odd prime. Then (3.2) implies that \( Z(Q_1) = U_1 \) has order \( q \), and \( Q_1 \) is an extraspecial group of order \( q^{2n-1} \). \( L_1 \approx \text{Sp}(2n-2, q) \) acts on \( Q_1/U_1 \) as described in (3.2).

By (10.11), \( U_r \) and \( U_r' \) are semiregular in \( \Omega \). Again by (3.2), \( U_rU_r'/U_r \) corresponds to an isotropic 1-space of \( Q_1/U_1 \), all elements of each nontrivial coset of \( U_r \) in \( Q_1 \) are conjugate in \( Q_1 \), and \( L_1 \) is transitive on these cosets. Thus, all elements in \( Q_1 - U_r \) are conjugate, so \( Q_1 \) is semiregular on \( \Omega \). Then \( q^{2n-1} \mid m \), contradicting (10.13).

(11.2) Lemma. \( G \neq \text{PSO}^\pm(l, q). \)

**Proof.** Suppose \( G = \text{PSO}^\pm(l, q) \). By (11.1), \( q \) is odd if \( l \) is odd. \( L_1 = \text{SO}^\pm(l-2, q)' \) acts on the elementary abelian group \( Q_1 \) of order \( ℓ^l/2 \) in the natural manner as a group of \( F_q \)-transformations preserving a quadratic form, and \( U_r \) corresponds to an isotropic (or singular, if \( q \) is even) 1-space. Thus, by (10.11), isotropic (or singular) 1-spaces of \( Q_1 \) are semiregular.

By (10.13), \( q^{-l/2} \nmid m \), so \( Q_1 \) is not semiregular. Then \( (Q_1)_α \) is a nontrivial subspace of \( Q_1 \); moreover, it must be anisotropic (or nonsingular). Consequently, \( |(Q_1)_α| \leq q^2 \) for each \( α \), so \( q^{-l/4} \) divides the length of each orbit of \( Q_1 \).

Let \( v \neq 1 \) be any element of \( Q_1 \) whose set \( Ω(v) \) of fixed points is nonempty. Since \( Q_1 \) acts on \( Ω(v) \), \( q^{-l/4} \mid |Ω(v)| \). Since \( v \in Q_1 \) is an anisotropic (or nonsingular) vector, \( |L_1 : C_{L_1}(v)| \) is divisible by \( q^{(l-3)/2} \) or \( q^{(l-4)/2} \), depending on whether \( l \) is odd or even. Thus, in (9.1) (applied to \( P = G_1 \), which is transitive by (10.10)), each summand is divisible by \( q^{-l/4}q^{(l-3)/2} \) or \( q^{-l/4}q^{(l-4)/2} \), so that one of these powers of \( q \) divides \( m \). Since we may assume that \( l \geq 7 \), it follows that \( q^{l/2} \mid m \). This contradicts (10.13).

(11.3) Lemma. \( G \neq \text{PSU}(l, q). \)

**Proof.** Suppose \( G = \text{PSU}(l, q) \). Here \( Q_1 \) is extraspecial of order \( q^{2l-3} \), \( Z(Q_1) = Z(U_1), \) and \( L_1 \approx \text{SU}(l-2, q) \) acts on \( Q_1/Z(Q_1) \) as a group of \( F_q \)-transformations preserving a nondegenerate hermitian form (see (3.3)). Also, \( U_rZ(U_r)/Z(U_r) \) is an isotropic 1-space, and all elements of \( U_rZ(U_r) - Z(U_r) \) are conjugate in \( L_1Q_1 \).

By (10.11), \( Z(U_1) \) and \( U_1 \) are semiregular, but by (10.13), \( Q_1 \) is not semiregular. Take \( 1 \neq g \in Q_1 \) with a nonempty set \( Ω(g) \) of fixed points. Then \( g \notin Z(Q_1) \). There is an extraspecial subgroup \( T \) of \( C_{Q_1}(g) \) of order \( q^{2l-5} \). Since \( Z(T) = Z(Q_1) \) is semiregular, for each \( α \in Ω(g) \) we have \( T_α \cap Z(T) = 1 \). Then \( T_α \) is abelian, so \( |T_α| \leq q^{l-3} \). Consequently, \( q^{l-2} \mid |Ω(g)| \). Also, \( gZ(Q_1)_α \) is an anisotropic vector of the \( F_q \)-space \( Q_1/Z(Q_1) \), so the number of conjugates of \( gZ(Q_1) \) under \( L_1 \) is also divisible by \( q^{l/2} \). Then \( q^{-l/2} \mid |L_1 : C_{L_1}(g)| \). By (9.1) (applied to \( P = G_1 \), which is transitive by (10.10)), \( q^{-l/2} |q|^{l/2} \mid m \). This contradicts (10.13).

