TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 218, 1976

THE 2-TRANSITIVE PERMUTATION REPRESENTATIONS OF THE FINITE CHEVALLEY GROUPS

BY

CHARLES W. CURTIS, WILLIAM M. KANTOR AND GARY M. SEITZ(1)

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 $G \leqslant G^* \leqslant \mathrm{Aut}\, G$. Suppose that G^* has a faithful 2-transitive permutation representation. Then one of the following holds.*

(i) $PSL(l, q) \leqslant G^* \leqslant P\Gamma L(l, q)$, $l \geqslant 3$, *and G^* acts in one of its usual 2-transitive representations of degree* $(q^l - 1)/(q - 1)$.

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

(iii) G^* *is* $PSL(2, 4) \approx PSL(2, 5) \approx A_5$ *or* $P\Gamma L(2, 4) \approx PGL(2, 5) \approx S_5$.

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

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

(vi) G^* *is* $P\Gamma L(2, 8) \approx {}^2G_2(3)$.

Presented to the Society, January 25, 1973; received by the editors April 3, 1974.

AMS (MOS) subject classifications (1970). Primary 20B10, 20B20, 20G99.

(1)The research of the authors was supported in part by NSF grants GP 20308, 33223 and 29401X1, respectively.

(vii) G^* *is* $PSL(3, 2) \approx PSL(2, 7)$ *or* Aut $PSL(3, 2) \approx PGL(2, 7)$.

(viii) G^* *is* $PSL(4, 2) \approx A_8$ *or* Aut $PSL(4, 2) \approx S_8$.

(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* $GO^{\pm}(2n, 2)$.

(x) G^* *is* $G_2(2) \approx PSU(3, 3) \cdot$ Aut $GF(9)$ *or* Aut $G_2(2) \approx P\Gamma U(3, 3)$.

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 ≥ 3, there are at most a finite number of exceptions G to the main theorem having that Weyl group, where $G^* \geq G$ 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 ≥ 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 χ 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 $(\theta, 1_B^G) = 1$, $\chi(1)$ is divisible by the characteristic p of G, or $\theta(1)$ is a power of p. Thus, if G is a counter-example, then χ 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 $\mathbf{F}_p$ 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, $(\theta, 1_P^G) = 1$; 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 $\chi(1) \mid |G : C(U_r)|$. On the other hand, using structural properties of some parabolic subgroups, we show that $p^k \mid \theta(1)$ 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 $PSL(l, q) \leqslant G^* \leqslant P\Gamma L(l, q)$, 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 Δ 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 Δ, and defined over k, is a finite group generated by certain p-groups U_α, $\alpha \in \Delta$, 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 Δ_0 is a root system generated by some subset of a fundamental system of roots in Δ, then $G_0 = \langle U_\alpha \rangle_{\alpha \in \Delta_0}$ is a Chevalley group associated with the root system Δ_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 Δ, 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 $U \trianglelefteq B$, $B = UH$, and H is abelian. There exists a subgroup $N \trianglerighteq H$ 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 Δ. 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 $U_{-\alpha_i} = U_{-i}$, $1 \leqslant i \leqslant n$. We may assume that $s_i \in \langle U_i, U_{-i} \rangle$ for $1 \leqslant i \leqslant n$.

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

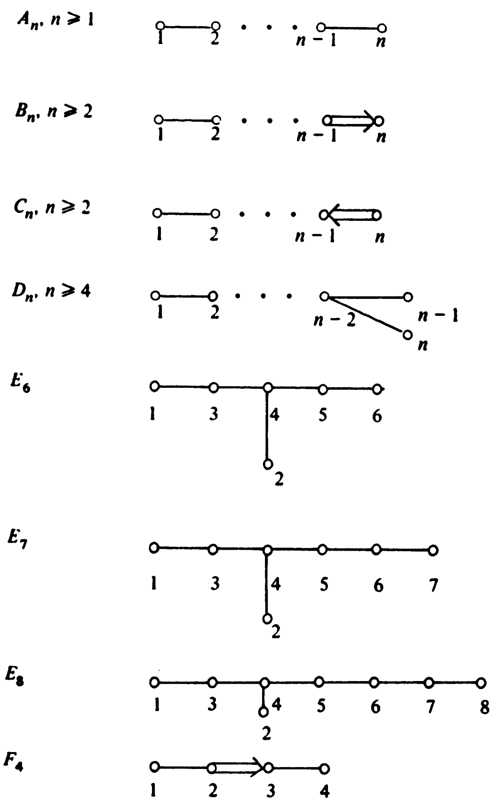

TABLE 2

Classical Group Notation	(B, N)-Notation	Type of Δ
$PSO(2n+1, q)'$	$B_n(q)$	B_n
$PSp(2n, q)$	$C_n(q)$	C_n
$PSO^+(2n, q)'$	$D_n(q)$	D_n
$PSO^-(2n, q)'$	${}^2D_n(q)$	B_{n-1}
$PSU(2n, q)$	${}^2A_{2n-1}(q)$	C_n
$PSU(2n+1, q)$	${}^2A_{2n}(q)$	BC_n

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

$W_I = \langle s_j \mid j \notin I \rangle$;

$G_I = \langle B, U_{-j} \mid j \notin I \rangle = \langle B, W_I \rangle = BW_IB$;

$L_I = \langle U_j, U_{-j} | j \notin I \rangle$; and

$Q_I = \langle U_\alpha | \alpha > 0$ and $\alpha = \Sigma m_j \alpha_j$ with $m_j > 0$ 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 α, β be independent roots. Then*

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

PROOF. [36, pp. 24, 181].

We remark that $i, j \in Z$ in (2.1) unless Δ has type BC_n, in which case $2i, 2j \in Z$. 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) $Q_I \trianglelefteq G_I$, $Q_I L_I \trianglelefteq G_I$, and $G_I = Q_I L_I H$.

(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 $Q_I \leqslant U$, 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 $U \leqslant L$ then $L \leqslant G_i$ 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 $\Delta_1 = \Delta \cap V_1$ contains a basis of V_1, and let W_1 be the Weyl group of Δ_1. Let $\alpha, \beta \in \Delta - \Delta_1$ be such that $\alpha \equiv \beta \pmod{V_1}$ 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 $(U_\alpha)^w = U_{(\alpha)w}$, so that, in particular, $\Sigma = \{U_{\alpha_i}^w | 1 \leqslant i \leqslant n, w \in W\}$. W acts on Σ by conjugation. The permutation groups (W, Δ) and (W, Σ) are isomorphic, with the isomorphism induced by the correspondence $\alpha \longleftrightarrow U_\alpha$.*

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 $G^\natural$ be the subgroup of* Aut G *generated by G together with all the diagonal and field automorphisms of G. Then $G^\natural \trianglelefteq$* Aut G, *and the index divides* 6. Aut G *is generated by $G^\natural$ and the graph automorphisms of G. If $G \leqslant G^* \leqslant$* Aut G, *then G^* has a normal subgroup $G^+ = G^\natural \cap G^*$ 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 $(1_L^T, 1_M^T)$ is the number of (L, M)-double cosets in T.*

The proof is omitted.

(2.8) LEMMA. *Let $I, J \subset \{1, \ldots, n\}$. Then $(1_{G_I}^G, 1_{G_J}^G) = (1_{W_I}^W, 1_{W_J}^W)$ 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 $G^+ \leqslant$* Aut G *be as in* (2.6). *Then $1_{B^+}^{G^+}|G = 1_B^G$, and each irreducible constituent of $1_{B^+}^{G^+}$ 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

$$(1_B^G, 1_B^G) = (1_W^W, 1_W^W) = (1_{B^+}^{G^+}, 1_{B^+}^{G^+}),$$

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 $\chi \in 1_{B^+}^{G^+}$, then G has a 2-transitive permutation representation.

(2.10) PROPOSITION. *Let G be a Chevalley group and $G^\natural$ be as in* (2.6). *Let $G \leqslant \widetilde{G} \leqslant G^\natural$, and let $\widetilde{B}$ be a Borel subgroup of $\widetilde{G}$. Suppose that $n \geqslant 2$, and $\widetilde{G}$ has a subgroup L such that $L\widetilde{B} = \widetilde{G}$. Then either $G \leqslant L$ or one of the following holds:*

(i) $G = PSL(3, 2)$ *and* $|L| = 3 \cdot 7$.

(ii) $G = P\Gamma L(3, 8)$ *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 $PSp(2n, q)$, $PSO^{\pm}(l, q)'$, and $PSU(l, q)$. We define $SO^{\pm}(l, q)$ 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 $SO^{\pm}(l, q)$ is the set of elements of $GO^{\pm}(l, q)$ 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 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, ρ is the reflection character (see (5.4)), while $\sigma = 1_{G_1}^G - 1_G - \rho$. We first state the main results; the proofs will be given later in this section.

(3.1) PROPOSITION. *Let $G = PSO^{\pm}(l, q)'$, $l \geqslant 7$.*

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

(ii) *$L_1 \approx SO^{\pm}(l-2, q)'$, 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 Δ 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 $G = PSp(2n, q)$, $n \geqslant 2$.*

(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 $Z(Q_1L_1) = U_r$ 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_1L_1.*

(iii) *$L_1 \approx Sp(2n-2, q)$, 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_sU_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) *$Q_{12} = Q_2U_1$, $Q_2 \trianglelefteq G_{12}$, $Q_2L_{12} \trianglelefteq G_2$, $Q_2L_{12} \leqslant C(U_s)$, and $G_{12} = (Q_2L_{12})U_1H = C_{G_{12}}(U_s)U_1H$.*

(3.3) PROPOSITION. *Let $G = PSU(l, q)$, $l \geqslant 4$.*

(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) *$L_1 \approx SU(l-2, q)$, and acts on $Q_1/Z(Q_1)$ as a group of $\mathbf{F}_{q^2}$-linear transformations preserving a nondegenerate hermitian form. The commutator function induces a nondegenerate alternating form on the $\mathbf{F}_q$-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 $U_sZ(Q_1)/Z(Q_1)$ is central in $U/Z(Q_1)$ and is an isotropic* 1*-space of the unitary space $Q_1/Z(Q_1)$. Here, $|U_s| = q^2$.*

(v) *$Q_{12} = Q_2U_1$, $Q_2 \trianglelefteq G_{12}$, $Q_2L_{12} \trianglelefteq G_2$, $Q_2L_{12} \leqslant C(U_s)$, and $G_{12} = (Q_2L_{12})U_1H = C_{G_{12}}(U_s)U_1H$.*

These properties will be proved, for the most part, together. The case of $PSO(2n + 1, 2^t)'$ is left to the reader. We can replace G by the corresponding linear group $G = SO^{\pm}(l, q)'$, $Sp(2n, q)$, 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 $\mathrm{rad}(V) = 0$.

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_{l-i+1} is a hyperbolic pair in V_i $(1 \leqslant i \leqslant k)$ 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 $U \trianglelefteq B$ 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 $V = V_0 \perp V_0^{\perp}$ and U acts faithfully on $V_0^{\perp}$. 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 $V_0^{\perp}$ is a nondegenerate orthogonal space of dimension less than $\dim V$. Also, U acts faithfully on $V_0^{\perp}$, 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 $B \leqslant N_G(V_0)$ and $B \leqslant N_G(V_0') = N_G(V_0)^g$. The theory of parabolic subgroups implies that $g \in \mathrm{stab}(V_0)$ 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 $B \leqslant N_G(\langle v_1 \rangle) = Y$, so that Y is a parabolic subgroup of G. Since $V = \langle v_1, v_l \rangle \perp \langle v_1, v_l \rangle^{\perp}$, Y contains a subgroup Y_0 such that Y_0 is trivial on $\langle v_1, v_l \rangle$ and induces on $\langle v_1, v_l \rangle$ the derived group of the group of isometries of $\langle v_1, v_l \rangle^{\perp}$. Let $Q = O_p(Y)$. Then since Y acts irreducibly on the space $\langle v_1 \rangle^{\perp}/\langle v_1 \rangle$, Q is trivial on this space. Also, $V/\langle v_1 \rangle^\perp$ is 1-dimensional and $\langle v_1 \rangle$ is 1-dimensional, so that $(Y/Q)'$ is trivial on these spaces and, hence, faithful on $\langle v_1 \rangle^\perp / \langle v_1 \rangle$. 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 $\langle v_1 \rangle^\perp / \langle v_1 \rangle$.

(3.4) *G symplectic.*

$$\begin{pmatrix} 1 & & & & \\ -a_2 & 1 & & & \\ \vdots & & \ddots & & 0 \\ -a_k & & & \ddots & \\ a_{k+1} & 0 & & \ddots & \\ \vdots & & & & 1 \\ a_{l-1} & & & & \\ a_l & a_{l-1} & \cdots & a_2 & 1 \end{pmatrix}.$$

(3.5) *G unitary.*

$$\begin{pmatrix} 1 & & & & \\ -\bar{a}_2 & 1 & & & \\ \vdots & & \ddots & 0 & \\ \vdots & 0 & & \ddots & \\ -\bar{a}_{l-1} & & & & 1 \\ -\bar{a}_l & a_{l-1} & \cdots & a_2 & 1 \end{pmatrix}.$$

Here $a_l + \bar{a}_l = (a_{l-1}v_2 + \cdots + a_2 v_{l-1}, a_{l-1}v_2 + \cdots + a_2 v_{l-1})$, and $\bar{a} = a^q$.

(3.6) *G orthogonal.*

$$\begin{pmatrix} 1 & & & & \\ -a_2 & 1 & & & \\ \vdots & & \ddots & 0 & \\ \vdots & & & \ddots & \\ -a_{l-1} & 0 & & & 1 \\ +a_l & a_{l-1} & \cdots & a_2 & 1 \end{pmatrix}.$$

Here $a_l = -t(a_{l-1}v_2 + \cdots + a_2 v_{l-1})$, where $t(\ )$ is the quadratic form on V.

If $g \in Q_1$ has one of the above forms, set $v_g = a_{l-1}v_2 + \cdots + a_2 v_{l-1}$. Then v_g satisfies the condition:

$$(v_l)g = a_l v_1 + v_l + v_g \quad \text{(symplectic case)},$$

$$(v_l)g = -\bar{a}_l v_1 + v_l + v_g \quad \text{(unitary case)},$$

$$(v_l)g = a_l v_1 + v_l + v_g \quad \text{(orthogonal case)}.$$

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 $g, h \in Q_1$,

$$(3.7) \qquad [g, h] = \begin{pmatrix} 1 & & & & 0 \\ 0 & \ddots & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & \ddots & 0 \\ (v_g, v_h)' & 0 & \cdots & 0 & 1 \end{pmatrix},$$

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 $V_1^\perp = V_2 \perp \cdots \perp V_{k+1}$. If $g \in Q_1$ and $y \in C_G(V_1)$, then $g^y \in Q_1$. We have

$$(v_l)y^{-1}gy = cv_1 + (v_g)y + v_l,$$

where c is the coefficient of v_1 in $(v_l)g$. In particular, $v_{y^{-1}gy} = (v_g)y$. 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 $v_g \longmapsto v_g y$, $g \in Q_1$, $y \in C_G(V_1)$. 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 $L_1 \leqslant C_G(X)$.

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 $|X_1| = q^{l-2}$, 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]:

$$B_n\colon \alpha_1 + 2\sum_{1<i} \alpha_i.$$

(3.8)
$$C_n\colon 2\sum_{i<n} \alpha_i + \alpha_n.$$

$$D_n\colon \alpha_1 + 2\sum_{1<i<n-1} \alpha_i + \alpha_{n-1} + \alpha_n.$$

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) *$G = SO^{\pm}(l, q)'$, where q is odd if l is.* Here Δ has type B_n or D_n. Define r by (3.8). By the commutator relations (2.1), $C(U_r) \geqslant \langle U^w | w \in W_2 \rangle \geqslant Q_2L_2$, so $N(U_r) \geqslant Q_2L_2H = G_2$ 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 Δ 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 $C(U_r) \geqslant \langle U^w | w \in W_1 \rangle \geqslant Q_1L_1$. 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 $\neq \pm\alpha_1$ which involves α_1 also involves α_2, $Q_2 = \langle U_\alpha | \alpha > 0, \alpha \neq \alpha_1$, and α involves α_1 or $\alpha_2 \rangle$. Thus, $Q_{12} = Q_2U_1$. Moreover, $Q_2 \lhd Q_{12}L_{12}$.

The root $s = r - \alpha_1$ is the highest short root, and is fixed by W_{12}. The commutator relations (2.1) imply $C(U_s) \geqslant \langle U_\alpha^w | \alpha > 0, \alpha \neq \alpha_1, w \in W_{12} \rangle = Q_2L_{12}$. Then $G_{12} = Q_2L_{12}U_1H = C_{G_{12}}(U_s)U_1H$. Also, $L_2 = L_{12}\langle U_1, U_{-1} \rangle$ with $[L_{12}, U_1] = [L_{12}, U_{-1}] = 1$. Since $G_2 = Q_2L_2H$, and since H normalizes L_{12}, we have $Q_2L_{12} \lhd G_2$.

The group $U_sU_r/U_r \leqslant Z(U/U_r)$. 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_sU_r/U_r is an isotropic 1-space of Q_1/U_r.

(3) $G = SU(2n + 1, q)$. This time Δ 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_s is elementary abelian of order q^2 and U_r is special of order q^3 with center of order q.

The only roots α not of length $\sqrt{2}$ for which $U_\alpha \leqslant Q_1$ are r and $r/2$ [8, pp. 252, 254]. 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 $s = r - \alpha_1$, the commutator relations (2.1) yield $[U \cap L_1, U_s] = 1$. So again we find that U_sX/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 χ be an irreducible constituent of both 1_B^G and $1_{C(x)}^G$, where $1 \neq x \in U_s$. Then χ is a constituent of $1_{G_{12}}^G$.*

PROOF. Set $T = Q_2L_{12}$. By (3.2) and (3.3), we know that $T \leqslant C(x)$, $T \trianglelefteq G_2$, and $G_{12} = TU_1H$. In particular, $\chi \in 1_T^G$. Write

$$1_T^G = (1_T^{G_2})^G = (1_{G_2} + \theta_1 + \cdots + \theta_k)^G,$$

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

$$0 < (\theta_i^G, 1_B^G) = \sum_{G_2wB} (\theta_i^{w^{-1}}, 1)_{G_2^w \cap B},$$

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

There is a double coset G_2wB for which $(\theta_i^{w^{-1}}, 1)_{G_2^w \cap B} > 0$. We can consider w to be in W. Since $s_1 \in W_2$, we may assume that every minimal expression for w as a word in the s_i's has the form $w = s_{i_1} \cdots s_{i_t}$ with $s_{i_1} \neq s_1$. Then $(\alpha_1)w$ is a positive root, so $G_2^w \cap B \geqslant U_1^wH$. Consequently,

$$0 < (\theta_i^{w^{-1}}, 1)_{G_2^w \cap B} \leqslant (\theta_i^{w^{-1}}, 1)_{U_1^wH} = (\theta_i^{w^{-1}}, 1)_{(U_1H)^w},$$

so $(\theta_i, 1)_{U_1H} > 0$. That is, $1_{U_1H} \in (\theta_i)_{U_1H}$. But T is in the kernel of θ_i, so $1_{U_1HT} \in (\theta_i)_{U_1HT}$, where $G_{12} = U_1HT$. Thus, $\theta_i \in 1_{G_{12}}^G$, 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 $U_r \leqslant Z(U)$. By [8, pp. 260, 265, 269, and 272], r is as follows.

(4.1)
$$F_4\colon r = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4,$$
$$E_6\colon r = \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6,$$
$$E_7\colon r = 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7,$$
$$E_8\colon r = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8.$$

(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) $(1_{G_i}^G, 1_{G_i}^G) = (1_{W_i}^W, 1_{W_i}^W) = 5.$

TABLE 3

G	$\|G:G_1\|$	$\|G:G_2\|$	$\rho(1)$	$\sigma(1)$
$PSO(2n+1,q)$	$\frac{q^{2n}-1}{q-1}$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$\frac{q(q^n-1)(q^{n-1}+1)}{2(q-1)}$	$\frac{q(q^n+1)(q^{n-2}-1)}{2(q-1)}$
$PSp(2n,q)$	$\frac{q^{2n}-1}{q-1}$	$\frac{(q^{2n}-1)(q^{2n-2}-1)}{(q-1)(q^2-1)}$	$\frac{q(q^n-1)(q^{n-1}+1)}{2(q-1)}$	$\frac{q(q^n+1)(q^{n-2}-1)}{2(q-1)}$
$PSO^+(2n,q)$	$\frac{(q^n-1)(q^{n-1}+1)}{q-1}$	$\frac{(q^n-1)(q^{n-1}+1)(q^{n-1}-1)(q^{n-2}+1)}{(q-1)(q^2-1)}$	$\frac{q(q^n-1)(q^{n-2}+1)}{q^2-1}$	$\frac{q^2(q^{n-1}-1)(q^{n-1}+1)}{q^2-1}$
$PSO^-(2n,q)$	$\frac{(q^n+1)(q^{n-1}-1)}{q-1}$	$\frac{(q^n+1)(q^{n-1}-1)(q^{n-1}+1)(q^{n-2}-1)}{(q-1)(q^2-1)}$	$\frac{q^2(q^{n-1}-1)(q^{n-1}+1)}{q^2-1}$	$\frac{q(q^n+1)(q^{n-2}-1)}{q^2-1}$
$PSU(2n,q)$	$\frac{(q^{2n}-1)(q^{2n-1}+1)}{q^2-1}$	$\frac{(q^{2n}-1)(q^{2n-1}+1)(q^{2n-2}-1)(q^{2n-3}+1)}{(q^2-1)(q^4-1)}$	$\frac{q^2(q^{2n}-1)(q^{2n-3}+1)}{(q+1)(q^2-1)}$	$\frac{q^3(q^{2n-1}+1)(q^{2n-2}-1)}{(q+1)(q^2-1)}$
$PSU(2n+1,q)$	$\frac{(q^{2n+1}+1)(q^{2n}-1)}{q^2-1}$	$\frac{(q^{2n+1}+1)(q^{2n}-1)(q^{2n-1}+1)(q^{2n-2}-1)}{(q^2-1)(q^4-1)}$	$\frac{q^3(q^{2n}-1)(q^{2n-1}+1)}{(q+1)(q^2-1)}$	$\frac{q^2(q^{2n+1}+1)(q^{2n-2}-1)}{(q+1)(q^2-1)}$

(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	$\lvert G:G_i \rvert$	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	$(q^4+1)\frac{q^9+1}{q^3+1}\frac{q^{12}-1}{q-1}$	1, 2, 9, 4, 8	$q^2(q^4+1)(q^6+1)\frac{q^5+1}{q+1}$
$E_6(q)$	2	$(q^4+1)\frac{q^9-1}{q-1}\frac{q^{12}-1}{q^3-1}$	1, 15, 20, 6, 30	$q(q^4+1)\frac{q^9-1}{q^3-1}$
$E_7(q)$	1	$\frac{q^{14}-1}{q-1}\frac{q^{12}-1}{q^4-1}\frac{q^{18}-1}{q^6-1}$	1, 27, 35, 7, 56	$\frac{q(q^6+1)}{q^2+1}\frac{q^{14}-1}{q^2-1}$
$E_8(q)$	8	$(q^{10}+1)\frac{q^{24}-1}{q^6-1}\frac{q^{30}-1}{q-1}$	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 $G_i = \langle U^w, H \mid w \in W_i \rangle \leqslant N_G(U_r)$. Thus, $G_i = N_G(U_r)$ by the maximality of G_i. Moreover, if $(r)w = r$, then $(U_r)^w = U_r$, 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, $\mathcal{O}_m = \{\alpha \in (r)W \mid \alpha$ has m as coefficient of $\alpha_i\}$ is either empty or an orbit of W_i. Again by [8], $\mathcal{O}_0$, $\mathcal{O}_1$, $\mathcal{O}_{-1}$, $\mathcal{O}_2$, and $\mathcal{O}_{-2}$ 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 $\widetilde{W}_i = W_i\langle w_0 \rangle$.