12. The exceptional groups. We again recall that \( q \) is prime.

(12.1) Lemma. \( G \) is not \( E_6(q), E_7(q), \) or \( E_8(q) \).

**Proof.** Suppose \( G = E_6(q), E_7(q), \) or \( E_8(q) \). All root subgroups are conjugate
to $U_r$, and hence are semiregular by (10.11). By (10.10), $G_i$ is transitive on $\Omega$, where $i = 2, 1, \text{ or } 8$, respectively. Consequently, for all $a \in \Omega$, $(Q_i)_a$ contains no nontrivial element of a root group.

By (4.4), $Q_i$ is extraspecial of order $q^{21}, q^{33}, \text{ or } q^{57}$, respectively. Since $(Q_i)_a \cap Z(Q_i) = 1$, it follows that $(Q_i)_a$ is abelian, and hence (from the theory of extraspecial groups) that $|J(Q_i)_a| \leq \sqrt{|Q_i|}/q$. Then $|Q_i| : |(Q_i)_a|$ is divisible by $q^{11}, q^{17}$, or $q^{29}$, respectively. Since $a$ is arbitrary, $q^{11}, q^{17}$, or $q^{29}$ divides $m$. This contradicts (10.13).

(12.2) **Lemma.** $G \neq F_4(q), q > 2$.

**Proof.** Suppose $G = F_4(q), q > 2$. By (10.7) and (5.6), $q = 3$.

By (4.5), $G_4$ has a normal subgroup $R_4$ such that $R_4$ is elementary abelian of order $3^7$, and $L_4 \approx SO(7, 3)'$ acts on $R_4$ preserving a nondegenerate quadratic form. Moreover, the isotropic 1-spaces in $R_4$ are all conjugates of $U_r$, where $r$ is the root of maximal height. Since $U_r$ is semiregular on $\Omega$ by (10.11), all nontrivial isotropic vectors in $R_4$ are semiregular. $R_4$ is not semiregular, as otherwise $3^7 \mid m$, contradicting (10.13). We will apply the formula in (9.1) to $P = G_4$.

Let $v$ be a nonisotropic vector in $R_4$. The centralizer in $L_4$ of $v$ stabilizes $\langle v \rangle$ and $\langle v \rangle$, so that $C_{L_4}(v) \approx O^+(6, 3)$, and consequently $R_4$ contains $3^3 z$ conjugates of $v$ under the action of $L_4$, where $z \in \mathbb{Z}$. Clearly, $R_4$ centralizes $v$ and acts on $\Omega(0)$. If $v$ fixes $a$, then $(R_4)_a$ contains no nonzero isotropic vector, so $|(R_4)_a| \leq 3^2$. Thus, $3^3 \mid |\Omega(0)|$. Now (9.1) implies that $3^3 \cdot 3^5 \mid m$, contradicting (10.13).

(12.3) **Lemma.** $G \neq 2E_6(q)$.

**Proof.** Suppose $G = 2E_6(q)$. Since $q$ is prime, by (4.6) $Q_1$ is extraspecial of order $q^{21}$ with center $U_r$. Also, by (10.11), $U_r$ is semiregular on $\Omega$. Thus, for each $a \in \Omega$, $(Q_1)_a$ is abelian, and consequently $|(Q_1)_a| \leq q^{10}$. Then $q^{11} \mid m$, contradicting (10.13).

13. Completion of the proof. At this point, we have proved the Main Theorem, except when $n = 2$ or $G$ is $G_2(3), F_4(2)$ or $Sp(2n, 2)$. These cases will be completed in this section. (At the end of this section we will also handle the Tits group $2F_4(2)'$.)

(13.1) **Lemma.** If $n = 2$, then $G = Sp(4, 2)$ or $G_2(2)$, and the Main Theorem holds for these cases.