Since w_0 sends positive roots to negative roots and $(\alpha_i)w_0 = -\alpha_i$, w_0 fixes $\mathcal{O}_0$ and interchanges both $\mathcal{O}_1$ and $\mathcal{O}_{-1}$, and $\mathcal{O}_2$ and $\mathcal{O}_{-2}$. Consequently, W acts as a rank 3 permutation group on $\{\{\alpha, -\alpha\} \mid \alpha \in (r)W\}$, the stabilizer of $\{r, -r\}$ being $\widetilde{W}_i$. Since $1_{W_i}^{\widetilde{W}_i} = 1_{\widetilde{W}_i} + \lambda$, with λ a linear character, we have $1_{W_i}^W = 1_{\widetilde{W}_i}^W + \lambda^W$. Here, $1_{\widetilde{W}_i}^W - 1_W$ is the sum of 2 irreducible characters, so by (ii), λ^W is also the sum of 2 irreducible characters.

Let V be the natural module for the reflection representation of W, and let τ be the corresponding reflection character. Then $\alpha_1, \ldots, \alpha_n$ can be regarded as a basis for V. Set $V_i = \langle \alpha_j \mid j \neq i \rangle$. 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, τ appears in $1_{W_i}^W$ with positive multiplicity (and, hence, multiplicity 1).

If $\tau \in 1_{W_i}^W$, then $1_{\langle w_0 \rangle} \in \tau|_{\langle w_0 \rangle}$. However, if W is not of type E_6, then w_0 is -1 on V. Thus, W is of type E_6, in which case w_0 stabilizes $V_i = V_2$ and is -1 on V/V_2 [8, p. 261]. In any case, V_i is the natural module for the reflection representation of W_i, so $\widetilde{W}_i$ is irreducible on V_i. In particular, $\widetilde{W}_i$ fixes no vector of V, so $\tau \notin 1_{\widetilde{W}_i}^W$.

It follows that $\tau \in \lambda^W$, so the degrees of the irreducible constituents of λ^W are $\tau(1)$ and $|W : \widetilde{W}_i| - \tau(1)$. The degrees of the three irreducible constituents of $1_{\widetilde{W}_i}^W$ 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 $|G : G_i|$ and degree of the reflection character ρ 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 $1_{W_4}^W$ decomposes into five irreducible characters of degrees* 1, 2, 9, 4, *and* 8. *Of these, the ones also in $1_{W_1}^W$ have degrees* 1, 4, *and* 9.

(ii) *Let $G = E_6(q)$. Then $1_{W_6}^W$ is the sum of three irreducible characters of degrees* 1, 6, *and* 20, *all of which occur in $1_{W_2}^W$. 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 $1_{W_7}^W$ decomposes into four irreducible characters, of degrees* 1, 27, 7, *and* 21, *of which only the first three appear in $1_{W_1}^W$. Also, $|G : G_7| = (q^5 + 1)(q^9 + 1)(q^{14} - 1)(q - 1)^{-1}$.*

Proof. In (i), (ii), and (iii), set $j = 4$, 6, and 7, respectively. Then $(1_{W_j}^W, 1_{W_j}^W) = 5$, 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 $s = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4$. The indices $|G : G_j|$ are easy to compute.

We next claim that $(1_{W_i}^W, 1_{W_j}^W) = 3$. To prove this, we must find the number of orbits of W_j on $(r)W$. 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 $1_{W_6}^W$. To find the degrees in (iii), introduce $\widetilde{W}_j = W_j\langle w_0 \rangle$ as in the proof of (4.2). This time, $1_{\widetilde{W}_j}^W$ 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, $1_{W_1}^W$ and $1_{W_4}^W$ have in common an irreducible character of degree 9; we already know by (4.2) that they have 1_W and the reflection character in common. We will show that the third common character φ cannot have degree 2 or 8.

Suppose $\varphi(1) = 8$. Set $\widetilde{W}_4 = W_4\langle w_0 \rangle$. The proof of (4.2) shows that $(1_{\widetilde{W}_1}^W, 1_{\widetilde{W}_4}^W) = 1$. Then $W = \widetilde{W}_1 \widetilde{W}_4$. Since $\widetilde{W}_1 \cap \widetilde{W}_4$ contains $W_{14}\langle w_0 \rangle$ of order 16, $|W|$ divides $(2^5 \cdot 3)^2/2^4$, which is not the case.

Finally, suppose $\varphi(1) = 2$. Then $\varphi|W_1 - 1_{W_1}$ and $\varphi|W_4 - 1_{W_4}$ are linear. Consequently, the reflections s_1, s_2, s_3, and s_4 commute mod ker φ, 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* $G = E_6(q), E_7(q)$, *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}, *or* q^{57}, *respectively.*

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

(iii) Q_i/U_r *can be turned into an* $\mathbf{F}_q$*-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* $\mathbf{F}_q$*-linear transformations preserving this form.*

PROOF. Again let $\mathcal{O}_1$ consist of those roots with ith coefficient 1. Then $Q_i = \langle U_r, U_s | s \in \mathcal{O}_1 \rangle$ [8, pp. 260–270]. Let $s, t \in \mathcal{O}_1$. 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, $r - \alpha_i = (r)s_i \in \mathcal{O}_1$. 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 $\langle U_s, U_{r-s}\rangle = U_s U_r U_{r-s}$, 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 $C(U_r) \geqslant Q_i L_i$. Then $N(U_r) \geqslant Q_i L_i H = G_i$, 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 $\widetilde{H}$ consist of all the elements $h(\chi)$, with χ a character of the additive group generated by the roots into $\mathbf{F}_q^{\#}$. Then $\widetilde{H} \geqslant H$, and $L_i\widetilde{H}$ and $Q_i L_i \widetilde{H}$ are groups. Let $H_0 = \{h(\chi) \in \widetilde{H} | \chi(\alpha_j) = 1 \text{ for all } j \neq i\}$. Then $|H_0| = q - 1$, and H_0 centralizes L_i while acting on Q_i. Moreover, if $h(\chi) \in H_0$, then $U_s(a)^{h(\chi)} = U_s(\chi(\alpha_i)a)$ for all $s \in \mathcal{O}_1$ and $a \in \mathbf{F}_q$. Consequently, H_0 acts fixed-point-freely on Q_i/U_r.

If $0 \neq a \in \mathbf{F}_q$, 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 $\mathbf{F}_q$-space as follows: for $v \in Q_1/U_r$ of the form $v = yU_r$, $y \in Q_1$, define $av = y^{h_a}U_r$. Since L_i centralizes H_0, it acts as a group of $\mathbf{F}_q$-transformations on this vector space. Finally, U_r can be regarded as a field via the correspondence $t \longrightarrow U_r(t)$. From the commutator relations (2.1), it follows that the commutator function is a nondegenerate alternating form on the $\mathbf{F}_q$-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 *special with center* U_r, *and* S *an elementary abelian normal subgroup of* G_1 *of order* q^7; *moreover,* G_1 *acts irreducibly on* U_r, S/U_r, *and* Q_1/S.

(ii) $|Q_4| = q^{15}$, *and* $L_4 \approx SO(7, q)'$. 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_α *with* α *a long root.*

(iv) *If* q *is even, then* $U_s \trianglelefteq G_4$. 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_α *with* α *a long root.*

(v) $G_1 = N(U_r) = C(U_r)H$. *If* q *is even,* $G_4 = N(U_s) = C(U_s)H$.

(4.6) PROPOSITION. *Let* $G = {}^2E_6(q)$.

(i) Q_1 *is special of order* q^{21} *with center* U_r *of order* q. G_1 *acts irreducibly on* Q_1/U_r. *Moreover,* $G_1 = N(U_r) = C(U_r)H$.

(ii) $|Q_4| = q^{24}$, *and* $L_4 \approx SO^-(8, q)'$. 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 nondegenerate quadratic form. The isotropic* 1*-spaces (or singular, if* q *is even) are conjugates of root groups* U_α *with* α *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 Δ: the long and short roots. Here α_2 and r are long while α_3 and s are short. The action of W is determined by the following equations.

$$(4.7)\qquad \begin{aligned} &(\alpha_j)s_j = -\alpha_j \quad \text{and} \quad (\alpha_j)s_k = \alpha_j \quad \text{for } |j-k| > 1,\\ &(\alpha_2)s_1 = \alpha_1 + \alpha_2, \quad (\alpha_3)s_4 = \alpha_3 + \alpha_4,\\ &(\alpha_1)s_2 = \alpha_1 + \alpha_2, \quad (\alpha_3)s_2 = \alpha_2 + \alpha_3,\\ &(\alpha_2)s_3 = \alpha_2 + 2\alpha_3, \quad \text{and} \quad (\alpha_4)s_3 = \alpha_3 + \alpha_4. \end{aligned}$$

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 α_i. Then

$$\begin{aligned} L_1^1 = \{&\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + 2\alpha_3, \alpha_1 + 2\alpha_2 + 2\alpha_3, \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4,\\ &\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4, \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4\}, \end{aligned}$$

$$\begin{aligned} S_1^1 = \{&\alpha_1 + \alpha_2 + \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_2 + 2\alpha_3 + \alpha_4,\\ &\alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4, \alpha_1 + 2\alpha_2 + 3\alpha_3 + \alpha_4, \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4\}, \end{aligned}$$

and $Q_1 = \langle U_\alpha | \alpha \in \{r\} \cup L_1^1 \cup S_1^1 \rangle$. Moreover, $W_1 = \langle s_1, s_2, s_3 \rangle$ is transitive on both L_1^1 and S_1^1 by (2.4). It follows that root groups U_α, $U_\beta < Q_1$ are conjugate under W_1 if and only if α and β are roots of the same length.

Before proceeding further, we note the following facts.

(4.8) LEMMA. *Let* α *and* β *be positive roots in* Δ.

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

(ii) *If* α *and* β *are long, and* $\alpha + \beta$ *is a root, then* $\alpha + \beta$ *is long. Suppose* α, β, *and* $\alpha + \beta$ *are all long or all short. Then* $[U_\alpha, U_\beta] = U_{\alpha+\beta}$, $\langle U_\alpha, U_\beta \rangle$ *is special with center* $U_{\alpha+\beta}$, *and* $[g, U_\beta] = U_{\alpha+\beta}$ *whenever* $1 \neq g \in U_\alpha$.

(iii) *Suppose* α *is short,* β *is long, and* $\alpha + \beta$ *is a root. Then* $\alpha + \beta$ *is short,* $2\alpha + \beta$ *is long,* $[U_\alpha, U_\beta] \leqslant U_{\alpha+\beta}U_{2\alpha+\beta}$, *and* $[U_\alpha, U_\beta] \nleqslant U_{2\alpha+\beta}$. *Moreover,* $[U_\alpha, g] \neq 1$ *whenever* $1 \neq g \in U_\beta$.

(iv) *Suppose* α *and* β *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,* $[U_\alpha, U_\beta] = U_{\alpha+\beta}$, $\langle U_\alpha, U_\beta \rangle$ *is special with center* $U_{\alpha+\beta}$, *and* $[g, U_\beta] = U_{\alpha+\beta}$ *whenever* $1 \neq g \in U_\alpha$.

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 α_1' and α_2' are roots generating a root system of rank 2 and $m_i \in \mathbf{Z}$. Now (4.8) can be checked from the structure of the rank 2 subgroup $\langle U_{\pm\alpha_1'}, U_{\pm\alpha_2'} \rangle = T$, where $T/Z(T) \approx PSp(3, q), PSp(4, q)$, or $PSU(4, q)$.

We now return to the proof of (4.5) and (4.6). By [8, p. 272], r is the only root for which α_1 has coefficient 2. Thus, for $\alpha, \beta \in O_1 = L_1^1 \cup S_1^1$, $\alpha + \beta$ is a root if and only if $\alpha + \beta = r$. Also, $r - \alpha_1 \in L_1^1$ and $r - (\alpha_1 + \alpha_2 + \alpha_3) \in S_1^1$. Consequently, the transitivity of W_1 on L_1^1 and S_1^1 implies that $r - \alpha \in L_1^1$ if $\alpha \in L_1^1$ and $r - \alpha \in S_1^1$ if $\alpha \in S_1^1$. Now (4.8) implies that, except when $G = F_4(q)$ with q even, Q_1 is the central product of the special groups $\langle U_\alpha, U_{r-\alpha} \rangle = U_\alpha U_r U_{r-\alpha}$, $\alpha \in L_1^1 \cup S_1^1$, each having center U_r, so Q_1 is special and $Z(Q_1) = U_r$. Set $L = \langle U_\alpha | \alpha \in L_1^1 \cup \{r\} \rangle$ and $S = \langle U_\alpha | \alpha \in S_1^1 \cup \{r\} \rangle$. 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, $S \trianglelefteq G_1$. For W_1 permutes the groups U_α, $\alpha \in S_1^1$. Also, H normalizes S. Thus, we need only check that U normalizes S. Consider $U_\alpha < S$ and U_β with $\beta \in \Delta^+$. If β is short then $[U_\alpha, U_\beta] \leqslant S$ by (4.8)(ii) and (iv). If β involves α_1, we have already seen that $[U_\alpha, U_\beta] = 1$. Suppose β is long and does not involve α_1. By (4.8)(iii), $\alpha + \beta \in S_1^1$, while $2\alpha + \beta$ is a root with first coefficient 2. Then $2\alpha + \beta = r$, and hence $[U_\alpha, U_\beta] \leqslant U_{\alpha+\beta}U_{2\alpha+\beta} \leqslant S$. Thus, $S \trianglelefteq G_1$ in this case.

Since r is the root of maximal height, $U_r \leqslant Z(U)$. Moreover, W_1 fixes r and H normalizes U_r, so $C(U_r) \geqslant \langle U, W_1 \rangle = Q_1L_1$ and $N(U_r) \geqslant Q_1L_1H = G_1$. 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 $G_4 = N(U_s) = C(U_s)H$. This proves (4.5)(v) and the last part of (4.6)(i).

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

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

PROOF. Suppose that M is a proper G_1-submodule of $V = Q_1/U_r$. Let bars denote images in V. Choose $\alpha \in L_1^1 \cup S_1^1$, and suppose that $\bar{U}_\alpha \cap M \neq 1$. Since H acts irreducibly on $\bar{U}_\alpha$, $\bar{U}_\alpha \leqslant M$. Thus, $\bar{U}_\alpha \leqslant M$ 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 β, where $U_\beta \leqslant G_1$, and then $M \geqslant [\bar{U}_\alpha, U_\beta] = \bar{U}_{\alpha+\beta}$ by (4.8)(iv). We must thus have $\alpha \in L_1^1$. Then there is a short root β such that $\alpha + \beta \in S_1^1$. By (4.8)(iii), $\alpha + 2\beta = r$. Also, $U_\beta \leqslant G_1$, so by (4.8)(iii) we have $[\bar{U}_\alpha, U_\beta] \leqslant M \cap \bar{U}_{\alpha+\beta}\bar{U}_{\alpha+2\beta} = M \cap \bar{U}_{\alpha+\beta}$ 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 $\alpha, \beta \in L_1^1$, 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 $\lambda + \lambda^* \in S_1^1$, and $\lambda \longrightarrow \lambda^*$ is bijective; 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 $U_\lambda \leqslant G_1$ for all $\lambda \in L_0^1$. Take $v \neq 1$ in M, and let $\Sigma(v)$ be minimal among those subsets Σ of $L_1^1 \cup S_1^1$ such that $v \in \Pi_{\sigma\in\Sigma} \bar{U}_\sigma$. 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 α and β 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 α, 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.

$$L_2^4 = \{\alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4,$$
$$\alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4, \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4, r\},$$
$$A_1 = \{\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3, \alpha_1 + \alpha_2 + 2\alpha_3, \alpha_1 + 2\alpha_2 + 2\alpha_3\}.$$

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 α_4-coefficient 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, $|U_1| = |U_r| = q$, while $|U_4| = |U_s| = q$ if $G = F_4(q)$ and $|U_4| = |U_s| = q^2$ 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 $L_4 \approx SO(7, q)'$ 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 $\mathbf{F}_q$-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 $\mathbf{F}_q$-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 $G = F_4(q)$, with q even, in which case $\mathrm{rad}(X) = U_\alpha$, where $\alpha = \alpha_1 + \alpha_2 + \alpha_3$. In any case, the isotropic (or singular, if q is even) 1-spaces of X are the conjugates of the root groups U_α with α a long root.

Set $w = s_4s_3s_2s_3s_4$. Then

$$(4.10)\qquad \begin{aligned} (A_1)w &= \{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4, \\ &\qquad \alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4, \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4, s\}, \\ (A_1)ws_1 &= \{\alpha_2 + 2\alpha_3 + 2\alpha_4, \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4, \\ &\qquad \alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4, r, s\}. \end{aligned}$$

Also, $(\alpha_2)w = \alpha_2$ and $(\alpha_3)w = \alpha_3$, so w centralizes L_{14}. Consequently, L_{14} acts on $X^w = \langle U_\alpha | \alpha \in (A_1)w\rangle$ as it does on X.

By (4.10), $(A_1)w \cup (A_1)ws_1 = L_2^4 \cup \{s\}$, so $R_4 = X^w X^{ws_1}$. In fact, $R_4 = X^w \times Y$ with $Y = U_{\alpha_2+2\alpha_3+2\alpha_4}U_r$. Since $\alpha_2 + 2\alpha_3 + 2\alpha_4$ is the only member of $L_2^4 \cup \{s\}$ not involving α_1, (4.8)(i) implies that $[L_{14}, Y] = 1$. Conjugating by s_1, we find that $R_4 = X^{ws_1}Y^{s_1}$ with $[L_{14}^{s_1}, Y^{s_1}] = 1$. By definition, $L_{14} = \langle U_2, U_3, U_{-2}, U_{-3}\rangle$, so $L_{14}^{s_1} = \langle U_{\alpha_1+\alpha_2}, U_3, U_{-(\alpha_1+\alpha_2)}, U_{-3}\rangle$. Since $[U_{\alpha_1+\alpha_2}, U_{-2}] = U_1$, it follows that $L_4 = \langle L_{14}, L_{14}^{s_1}\rangle$. We will determine the action of L_4 on R_4 by using the known actions of L_{14} and $L_{14}^{s_1} = L_{14}^{ws_1}$.

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 $\mathbf{F}_q$-space, so each $a \in \mathbf{F}_q$ determines a scalar multiplication $v \longrightarrow av$ 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,

$$V_2' = U_s \oplus U_{\alpha_1+2\alpha_2+2\alpha_3+2\alpha_4} \oplus U_{\alpha_1+2\alpha_2+4\alpha_3+2\alpha_4}.$$

Also, the commutator relations imply that

$$[U_{\pm 1}, U_s] = [U_{\pm 1}, U_{\alpha_1+2\alpha_2+2\alpha_3+2\alpha_4}] = [U_{\pm 1}, U_{\alpha_1+2\alpha_2+4\alpha_3+2\alpha_4}] = 1.$$

Thus, $\langle U_1, U_{-1}\rangle$ 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 $\mathbf{F}_q$-space. We know that L_{14} acts on V_1, while inducing the identity on V_2, and a similar statement holds for $L_{14}^{s_1}$. Thus, $L_1 = \langle L_{14}, L_{14}^{s_1}\rangle$ acts on V as a group of $\mathbf{F}_q$-linear transformations.

Consider the action of $L_{14}^{s_1} \approx SO(5, q)'$ or $SO^-(6, q)'$ on the space $(V_1)s_1$. Clearly $L_{124} = \langle U_3, U_{-3}\rangle = L_{124}^{s_1}$. Here $L_{124}^{s_1}$ is contained in a proper parabolic subgroup of $L_{14}^{s_1}$, and since α_2 is long, it follows as in (3.1) that $L_{124}^{s_1}$ stabilizes an isotropic (or singular) 1-space $\langle v\rangle \nleq \mathrm{rad}((V_1)s_1)$. (Actually, $\mathrm{rad}((V_1)s_1)$ 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 $\langle v\rangle^\perp/\langle v\rangle$ and acts irreducibly on this space, or $G = F_4(q)$ with q even and L_{124} acts irreducibly on $\langle v\rangle^\perp/\langle v\rangle$ + rad$((V_1)s_1)$, inducing $Sp(2, q)$ there. Now L_{14} is trivial on V_2, so $L_{124} \leqslant L_{14}^{s_1}$ is trivial on the subspace V_2 of $(V_1)s_1$. Thus, if rad$((V_1)s_1) = 0$, then V_2 must be a hyperbolic plane. If rad$((V_1)s_1) \neq 0$, then by (3.1) we have rad$((V_1)s_1) = U_{\alpha_1+\alpha_2+\alpha_3}^{ws_1} = U_s \nleqslant V_2$; once again it follows that V_2 is a hyperbolic plane. In either case, since $L_{124}^{s_1}$ fixes V_2' we have $(V_1)s_1 = V_2 \perp V_2'$.

Similarly, V_1 is the usual module for L_{14}, and we can write $V_1 = V_2^* \perp V_2'$ for a hyperbolic plane $V_2^* = (V_2)s_1^{-1}$. 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 $L_{14}^{s_1}$, respectively. The form on V restricts to V_1 and $(V_1)s_1$ in the obvious way. This is well defined. Indeed, as before, s_1 is trivial on $V_2' = V_1 \cap (V_1)s_1$, so the forms on V_1 and $(V_1)s_1$ agree on their intersection V_2'.

Finally, $L_{14}^{s_1}$ is trivial on V_2 and L_{14} is trivial on V_2^*. Thus, $L_4 = \langle L_{14}, L_{14}^{s_1}\rangle$ 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 rad(V) = rad$((V_1)s_1) = U_s$. 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 $\chi(1) \geqslant q^{28}(q-1)$.*

Proof. Let $Q = Q_8$, and consider $\chi|Q$. By (4.4) Q is special of order q^{57}, $|U_r| = |Z(Q)| = q$, and if $|Z(Q):T| = p$, then Q/T is extraspecial of order $q^{56}p$. Let φ be a nonlinear irreducible constituent of $\chi|Q$, and set $T = Z(Q) \cap \ker\varphi$. Then $|Z(Q):T| = p$ and φ is faithful on Q/T. Thus, $\varphi(1) = q^{28}$. Also, φ is determined by $\varphi|Z(Q)$. Since H is transitive on $U_r^\# = Z(Q)^\#$ and $\varphi^h \in \chi|Q$ for each $h \in H$, $\chi(1) \geqslant q^{28}(q-1)$, as claimed.

5. The constituents of 1_B^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 $n \geqslant 3$, whose Dynkin diagram is in Table 1. Let $S = \{G(q) | q$ 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) $|B(q):B(q) \cap B(q)^{s_i}| = q^{c_i}$;

(iii) $|U_i| = q^{c_i}$; 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 $n \leqslant 2$ will be handled separately.

TABLE 5

Type of Group	$c_1 = \cdots = c_{n-1}$	c_n
${}^2A_{2n}(q)$	2	3
${}^2A_{2n-1}(q)$	2	1
$B_n(q)$	1	1
$C_n(q)$	1	1
$D_n(q)$	1	1
${}^2D_{n+1}(q)$	1	2

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

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

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

and

$$(\psi, 1_{W_J}^W) = (\zeta_{\psi,q}, 1_{G(q)_J}^{G(q)})$$

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

(5.3) LEMMA. *Let $h(t) = \Sigma\, \psi(1) d_\psi(t)$, 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), $1_{B(q)}^{G(q)} = \Sigma\, \psi(1)\zeta_{\psi,q}$. Evaluating both sides at 1 yields the result.

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

We remark that groups of rank 2 also have reflection characters ρ, 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 jth 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 $f(t) = d_\psi(t)$. Then the following statements hold.*

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

(ii) *Write $|G(q) : B(q)| = g(q)$, so $g(t) \in Z[t]$ is a product of cyclotomic poly-*

nomials other than $t-1$. *Then*

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

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

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

(iv) *If p is a prime, then* $p^{k+1}\nmid b$.