**Proof.** The case $G = Sp(4, 2) \approx S_6$ is clear. Since $G_2(2)' \approx PSU(3, 3)$ the case $G = G_2(2)$ has been handled in (10.2). Suppose $n = 2$ but $G \neq Sp(4, 2), G_2(2)$. By (10.9), $G = G_2(3)$ or $2F_4(2)$.

If $G = G_2(3)$, by (7.26) we know that the degrees of the 6 irreducible constituents of $1^G_6$ are $1, 3^6, 91, 91, 104$ and 168. Since $\theta - 1_G$ decomposes into 1 or 2 irreducible constituents of $1^G_6$ of the same degree not divisible by $q = 3$, we must have $m - 1 = \theta(1) - 1 = 91, 104, \text{ or } 2 \cdot 91$. Then $m \mid |G_2(3)|$, which is a contradiction.

Similarly, if $G = 2F_4(2), (7.26)$ and (10.7) imply that $m - 1 = 3^3 \cdot 5^2 \text{ or } 3^3 \cdot 13$, and again $m \mid |2F_4(2)|$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(13.2) Lemma. $G \neq F_4(2)$.

Proof. Define $f_1(t)$ as in (7.19), so $9 \leq \deg f_1 \leq 15$. As usual, let $\rho$ be the reflection character of $G$. Then by Table 4, $\rho(1) + 1 \nmid |F_4(2)|$. If $1_{G^\alpha} = 1 + \xi_1 + \xi_2$ with $\xi_1, \xi_2$ conjugate characters, then $m = |G : G_\alpha|$ is odd, whereas $\rho m$ by §10. Thus, $\theta - 1_G$ is irreducible, and from (7.19) it follows that $\theta = 1_G + \chi$ where $\chi(1) = f_1(2)$. By (7.19), $f_1(t) = \frac{1}{2} f_1^*(t)$, where $3 \leq \deg f_1^* \leq 15$ and (by (5.5))

$$f_1^*(t)(t + 1)^2(t^2 + 1)^2(t^2 + t + 1)^2(t^2 - t + 1)^2(t^4 - t^2 + 1).$$

First consider the case $f_1(1) = 9$. Then $(t^2 + t + 1)^2 f_1^*(t)$. Also, $f_1^*(t)$ is divisible by precisely one of $t + 1, t^2 + 1, t^4 + 1$. Using this information, together with (13.3) and the restriction on $\deg f_1^*$, it is easy to write down all the possibilities for $f_1(t)$. In each case, we find that $\chi(1) + 1 \nmid |F_4(2)|$.

Thus, $f_1(1) \neq 9$. By Table 4, $f_1(1) = 2$ or 8. By (4.3)(i) and (5.2), $\chi$ is not contained in both $1_{G^\alpha}$ and $1_{G_4}$, so that $G_1$ or $G_4$ is transitive on $\Omega$. Since $q = 2$, by (4.5) both $G_1$ and $G_4$ have central involutions. Thus, as in (10.11) we find that $f_1^*(2) = m - 1$, which divides $|G : G_1| = |G : G_4| = 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17$. As $3 \nmid f_1(1), t^2 + t + 1 \nmid f_1^*(t)$, and hence $7 \nmid f_1^*(2)$. Also, $f_1(1) = 2$ or 8 implies that $f_1^*(t)$ is divisible by at least two of $t + 1, t^2 + 1, t^4 + 1$. In view of (13.3) and $\deg f_1^* \geq 8$, it is now easy to write down the possibilities for $f_1^*(2)$ and check that $f_1^*(2) + 1 = f_1^*(2) + 1 \nmid |F_4(2)|$ except when $f_1^*(t) = (t^2 - t + 1)(t^4 - 1)$. But in the latter case, $m = f_1(2) + 1 = 256$, and this contradicts (10.4).

(13.4) Lemma. If $G$ is $Sp(2n, 2)$, then $G_\alpha$ is $GO^\pm(2n, 2)$.

Proof. We may assume $n \geq 3$. By the proof of (11.1), $\theta(x) \neq 0$ for $1 \neq x \in U_r$. By the proof of (10.11), $G_1$ is intransitive, so that as in (10.10) we must have $\theta, 1_{G_1} > 1$. Since $\theta - 1_G$ is irreducible, $\theta \in 1_{G_1}^G$.