(v) *Let* $q=p^j$, *where p is a prime and* $j\geqslant 1$. *Then* $p\nmid f(q)$ *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 $\alpha\in Q$, $k\geqslant 0$, and $f^{\#}(0)=1$. For each prime power q, $f(q)|\,|G(q)|$, where $|G(q)|\,|q^N g(q)z(q)\Pi_{i=1}^{n}(q^{c_i}-1)$, for some positive integer N. Consequently, $f^{\#}(t)|g(t)z(t)\Pi_{i=1}^{n}(t^{c_i}-1)$. 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 $k\geqslant 1$, we first note that $h(t)=\Sigma\,\psi(1)d_{\psi}(t)$ is, by (5.3), a polynomial such that $h(0)=1$. Therefore $h(t)-1=\Sigma_{\psi\neq 1}\psi(1)d_{\psi}(t)$, and since each $d_{\psi}(t)=\alpha_{\psi}t^{k_{\psi}}f_{\psi}^{\#}(t)$, with $\alpha_{\psi}>0$, and $f_{\psi}^{\#}(0)=1$, 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 $(a/b)f^{\#}(1)=f(1)=\psi(1)|\,|W|$, so $a|\,|W|$, and $b|f^{\#}(1)$. By (ii), $b|g(1)z(1)\Pi_{i=1}^{n} c_i$. 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 $f^{\#}(p)\equiv 1 \pmod p$ by (i), this is impossible.

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

REMARK. The fact that $k\geqslant 1$ 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* $n\geqslant 3$. *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* $1_B^G-1_G$ *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* $n\geqslant 1$ *defined over a field of characteristic p.*

(i) *If* $n \leqslant 2$ *and* G *is not* $Sp(4, 2)$, $G_2(2)$, $G_2(3)$, *or* ${}^2F_4(2)$, *then each nonprincipal irreducible constituent of* 1_B^G *has degree divisible by* p.

(ii) *Suppose* $n \geqslant 3$ *and* G *is neither* $Sp(2n, 2)$, $PSO(2n+1, 2)'$, *nor* $F_4(2)$. *Define* i *as follows*: $i = 1$ *or* 2 *if* G *is a classical group*; $i = 1$ *or* 4 *if* G *is* $F_4(q)$; $i = 1$ *if* G *is* ${}^2E_6(q)$; $i = 1, 2$ *or* 6 *if* G *is* $E_6(q)$; $i = 1$ *or* 7 *if* G *is* $E_7(q)$; $i = 8$ *if* G *is* $E_8(q)$. *Then each nonprincipal constituent of* $1_{G_i}^G$ *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 §§6, 7. We remark that a straightforward modification of the proof yields the conclusion of (ii) if $i = 4$ and $G = {}^2E_6(q)$. For $n = 2$, the degrees of all the irreducible constituents of 1_B^G 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 $G \leqslant G^+ \leqslant G^\natural$, where $G^\natural$ is defined in (2.6).

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

Here, G_{12} is defined as in §2. The proof of (5.8) is postponed until §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* χ *of* $1_B^G - 1_G$ *has degree divisible by* q.

PROOF. According to [33], χ can be written $\chi = \Sigma a_J 1_{G_J}^G$ with $a_J \in Z$, where the sum is over all $J \subseteq \{1, \ldots, n\}$. Then also $\chi = \Sigma a_J(1_{G_J}^G - 1_G)$, where q divides the degree of $1_{G_J}^G - 1_G$. Thus, $q | \chi(1)$.

The following technical lemma will be needed in §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* $1_{P(q)}^{G(q)}$. *Thus*

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

For $j \geqslant 1$, *write* $f_j(t) = \alpha_j t^{k_j} f_j^{\#}(t)$ *as in* (5.5)(i), $d_j = \deg f_j$, *and* $d = \max_{j \geqslant 1} d_j$. *Assume that* $d_s = d$, *and write* $k = k_s$. *Then*

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

PROOF. $|G(q):P(q)| = h(q)$, where $h(t) \in Z[t]$. Then h and the $f_j^{\#}$ are products of cyclotomic polynomials other than $t - 1$. Since $f_j(t)$ has highest term $\alpha_j x^{d_j}$ with $\alpha_j > 0$, 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,

$$h(t)t^k = h(1/t)t^{d+k} = \left(1 + \sum_{j=1}^{s} f_j(1/t)\right)t^{d+k}$$

$$= t^{d+k} + \sum_{j=1}^{s} f_j(t)t^{d+k-d_j-k_j}.$$

Since $d + k - d_s - k_s = 0$, subtraction of $h(t)$ from this last relation yields the desired result.

We remark that is 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 $n \geqslant 4$. 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 $\epsilon_1, \ldots, \epsilon_n$ be an orthonormal basis. By [8], fundamental systems of roots of types B_n, C_n, and D_n are given as follows.

$$B_n\colon \alpha_1 = \epsilon_1 - \epsilon_2, \alpha_2 = \epsilon_2 - \epsilon_3, \ldots, \alpha_{n-1} = \epsilon_{n-1} - \epsilon_n, \alpha_n = \epsilon_n;$$

$$(6.1)\quad C_n\colon \alpha_1 = \epsilon_1 - \epsilon_2, \alpha_2 = \epsilon_2 - \epsilon_3, \ldots, \alpha_{n-1} = \epsilon_{n-1} - \epsilon_n, \alpha_n = 2\epsilon_n;$$

$$D_n\colon \alpha_1 = \epsilon_1 - \epsilon_2, \alpha_2 = \epsilon_2 - \epsilon_n, \ldots, \alpha_{n-1} = \epsilon_{n-1} - \epsilon_n, \alpha_n = \epsilon_{n-1} + \epsilon_n.$$

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.

$$B_n, C_n, \text{ and } BC_n\colon \text{If } j < n,\ (\epsilon_j)s_j = \epsilon_{j+1}, (\epsilon_{j+1})s_j = \epsilon_j,$$
$$(\epsilon_i)s_j = \epsilon_i,\ i \neq j, j+1;\ (\epsilon_n)s_n = -\epsilon_n,$$
$$(\epsilon_j)s_n = \epsilon_j,\ j < n.$$

$$(6.2)\qquad D_n\colon \text{If } j < n,\ (\epsilon_j)s_j = \epsilon_{j+1}, (\epsilon_{j+1})s_j = \epsilon_j,$$
$$(\epsilon_i)s_j = \epsilon_i,\ i \neq j, j+1;\ (\epsilon_n)s_n = -\epsilon_{n-1},$$
$$(\epsilon_{n-1})s_n = -\epsilon_n, (\epsilon_j)s_n = \epsilon_j,\ j \neq n-1, n.$$

The group W can be viewed as a transitive permutation group on the set $\{\pm\epsilon_1, \ldots, \pm\epsilon_n\}$, 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 $n \geqslant 4$, 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 $|W : W_2| = 2n(n-1)$. 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* $1_{G_2}^G$ *is multiplicity-free and contains* $1_{G_1}^G$. *Moreover,* $(1_{G_1}^G, 1_{G_1}^G) = 3$ *and* $(1_{G_2}^G, 1_{G_2}^G) = 6$.

PROOF. By (2.8), $(1_{G_i}^G, 1_{G_j}^G) = (1_{W_i}^G, 1_{W_j}^G)$ for all i and j. By (6.3), $(1_{W_1}^W, 1_{W_1}^W) = 3$ and $(1_{W_2}^W, 1_{W_2}^W) = 6$. Finally, since the unordered pairs $\{\pm i, \pm j\}$ correspond to the right cosets $W_2 w$, the orbits of W_1 on this set correspond to the double cosets $W_2 w W_1$. Since there are 3 orbits, we have $(1_{W_1}^W, 1_{W_2}^W) = 3$. 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.

	Orbit Representative	Size of Orbit	Double Coset Representation
	$\{1, 2\}$	1	$w_0^* = 1$
	$\{1, 3\}$	$4(n-2)$	$w_1^* = s_2$
	$\{-1, 2\}$	2	$w_2^* = s_2 \cdots s_n \cdots s_2$
(6.6)	$\{3, 4\}$	$2(n-2)(n-3)$	$w_3^* = s_2 s_3 s_1 s_2$
	$\{-1, 3\}$	$4(n-2)$	$w_4^* = s_2 \cdots s_{n-1} s_1 s_n s_{n-1} \cdots s_2$
	$\{-1, -2\}$	1	$w_5^* = s_2 \cdots s_n \cdots s_2 s_1 s_2 \cdots s_n \cdots s_2$

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

$$\xi_i = \frac{1}{|G_2|} \sum_{x \in G_2 w_i^* G_2} x, \qquad 0 \leq i \leq 5.$$

Note that ξ_0 is the identity element of $H(G, G_2)$. Let L_{ξ_i} denote the left multiplication by ξ_i on the space $H(G, G_2)$. We note that $H(G, G_2)$ is commutative since $1_{G_2}^G$ is multiplicity-free (by (6.4)). We shall compute the matrix of the left multiplication L_{ξ_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_{ξ_1} with respect to the basis $\xi_0, \xi_1, \ldots, \xi_5$ is given by*

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

where $x = q^{c_1} = q^{c_2} = \cdots = q^{c_{n-1}}$, and $y = q^{c_n}$, and

$$\lambda = x^2 + x - 1, \qquad \xi = \frac{1}{x-1}\{(2x^2-1)(x^{2n-6}y - 1) + \lambda x^{n-3}(x-y)\},$$

$$\mu = \frac{(x^{n-3}-1)(1+x^{n-4}y)}{x-1}, \qquad \eta = \frac{(x^{n-2}-1)(1+x^{n-3}y)}{x-1},$$

$$\nu = x^{2n-6}y, \qquad \theta = \frac{(x+1)(x^{2n-6}y - x^{n-2}y + x^{n-1} - \lambda)}{x-1}.$$

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

PROOF. We have, by [13],

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

where

$$\begin{aligned} b_{1ik} &= |G_2|^{-1}|G_2w_1^*G_2 \cap w_k^*G_2w_i^*G_2| \\ &= |G_2|^{-1}|w_k^*G_2w_1^*G_2 \cap G_2w_i^*G_2| \\ &= |G_2|^{-1}|G_2w_1^*G_2w_k^* \cap G_2w_i^*G_2|, \end{aligned}$$

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 $G_2w_1^*G_2w_k^*$ and $G_2w_i^*G_2$. 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 $G_2w_1^*G_2$. We have

$$W_2s_2W_2 = \left(\bigcup_{i=1}^{2(n-2)} W_2w_{1i}\right) \cup \left(\bigcup_{j=1}^{2(n-2)} W_2w'_{1,j}\right),$$

where

$$\begin{array}{lll} w_{1,1} = s_2, & & w'_{1,1} = s_2s_1, \\ w_{1,2} = s_2s_3, & \text{and} & w'_{1,2} = s_2s_1s_3, \\ \vdots & & \vdots \\ w_{1,2(n-2)} = s_2 \cdots s_{n-1}s_n \cdots s_3, & & w'_{1,2(n-2)} = s_2s_1 \cdots s_{n-1}s_n \cdots s_3. \end{array}$$

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]),

$$G_2s_2G_2 = \left(\bigcup_{i=1}^{2(n-2)} BW_2w_{1,i}B\right) \cup \left(\bigcup_{j=1}^{2(n-2)} BW_2w'_{1,j}B\right)$$
$$= \left(\bigcup_{i=1}^{2(n-2)} G_2w_{1,i}U\right) \cup \left(\bigcup_{j=1}^{2(n-2)} G_2w'_{1,j}U\right),$$

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

$$\begin{aligned} G_2s_2U &= G_2s_2U_2 \\ G_2s_2s_3U &= G_2s_2s_3U_2^{s_3}U_3 \\ &\vdots \\ G_2s_2 \cdots s_{n-1}s_n \cdots s_3U &= G_2s_2 \cdots s_{n-1}s_n \cdots s_3U_2^{s_3\cdots s_n \cdots s_3} \cdots U_4^{s_3}U_3 \end{aligned}$$

and

$$\begin{aligned} G_2s_2s_1U &= G_2s_2s_1U_2^{s_1}U_1 \\ &\vdots \\ G_2s_2s_1 \cdots s_{n-1}s_n \cdots s_3U &= G_2s_2s_1 \cdots s_{n-1}s_n \cdots s_3U_2^{s_3\cdots s_ns_{n-1}\cdots s_1}U_4^{s_3}U_3. \end{aligned}$$

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,

...

$G_2s_2 \cdots s_{n-1}s_n \cdots s_3U$ contains $x^{2n-5}y$ left G_2 cosets,

$G_2s_2s_1U$ contains x^2 left G_2 cosets,

...

$G_2s_2s_1 \cdots s_{n-1}s_n \cdots s_3$ contains $x^{2n-4}y$ left G_2 cosets.

In particular, $G_2w_1^*G_2$ 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 η is given in the statement of (6.7).

We shall now give, in tabular form, the distribution of the G_2-cosets in $G_2 w_1^* G_2 w_k^*$. (Zeros are omitted in the tables, except in the totals.) Determination of the double coset containing a given $w \in W$ is made by applying w to $\{\epsilon_1, \epsilon_2\}$ and finding the orbit to which $\{(\epsilon_1)w, (\epsilon_2)w\}$ belongs. Determination of whether $l(ws_i) \geqslant l(w)$, 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 $l(ws_i) \geqslant l(w)$. In computations with root systems we shall use the notation S_α for the linear map $x \longrightarrow x - 2(x, \alpha)\alpha/(\alpha, \alpha)$, where $\alpha \in E_n$. After each case some remarks will be made on some of the less obvious parts of the calculations.

	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2 w_1^* G_2 w_0^*$	0	$x(x+1)\eta$	0	0	0	0
$G_2 w_1^* G_2 w_1^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2 w_{1,2} U w_1^*$	1	$x-1$				
$G_2 w_{1,2} U w_1^*$		x^2				
$\vdots$		$\vdots$				
$G_2 w_{1,2n-5} B w_1^*$		$x^{2n-6}y$				
$G_2 w_{1,2n-4} B w_1^*$			$x^{2n-5}y$			
$G_2 w'_{1,1} B w_1^*$		x^2				
$G_2 w'_{1,2} B w_1^*$				x^3		
$\vdots$				$\vdots$		
$G_2 w_{1,2n-5} B w_1^*$				x^{2n-5}		
$G_2 w'_{1,2n-4} B w_1^*$					$x^{2n-4}y$	
Totals	1	$\lambda + \mu x^2$	$x\nu$	μx^3	$x^2\nu$	0

REMARKS. $G_2 w_{11} B w_1^* = G_2 s_2 U_2 s_2 \subset G_2 \cup G_2 s_2 U_2^\#$, since $s_2 U_2 s_2 = \{1\} \cup s_2 U_2^\# s_2$ and $s_2 U_2^\# s_2 \subset G_2 s_2 U_2$.

$G_2w_1^*G_2w_2^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_2^*$		1	$x-1$			
$G_2w_{12}Uw_2^*$		x	$x(x-1)$			
$\vdots$		$\vdots$	$\vdots$			
$G_2w_{1,2n-4}Uw_2^*$		$x^{2n-6}y$	$x^{2n-6}y(x-1)$			
$G_2w'_{1,1}Uw_2^*$					x^2	
$\vdots$					$\vdots$	
$G_2w'_{1,2n-4}Uw_2^*$					$x^{2n-4}y$	
Totals	0	η	$(x-1)\eta$	0	$x^2\eta$	0

REMARKS. $w_2^* = S_{\epsilon_2}$.

$$G_2w_{11}Uw_2^* = G_2s_2U_2w_2^* = G_2s_2U_2s_2(s_3w_2^*) = G_2s_2w_2^* \cup G_2w_2^*U_2^{\# s_2w_2^*},$$

and $(\alpha_2)w_2^* = (\alpha_2)S_{\epsilon_2} < 0$, giving 1 coset in $G_2w_1^*G_2$ and $x-1$ cosets in $G_2w_2^*G_2$.

$$G_2w_{12}Uw_2^* = G_2s_2s_3U_2^{s_3}U_3w_2^* = (G_2s_2U_2w_2^*)U_3^{w_2^*s_3},$$

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

$$G_2w'_{1i}Uw_2^* \subset G_2w_4^*G_2, \quad 1 \leq i \leq 2n-4.$$

$G_2w_1^*Uw_3^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_3^*$		1		$x-1$		
$G_2w_{12}Uw_3^*$		x		$x(x-1)$		
$G_2w_{13}Uw_3^*$				x^3		
$\vdots$				$\vdots$		
$G_2w_{1,2n-6}Uw_3^*$				$x^{2n-7}y$		
$G_2w_{1,2n-5}Uw_3^*$					$x^{2n-6}y$	
$G_2w_{1,2n-4}Uw_3^*$					$x^{2n-5}y$	
$G_2w'_{1,1}Uw_3^*$		x		$x(x-1)$		
$G_2w'_{1,2}Uw_3^*$		x^2		$x^2(x-1)$		
$G_2w'_{1,3}Uw_3^*$				x^4		
$\vdots$		$\vdots$		$\vdots$		
$G_2w'_{1,2n-6}Uw_3^*$				$x^{2n-6}y$		
$G_2w'_{1,2n-5}Uw_3^*$					$x^{2n-5}y$	
$G_2w'_{1,2n-4}Uw_3^*$					$x^{2n-4}y$	
Totals	0	$(x+1)^2$	0	θ	$(x+1)^2\nu$	0

$G_2w_1^*Uw_4^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_4^*$		1			$x-1$	
$G_2w_{1,2}Uw_4^*$				x	$x(x-1)$	
$\vdots$				$\vdots$	$\vdots$	
$G_2w_{1,2n-5}Uw_4^*$				$x^{2n-7}y$	$x^{2n-7}y(x-1)$	
$G_2w_{1,2n-4}Uw_4^*$					$x^{2n-5}y$	
$G_2w'_{11}Uw_4^*$			x		$x(x-1)$	
$G_2w'_{12}Uw_4^*$					x^3	
$\vdots$					$\vdots$	
$G_2w'_{1,2n-5}Uw_4^*$					$x^{2n-5}y$	
$G_2w'_{1,2n-4}Uw_4^*$						$x^{2n-4}y$
Totals	0	1	x	$x\mu$	ξ	$x^2\nu$

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

For $G_2w_{11}Uw_4^*$, $(\alpha_2)w_4^* < 0$.

For $G_2w_{12}Uw_4^*$, $(\alpha_3)w_4^* > 0$, $(\alpha_2)s_3w_4^* < 0$.

For $G_2w_{13}Uw_4^*$, $(\alpha_4)w_4^* > 0$, $(\alpha_3)s_4w_4^* > 0$, $(\alpha_2)s_3s_4w_4^* < 0$.

$\vdots$

For $G_2w_{1,2n-5}Uw_4^*$, $(\alpha_4)w_4^* > 0$, $(\alpha_5)s_4w_4^* > 0, \ldots,$

$$(\alpha_3)s_4 \cdots s_n \cdots s_4w_4^* > 0,$$

$$(\alpha_2)s_3 \cdots s_n \cdots s_3s_4^* < 0.$$

For $G_2w_{1,2n-4}Uw_4^*$, $(\alpha_2)s_2 \cdots s_n \cdots s_3w_4^* > 0$.

$G_2w_1^*Uw_5^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_5^*$					1	$x-1$
$\vdots$					$\vdots$	$\vdots$
$G_2w_{1,2n-4}Uw_5^*$					$x^{2n-6}y$	$x^{2n-6}y(x-1)$
$G_2w'_{11}Uw_5^*$					x	$x(x-1)$
$\vdots$					$\vdots$	$\vdots$
$G_2w'_{1,2n-4}Uw_5^*$					$x^{2n-5}y$	$x^{2n-5}y(x-1)$
Totals	0	0	0	0	$(x+1)\eta$	$(x^2-1)\eta$

REMARKS. $w_5^* = S_{\epsilon_2+\epsilon_1}$.
This completes the proof of (6.7).

(6.8) LEMMA. *The characteristic roots of M are*:

$$\theta_0 = x(x+1)(1+x^{n-3}y)(x^{n-2}-1)(x-1)^{-1},$$
$$\theta_1 = (x^{n-2}y+\lambda)(x^{n-2}-1)(x-1)^{-1},$$
$$\theta_2 = (x^{n-1}-\lambda)(1+x^{n-3}y)(x-1)^{-1},$$
$$\theta_3 = -(x+1)(1+x^{n-3}y),$$
$$\theta_4 = (x+1)(x^{n-2}-1),$$
$$\theta_5 = -(x+1+x^{n-3}(y-x)).$$

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 L_{ξ_1} has 6 distinct characteristic roots, it follows that the Hecke algebra $H(G, G_2)$ is generated by ξ_1. Recall that $\xi_0 = |G_2|^{-1}\Sigma_{x\in G_2} x$ 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 $1_{G_2}^G$. 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 ξ_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) $1_{G_2}^G = 1_{G(q)_2}^{G(q)}$ *has exactly* 6 *irreducible constituents* $\zeta_{0,q}, \zeta_{1,q}, \ldots, \zeta_{5,q}$, *which are afforded by the subspaces of V belonging to the characteristic roots* $\theta_0, \ldots, \theta_5$ *of A. The degree of* $\zeta_{i,q}$ *is the multiplicity of* θ_i *as a characteristic root of A.*

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

PROOF. Since the 6×6 matrix M has 6 different characteristic roots, we know that the characteristic and minimal polynomials of M coincide. Since $\beta \longrightarrow L_\beta$ is a faithful representation of the algebra $H(G, G_2)$, we have $p(\xi_1) = 0$ in $H(G, G_2)$. Also, $\xi_1 \longrightarrow A$ 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 ξ_1. Therefore, if, for some polynomial $f(t)$, $f(A) = 0$, we have $f(R_{\xi_1}) = 0$, where R_{ξ_1} is the right multiplication by ξ_1 in $H(G, G_2)$, then $f(\xi_1) = 0$. Therefore $p(t)|f(t)$, 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 $\mathrm{Hom}_{CG}(V, V)$, 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 $1_{G_2}^G$ 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 ξ_1 on V and let $s \geqslant 0$ be an integer. Then* trace $A^s = |G:G_2|\eta_{s0}$, *where η_{s0} is defined by* $\xi_1^s = \Sigma_{i=0}^5 \eta_{si}\xi_i$.

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

$$\operatorname{trace}(A^s) = \operatorname{trace}(\xi_1^s)_R = \sum_{i=0}^{5} \eta_{si} \operatorname{trace}(\xi_i)_R.$$

Moreover, $\operatorname{trace}(\xi_0)_R = \dim V = |G:G_2|$. It suffices to show that $\operatorname{trace}(\xi_i)_R = 0$ for $i \geqslant 0$. Let $G_2w_i^*G_2 = \bigcup g_{ji}w_i^*G_2$ (disjoint), for $i = 0, \ldots, 5$. Then the elements $\{g_{ji}w_i^*\xi_0\}_{i,j}$ form a basis for V. For $t = 0, \ldots, 5$ we have

$$g_{ji}w_i^*\xi_0\xi_t = \sum_{l,k} a_{ji,lk}^t g_{lk}w_k^*\xi_0, \tag{6.11}$$

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

$$\xi_t = a_{ji,ji}^t\xi_0 + \sum_{h,l} b_{lh}g_{lh}w_h^*\xi_0,$$

with $b_{lh} \geqslant 0$. 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*

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

for $n \geqslant 4$. 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 $\eta_{si}(x, y) \in Z[x, y]$ such that $\xi_1^s = \Sigma_{i=0}^5 \eta_{si}(q^{c_1}, q^{c_n})\xi_i$, as in (6.10). Define $T_s(x, y) = F(x, y)\eta_{s0}(x, y)$, for $s \geqslant 0$. Then $T_s(x, y) \in Z[x, y]$, and $T_s(q^{c_1}, q^{c_n}) = \operatorname{trace} A^s$, $s \geqslant 0$.

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

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

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

(6.13) LEMMA. *Let*

$$K(x, y) = F(x, y)\left(\sum_{k=0}^{4} h_k(x, y)\eta_{k,0}(x, y)\right).$$

Then

$$K(q^{c_1}, q^{c_n}) = \text{trace } p_i(q^{c_1}, q^{c_n}, A).$$

PROOF. The result is immediate from (6.10) and (6.12).