Consequently, $\theta$ is precisely the permutation character of $G$ in its permutation representation on the cosets of $GO^\pm(2n, 2)$. There are $(2^{2n} - 1)\theta(x)\theta(1)$ transvections in $G_\alpha$; just count the pairs $(x, \alpha)$ with $x$ a transvection in $G_\alpha$. Since this is also true of the representation of $G$ on the cosets of $GO^\pm(2n, 2)$, $G_\alpha$ contains $2^{n-1}(2^n - 1)$ transvections.

Regard $G$ as acting as usual on a $2n$-dimensional vector space $V$. The subgroup $X$ of $G_\alpha$ generated by its transvections is irreducible. For suppose $M$ is an $X$-invariant $e$-space of $V$ with $1 \leq e \leq 2n - 1$. If $1 < e < 2n - 1$, $M$ is fixed by at most $2^e - 1 + 2^{2n - e} - 1$ transvections. We may thus assume that $e = 1$ and $G_\alpha$ fixes $M$. Then $|G_\alpha| \leq |G_1|$, which is not the case.

From [25] it follows that $G_\alpha$ is contained in an orthogonal group, so the maximality of $G_\alpha$ yields the lemma.

Remark. In fact, only Lemmas 2.3, 2.6, and 4.1 of [25] are needed in our situation.

This completes the proof of the Main Theorem.

(13.5) Theorem. The Tits group $\tilde{F}_4(2)$ has no faithful 2-transitive permutation representation.
2-TRANSITIVE PERMUTATION REPRESENTATIONS

Proof. Let \( G = \Gamma F_4(2) \), and suppose that \( G' \) has such a representation on a set \( \Omega \). Let \( \alpha \in \Omega \). Then \( 1^G_\alpha \) is the permutation character, so that \( 1^G_\alpha = 1_G + \lambda + \chi \) or \( 1_G + \lambda + \chi + \chi' \), where \( \lambda \) is the nonprincipal linear character of \( G \) and \( \chi \) (and \( \chi' \)) are nonlinear irreducible characters of \( G \) having the same degree.

As \( G = G'B = G'U \), \( (\lambda, 1^G_B) = 0 \), while \( (1^G_\alpha, 1^G_B) > 1 \) by (2.10). We may assume that \( \chi \) is a constituent of \( 1^G_B \). Clearly \( 2|\Omega| = 2 + \chi(1) \) or \( 2 + 2\chi(1) \) must divide \( |G| \).

By (7.26), \( \chi(1) = 2 \cdot 3 \cdot 13 \), \(|\Omega| = 40 \), and \( 1^G_\alpha = 1_G + \lambda + \chi \). Let \( \Omega^* \) be the set of right cosets of \( G_\alpha \) in \( G \).

In the notation of [12], \( \chi = d_{\sigma_2}(2) \). In particular, \( \chi \) appears with multiplicity 1 in one maximal parabolic subgroup of \( G \) and does not appear in the other (see the proof of (7.26)). Thus, either \( G_1 \) or \( G_2 \) is transitive on \( \Omega \). Choose the notation so that \( G_1 \) is transitive. Then \( 5| \Omega | \).

The structure of \( G_1 \) is determined in [17, §10]. (Note that the correspondence between our notation and that of [17] is: \( G_1 = P_2 \), \( L_1 = R_2 \).) According to [17, (10.1)], \( L_1 \) is the holomorph of \( Z_5 \). We know that \( G_1 = Q_1 L_1 \) is transitive on \( \Omega \), where \( |\Omega|^* = 80 \), so a Sylow 5-subgroup of \( G_1 \) must be semiregular on \( \Omega^* \). On the other hand, \( |G : G_1^a| = 80 \) implies that \( 5| |G_1^a| \), so some element of \( G' \) of order 5 fixes \( \alpha \). This will be a contradiction if we can show that all elements of \( G \) of order 5 are conjugate.

From [17, (10.2)], it follows that \( [L_1, L_1^{s_1 s_2 s_1}] = 1 \), where \( L_1 \cap L_1^{s_1 s_2 s_1} = 1 \). Set \( M = (L_1, x L_1^{s_1}) \). Then \( |M| = 5^2 \cdot 2^5 \), and \( M \) has a normal self-centralizing Sylow 5-subgroup \( F \). We will show that \( N_G(F) \) acts transitively on the nontrivial elements of \( F \).