(6.14) PROPOSITION. *Let t be an indeterminate, and let*

$$\delta_i(t) = \prod_{j \neq i} (\theta_i(t^{c_1}, t^{c_n}) - \theta_j(t^{c_i}, t^{c_n})),$$

and

$$d_i(t) = K(t^{c_1}, t^{c_n})/\delta_i(t).$$

Then $d_i(q) = \zeta_{i,q}(1)$ *for all q.*

PROOF. Immediate from (6.9)(iii) and (6.13).

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

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

Using (6.8), direct computation (which is omitted) shows that $\delta_i(t) \in Z[t]$, 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 $K(t^{c_1}, t^{c_2}) \in Z[t]$, it follows that $d_i(t) \in Z[t]$ if $\delta_i(t)$ is monic, and $d_i(t) = \frac{1}{2}d_i'(t)$, with $d_i'(t) \in Z[t]$ 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 $d_i(t) \in Z[t]$, 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, $G = PSO^-(2n + 2, 2)'$. Assume one or both of $d_4(2), d_5(2)$ is odd. The odd degrees must be associated with characters in $1_{G_2}^G - 1_{G_1}^G$ because of the formulas of the degrees in $1_{G_1}^G$ given in Table 3. The sum of the generic degrees of the characters in $1_{G_2}^G - 1_{G_1}^G$ is, by Table 3,

$$f(t) = (t^{n+1} + 1)(t^{2n} - 1)(t^{n-1} - 1)(t - 1)^{-1}(t^2 - 1)^{-1}$$
$$- (t^{n+1} + 1)(t^n - 1)(t - 1)^{-1}.$$

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 $1_{G_2}^G - 1_{G_1}^G$. If $d(t)$ is a generic degree for which $d(2)$ is odd, we have $t^2 | d(t)$, and $2d(t) \in Z[t]$. 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 $\epsilon_1, \ldots, \epsilon_n$ of E_n so that the roots in Δ' are $\pm\epsilon_i$, $1 \leq i \leq n$, and $\pm(\epsilon_i \pm \epsilon_j)$, for $1 \leq i < j \leq n$. For a fundamental system we take $\alpha'_1 = \epsilon_1 - \epsilon_2, \ldots, \alpha'_{n-1} = \epsilon_{n-1} - \epsilon_n$, and $\alpha'_n = \epsilon_n$.

Now let Δ be the set of roots consisting of $\pm 2\epsilon_i$, $1 \leq i \leq n$, and $\pm(\epsilon_i \pm \epsilon_j)$, for $1 \leq i < j \leq n$. Then Δ is a system of type C_n, and as a base we may take $\alpha_1 = \epsilon_1 - \epsilon_2, \ldots, \alpha_{n-1} = \epsilon_{n-1} - \epsilon_n$ and $\alpha_n = 2\epsilon_n$. There is an obvious bijection from Δ' to Δ sending α'_i to α_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 $1_{G_2}^G$ except when $c_1 = \cdots = c_{n-1} = c_n = 1$ and $q = 2$, where $G = C_n(2) \cong Sp(2n, 2)$. 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 $\epsilon_1, \ldots, \epsilon_n$ 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).

(6.17)

Orbit Representative	Size of Orbit	Double Coset Representatives
$\{1, 2\}$	1	$w_0^* = 1$
$\{1, 3\}$	$4(n-2)$	$w_1^* = s_2$
$\{-1, 2\}$	2	$w_2^* = s_2 \cdots s_{n-2}s_{n-1}s_ns_{n-2} \cdots$
$\{3, 5\}$	$2(n-2)(n-3)$	$w_3^* = s_2s_3s_1s_2$
$\{-1, 3\}$	$4(n-2)$	$w_4^* = s_2 \cdots s_{n-2}s_1s_{n-1}s_ns_{n-2} \cdots$
$\{-1, -2\}$	1	$w_5^* = w_2^*s_1w_2^*$

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_{ξ_1}.

(6.18) LEMMA. *The matrix M' of the left multiplication L_{ξ_1} with respect to the basis $\xi_0, \xi_1, \ldots, \xi_5$ is*

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

where

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

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

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

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

PROOF. As in the case of B_n, we begin by finding a set of shortest W_2-coset representatives in $W_2 w_1^* W_2$. Using the same notation as in the case of B_n, we have

$$W_2 s_2 W_2 = \left(\bigcup_{i=1}^{2n-4} W_2 w_{1i}\right) \cup \left(\bigcup_{j=1}^{2n-4} W_2 w'_{1j}\right) \quad \text{(disjoint)},$$

where

$$\begin{aligned} w_{1,1} &= s_2, \\ w_{1,2} &= s_2 s_3, \\ &\vdots \\ w_{1,n-2} &= s_2 \cdots s_{n-1}, \\ w_{1,n-1} &= s_2 \cdots s_{n-2} s_n, \\ w_{1,n} &= s_2 \cdots s_{n-2} s_{n-1} s_n, \\ w_{1,n+1} &= s_2 \cdots s_n s_{n-2}, \\ &\vdots \\ w_{1,2n-4} &= s_2 \cdots s_n s_{n-2} \cdots s_3, \end{aligned}$$

and

$$w'_{1j} = s_2 s_1 s_2 w_{1j} \quad \text{for } 1 \leq j \leq 2n - 4.$$

As in the case of B_n, this is verified by checking that the elements of $\{w_{1i}\}$ 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 $G_2 w_1^* G_2 w_k^*$ in the different (G_2, G_2)-double cosets. The first step is to find G_2-coset representatives in $G_2 w_1^* G_2$. This is done using the root structure in G_2, and the formulas $G_2 w_{1,1} G_2 s_2 U = G_2 s_2 U_1$, $G_2 w_{1,2} G_2 = G_2 s_2 s_3 U = G_2 s_2 s_3 U_3 U_2^{s_3}$, etc. The following tables give the required information.

$G_2 w_1^* G_2 w_0^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2 w_{11} U w_0^*$		x				
⋮		⋮				
$G_2 w_{1,n-2} U w_0^*$		x^{n-2}				
$G_2 w_{1,n-1} U w_0^*$		x^{n-2}				
⋮		⋮				
$G_2 w_{1,2n-4} U w_0^*$		x^{2n-5}				
$G_2 w'_{1,1} U w_0^*$		x^2				
⋮		⋮				
$G_2 w'_{1,2n-4} U w_0^*$		x^{2n-4}				
Totals	0	$x(x+1)\eta'$	0	0	0	0

$G_2 w_1^* G_2 w_1^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2 w_{11} U w_1^*$	1	$x - 1$				
$G_2 w_{12} U w_1^*$		x^2				
⋮		⋮				
$G_2 w_{1,2n-5} U w_1^*$		x^{2n-6}				
$G_2 w_{1,2n-4} U w_1^*$			x^{2n-5}			
$G_2 w'_{11} U w_1^*$		x^2		x^3		
⋮				⋮		
$G_2 w'_{1,2n-5} U w_1^*$				x^{2n-5}		
$G_2 w'_{1,2n-4} U w_1^*$					x^{2n-4}	
Totals	1	$\lambda + \mu' x^2$	$x\nu'$	$\mu' x^3$	$x^2 \nu'$	0

$G_2w_1^*G_2w_2^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_2^*$		1	$x-1$			
$\vdots$		$\vdots$	$\vdots$			
$G_2w_{1,2n-4}Uw_2^*$		x^{2n-6}	$x^{2n-6}(x-1)$			
$G_2w'_{11}Uw_2^*$					x^2	
$\vdots$					$\vdots$	
$G_2w'_{1,2n-4}Uw_2^*$					x^{2n-4}	
Totals	0	η'	$(x-1)\eta'$	0	$x^2\eta'$	0

REMARK. In checking these results, it is useful to know that w_2^* has the following expression as a product of two commuting reflections:

$$w_2^* = S_{(\alpha_n)s_{n-2}\cdots s_n} S_{(\alpha_{n-1})s_{n-2}\cdots s_2} = S_{\epsilon_2+\epsilon_n} S_{\epsilon_2-\epsilon_n}.$$

$G_2w_1^*G_2w_3^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_3^*$		1		$x-1$		
$G_2w_{12}Uw_3^*$		x		$x(x-1)$		
$G_2w_{13}Uw_3^*$				x^3		
$\vdots$				$\vdots$		
$G_2w_{1,2n-6}Uw_3^*$				x^{2n-7}		
$G_2w_{1,2n-5}Uw_3^*$					x^{2n-6}	
$G_2w_{1,2n-4}Uw_3^*$					x^{2n-5}	
$G_2w'_{11}Uw_3^*$		x		$x(x-1)$		
$G_2w'_{12}Uw_3^*$		x^2		$x^2(x-1)$		
$G_2w'_{13}Uw_3^*$				x^4		
$\vdots$				$\vdots$		
$G_2w'_{1,2n-6}Uw_3^*$				x^{2n-6}		
$G_2w'_{1,2n-5}Uw_3^*$					x^{2n-5}	
$G_2w'_{1,2n-4}Uw_3^*$					x^{2n-4}	
Totals	0	$(x+1)^2$	0	θ'	$\nu'(x+1)^2$	0

$G_2w_1^*G_2w_4^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_4^*$		1			$x-1$	
$G_2w_{12}Uw_4^*$				x	$x(x-1)$	
⋮				⋮	⋮	
$G_2w_{1,2n-5}Uw_4^*$				x^{2n-7}	$x^{2n-7}(x-1)$	
$G_2w_{1,2n-4}Uw_4^*$					x^{2n-5}	
$G_2w'_{11}Uw_4^*$			x		$x(x-1)$	
$G_2w'_{12}Uw_4^*$					x^3	
⋮					⋮	
$G_2w'_{1,2n-5}Uw_4^*$					x^{2n-5}	
$G_2w'_{1,2n-4}Uw_4^*$						x^{2n-4}
Totals	0	1	x	$\mu'x$	ξ'	x^{2n-4}

REMARK. In this case, it is helpful to express w_4^* as a product of three commuting reflections:

$$w_4^* = S_{\epsilon_2+\epsilon_n}S_{\epsilon_2-\epsilon_n}S_{\epsilon_1-\epsilon_3}.$$

$G_2w_1^*G_2w_5^*$	w_0^*	w_1^*	w_2^*	w_3^*	w_4^*	w_5^*
$G_2w_{11}Uw_5^*$					1	$x-1$
⋮					⋮	⋮
$G_2w_{1,2n-4}Uw_5^*$					x^{2n-6}	$x^{2n-6}(x-1)$
$G_2w'_{11}Uw_5^*$					x	$x(x-1)$
⋮					⋮	⋮
$G_2w'_{1,2n-4}Uw_5^*$					x^{2n-5}	$x^{2n-5}(x-1)$
Totals	0	0	0	0	$(x+1)\eta'$	$(x^2-1)\eta'$

REMARK. As in the case of B_n, this time $w_5^* = S_{\epsilon_1+\epsilon_2}$.
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 $1_{G_2}^G$, as in (6.14).

Let $\delta_i(t, 1) = \Pi_{j \neq i}(\theta_i(t, 1) - \theta_j(t, 1))$. 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 $h(t) = \alpha_k t^k + \alpha_{k+1}t^{k+1} + \cdots + \alpha_l t^l$, where $k \leqslant l$ and $\alpha_i \in Q$, we will say that $h(t)$ *leads with* $\alpha_k t^k$ and has *highest term* $\alpha_l t^l$.

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

PROOF. By (5.4), $1_{G_1}^G$ contains the reflection character ρ. By (4.3)(ii) and Table 4, $1_{G_1}^G - 1_G$ is the sum of ρ 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 $1_{G_2}^G$. By (4.3)(ii), $1_{G_2}^G \supset 1_{G_1}^G$.