First consider \( C_G(F) \), and suppose it has even order. Then the subgroup \( U_2^{s_1 s_2 s_1} \) of \( N_G(F) \) centralizes some involution \( v \in C_G(F) \). According to [17, (10.3)(i)], \( U_2^{s_1 s_2 s_1} \) contains the central involution \( t \) of \( G_1 \), so that \( G_1 = C_G(t) \) is maximal in \( G \). Thus, \( v \in C(t) = G_1 \), so \( v \in C_G(F \cap G_1) = C_G(O_5(L_1)) \). However, \( C_G(O_5(L_1)) = O_5(L_1) \times U_2^{s_1 s_2 s_1} \) (this follows from [17, §10], in particular, from the paragraphs following (10.3) and (10.10)). Then \( v \in U_2^{s_1 s_2 s_1} \), whereas \( U_2^{s_1 s_2 s_1} \) is fixed-point-free on \( F \cap L_1^{s_1 s_2 s_1} \).

Thus, \( |C_G(F)| \) is odd. Since \( |GL(2, 5)| = 5 \cdot 3 \cdot 5 \), it follows that \( M \) contains a Sylow 2-subgroup of \( N_G(F) \).

Since \( |G : N_G(F)| \equiv 1 \pmod 5 \), \( |N_G(F)| = 3|M| \) or \( 13|M| \). Suppose \( |N_G(F)| = 13|M| \). Since \( 13 \nmid |GL(2, 5)| \), \( C_G(F) = F \times X \) with \( |X| = 13 \). Here \( N_G(F) \leq N_G(X) \). Applying Sylow's theorem to both \( F \) and \( X \), we find that \( |G : N_G(X)| \equiv 1 \pmod 65 \). An easy check shows this to be impossible.

Thus, \( |N_G(F)| = 3|M| \). Let \( X < N_G(F) \) with \( |X| = 3 \). Suppose \( 3| |C_G(F)| \). Then \( C_G(F) = F \times X \). With the same notation as before, \( t \in U_2^{s_1 s_2 s_1} \leq N_G(X) \) and \( |U_2^{s_1 s_2 s_1}| = 1 \) imply that \( t \in C(X) \). Then \( X < C_G(t) = G_1 \), whereas \( 3 \nmid |G_1| \).

Consequently, \( X \) is fixed-point-free on \( F \). It is now easy to see that \( N_G(F) = \langle M, X \rangle \) is transitive on the nontrivial elements of \( F \). This completes the proof of (13.5).

Added in proof. Since this research was completed, further results have been
obtained which can simplify both the proof of the Main Theorem and much of §§6–7. Howlett [44] proved that \( p \) divides the degree of each nonprincipal constituent of \( 1_B^G \), provided that \( G \) is an untwisted Chevalley group other than \( G_2(2), G_2(3), F_4(2), Sp(2n, 2), \) and \( PSO(2n + 1, 2) \). In his thesis [43], Hoefsmit obtained inductive formulas for the degrees of the irreducible constituents of \( 1_B^G \) when \( W \) has type \( A_n, B_n \) or \( D_n \) (cf. Benson and Gay [41] in the case of \( D_n \)). Presumably one can deduce precisely when \( p \) divides the degrees in \( 1_B^G - 1_G \). Finally, Benson, Grove and Surowski [42] have obtained all the degrees in \( 1_B^G \) for \( G = F_4(q) \) and \( 2E_6(q) \). It should be noted that these results—and especially those of Hoefsmit—are far from easy.

Assuming that results imply that \( p \) divides each degree in \( 1_B^G - 1_G \), except for \( G = G_2(2), G_2(3), 2F_4(2), F_4(2), Sp(2n, 2), \) and \( PSO(2n + 1, 2) \), the proof of the Main Theorem would proceed as follows. Begin with (10.1)–(10.7). Eliminate the cases \( G = G_2(3), 2F_4(2) \) and \( F_4(2) \) by checking that \( 1 + x(1) \) (and \( 1 + 2x(1) \) in the case \( G_2(3) \)) does not divide \( |G| \), whenever \( x \) is an irreducible constituent of \( 1_B^G - 1_G \) such that \( p \nmid x(1) \). Finally, handle \( Sp(2n, 2) \) as in (13.4).

REFERENCES

20. R. W. Hartley, Determination of the ternary collineation groups whose coefficients lie in the \( GF(2^m) \), Ann. of Math. 27 (1926), 140–158.

ADDED IN PROOF


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OREGON, EUGENE, OREGON 97403