Suppose some irreducible constituent of $1_{G_2}^G - 1_G$ 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 $1_{G_2}^G - 1_{G_1}^G$ has degree not divisible by p, and we can write

$$f_1(t) + f_2(t) = (t^4 + 1)(t^9 - 1)(t - 1)^{-1}(t^{12} - 1)(t^3 - 1)^{-1} - (t^9 - 1)(t - 1)^{-1}(t^{12} - 1)(t^4 - 1)^{-1}, \tag{7.2}$$

where $f_i(t) \in Q[t]$, $f_1(1) = 15$ 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 $f_1(t) = (a/c)t^3 f_1^\#(t)$ and $f_2(t) = (b/d)t^3 f_2^\#(t)$, 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 $q^3 | c$ imply that $q = 2$ or 3 (see (5.5)(v)).

The right side of (7.2) is divisible by $\Phi_5(t)$, where $\Phi_5(1) = 5$. Also, $5 | f_1(1)$ and $5 | f_2(1)$, while 5 cannot divide both a and b. As $f_i^\#(t)$ is a product of cyclotomic polynomials by (5.5)(i), $\Phi_5(t)$ divides one and, hence, both $f_i(t)$'s. As $5^2 \nmid f_i(1)$, $5 \nmid a, b$. Also, $5^2 \nmid |W|$, so $\Phi_5(t)^2 \nmid f_i^\#(t)$. Since $5 | f_i(1)$, 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 $1_{G_l}^G$ is the sum of 1, $\zeta_{\varphi,q}$ (the reflection character; see (5.4)) and three other characters of G. Accordingly, we apply (5.5) and write

$$f_1(t) + f_2(t) + f_3(t) = l(t) - 1 - d_\varphi(t), \tag{7.3}$$

where $l(t) \in Z[t]$ is the polynomial such that $l(q) = [G(q):G_l(q)]$, and $f_j(t) \in Q[t]$ for $j = 1, 2, 3$ are the generic degrees of the three other characters of G in $1_{G_l}^G$. Let $\varphi_1, \varphi_2, \varphi_3$ be the irreducible characters of W such that $f_j(t) = d_{\varphi_j}(t)$, $j = 1, 2, 3$. Write $f_j(t) = \alpha_j t^{k_j} f_j^{\#}(t)$ as in (5.5), and let $d_j = \deg f_j(t)$, $j = 1, 2, 3$. Arrange the indexing so that $d = d_3 = \max\{d_1, d_2, d_3\}$, and set $k = k_3$.

(7.4) LEMMA. *Let $G = {}^2E_6(q), E_7(q), E_8(q)$, or $F_4(q)$, and let $h(t) = \Sigma\,\psi(1)d_\psi(t)$ as in (5.3). The leading term of $h(t) - 1 - \varphi(1)d_\varphi(t)$, where φ is the reflection character, is, respectively, $2t$, $27t^2$, $35t^2$ and t. In each case this term is $\varphi_j(1)t^{k_j}$ for some $j = 1, 2$ or 3. If G is ${}^2E_6(q), E_7(q)$ or $E_8(q)$, then $f_j(t)$ is monic. If $G = F_4(q)$, then $\alpha_j = ½$.*

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, t^2, $½t$, respectively. Consequently, this term has the form $\alpha_j t^{k_j}$, $(\alpha_j + \alpha_l)t^{k_j}$ or $(\alpha_1 + \alpha_2 + \alpha_3)t^{k_1}$, respectively. Therefore $1 = \alpha_j$, $\alpha_j + \alpha_l$ or $\alpha_1 + \alpha_2 + \alpha_3$ if $G = {}^2E_6(q), E_7(q)$, or $E_8(q)$, and $½ = \alpha_j$, $\alpha_j + \alpha_l$ 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 $h(t) - 1 - \varphi(1)d_\varphi(t)$ is at least $\varphi_j(1)\alpha_j$, $\varphi_j(1)\alpha_j + \varphi_l(1)\alpha_l$, or $\varphi_1(1)\alpha_1 + \varphi_2(1)\alpha_2 + \varphi_3(1)\alpha_3$, depending on the form of the leading term of (7.3). The only possibilities are as follows: $\alpha_j = 1$ and $\varphi_j(1) = 2, 27$, or 35, respectively, if $G = {}^2E_6(q), E_7(q)$ or $E_8(q)$; and $\alpha_j = ½$ and $\varphi_j(1) = 2$ if $G = F_4(q)$. This completes the proof of (7.4).

Next apply (5.10) to (7.3) to obtain

$$\begin{aligned} &f_1(t)(t^{d+k-d_1-k_1} - 1) + f_2(t)(t^{d+k-d_2-k_2} - 1) \\ &\qquad = l(t)(t^k - 1) - (t^{d+k} - 1) - d_\varphi(t)(t^{d+k-a-b} - 1) \end{aligned} \tag{7.5}$$

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

$$\begin{aligned} &f_1(1)(d + k - d_1 - k_1) + f_2(1)(d + k - d_2 - k_2) \\ &\qquad = l(1)k - (d + k) - \varphi(1)(d + k - a - b). \end{aligned} \tag{7.6}$$

(7.7) PROPOSITION. *If $G = {}^2E_6(q)$, then Theorem (5.7) holds.*

PROOF. Assume the result is false. By Table 4, $q | \rho(1)$, and so $p \nmid f_i(q)$ for some $i = 1, 2, 3$. For j 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

$$f_1(1)(21 + k - d_1 - k_1) + f_2(1)(21 + k - d_2 - k_2) = 19k - 33. \tag{7.8}$$

By Table 4, $\{f_1(1), f_2(1), f_3(1)\} = \{2, 8, 9\}$, and by (7.4), $f_j(1) = 2$ and $f_j(t)$ is monic. We claim that for $s = 1, 2$ or 3, $f_s(1) = 9$ implies $k_s \geqslant 3$. By (4.3)(i) and (5.2) the constituent of $1_{G_1}^G - 1_G - \rho$ with generic degree $f_s(t)$ also appears in $1_{G_4}^G$. Writing down the analogue of (7.3) for $1_{G_4}^G$, we obtain an equation in which the right-hand side leads with t^3. By (5.5)(i), $t^3 | f_s(t)$, and $k_s \geqslant 3$, as required.

If $k = 1$, then $f_1(t) + f_2(t) = l(t) - 1 - d_\varphi(t) - f_3(t)$, and the right side is in $Z[t]$ since $l(t) - 1 - d_\varphi(t)$ leads with t. Thus $k_1 = k_2 \geqslant 3$ 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 $k_2 = k_3 \geqslant 3$. 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), $q^k | c$; a and b divide $|W|$; and $c \,|\, |W|2^2$. Since $(a, b) = 1$ and $k \geqslant 3$, 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 ${}^2E_6(q)$. By Table 4, $q | \rho(1)$, so $p \nmid f_i(q)$ 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

$$f_1(1)(33 + k - d_1 - k_1) + f_2(1)(33 + k - d_2 - k_2) = 118k - 138. \tag{7.10}$$

If k is 2, then $f_3(t)$ is monic, and as in the case of ${}^2E_6(q)$, 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 $d_1 < 33$, $k_2 = k_3 \geqslant 3$, 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 $|W|$, and $c \,|\, |W|$. We may assume that $f_2(1) = 35$ and $f_3(1) = 56$.

(7.11) LEMMA. *Each nonprincipal irreducible constituent of $1_{G_7}^G$ has degree divisible by q. Moreover, $1_{W_7}^W = 1 + \varphi + \varphi_1 + \tau$, where φ is the reflection character and $d_\tau(t)$ is monic.*

PROOF. By (4.3)(iii), $1_{W_7}^W$ decomposes as in the statement of (7.11), and $\tau(1) = 21$. It suffices to show that $d_\tau(t)$ is monic. From (5.2) and (4.3) we obtain

$$\begin{aligned} d_\tau(t) + f_1(t) &= (t^5 + 1)(t^9 + 1)(t^{14} - 1)(t - 1)^{-1} - 1 \\ &\quad - t(t^6 + 1)(t^{14} - 1)(t^2 + 1)^{-1}(t^2 - 1)^{-1}. \end{aligned} \tag{7.12}$$

Since $f_1(t)$ is monic, $d_\tau(t) \in Z[t]$. The right side of (7.12) is monic of degree 27, so if $d_\tau(t)$ is not monic, $\deg(d_\tau(t)) < 27$ and $d_1 = 27$. Apply (5.10) to (7.12) to obtain

$$d_T(t)(t^{29-u-v}-1) = (t^5+1)(t^9+1)(t^{14}-1)(t-1)^{-1}(t^2-1)-(t^{29}-1)$$
$$\qquad - t(t^6+1)(t^{14}-1)(t^2+1)^{-1}(t^2-1)^{-1}(t^{29-17-1}-1). \tag{7.13}$$

where $u = \deg(d_T(t))$ and t^v is the highest power of t dividing $d_T(t)$. Differentiate (7.13), and evaluate at $t = 1$, to obtain

$$21(29-u-v) = 6, \tag{7.14}$$

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 $a|\varphi_2(1)$ and $b|\varphi_3(1)$, 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 $q^k|c$, and $c|f_2^{\#}(1)$, and $f_2^{\#}(1)|\,|W|$, by (5.5). Since $5^2 \nmid |W|$ and $7^2 \nmid |W|$, 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), $d_T(t)$ is monic. Since $d_T(1)$ has to be a multiple of 7, a check of the cyclotomic polynomials in the formula for the order of $E_7(q)$ shows that $\Phi_7(t)|d_T(t)$. 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 $7^2 \nmid |W|$, 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 $G = E_8(q)$, then Theorem (5.7) holds.*

PROOF. Assume once more that the result is false. By Table 4, $q|p(1)$, 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

$$f_1(1)(57+k-d_1-k_1)+f_2(1)(57+k-d_2-k_2) = 21(11k-13). \tag{7.16}$$

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 $k = 2, f_j(t) = f_3(t)$ 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

$$(84+112)(57+2-d_1-k_1) = (21)9, \tag{7.17}$$

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 $f_3(t) \in Z[t]$, then $f_2(t)$ also belongs to $Z[t]$, which is not the case. Therefore $f_3(t) \notin Z[t]$, and this time $d_2 = d_3$, and $k_2 = k_3$.

Put $\alpha_2 = a/c$, $\alpha_3 = b/c'$ as in (5.5). Then $(a/c)+(b/c') = 1$ so $a+b = c = c'$. By (5.5), $q^k|c$, 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 $2^5 \nmid b$.

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 $\Phi_7(t)$ 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 $c = a + b \leq 1 + 16$ 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) $f_1(t) = (\frac{1}{2}) t f_1^{\#}(t)$, $f_1^{\#}(t) \in Z[t]$, $f_1^{\#}(0) = 1$, $f_1(1) = 2$. *In particular*, $f_1(2)$ *is odd, and* $3 | f_1(3)$.

(iv) $t^2 | f_2(t), f_3(t)$.

(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 $f_j(1) = 2$, then $f_j(t) = (\frac{1}{2}) t f_j^{\#}(t)$. Since the right side of (7.3) leads with $(\frac{1}{2})t$, if $i \neq j$, then $k_i \geq 2$.

Reorder the $f_i(t)$'s so that $j = 1$. Then (iii) 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 $\frac{1}{2}$, a contradiction. Thus $d_2 = d_3 = 15$, and $\alpha_2 + \alpha_3 = 1$ or $\frac{1}{2}$. This implies that $k = 2$, and $k_2 = 2$. Now (7.6) reads $f_1(1)(15 + 2 - d_1 - 1) = 11$, 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 α_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 $27 \nmid |W|$, $k = 2$. This leads to the same contradiction as before.

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

It remains only to prove (ii). We will show that $f_i(q) \geq q^7(q-1)$ 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 $\alpha_1 = \frac{1}{2}$. 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 extraspecial of order q^{15} with center U_r. Let χ be a nonprincipal irreducible constituent of 1_B^G of degree $f_i(q)$. Then χ is faithful, so there is an irreducible constituent θ of $\chi | G_1$ with $U_r \not\leq \ker \theta$. Applying Clifford's theorem, we obtain $\theta | Q_1 =$

$a(\zeta_1 + \cdots + \zeta_v)$, where $a \in Z$ and the ζ_i's are distinct conjugate irreducible characters of Q_1. Then $\zeta_j|U_r = \zeta_j(1)\varphi_j$ for a nonprincipal linear character φ_j of U_r. Moreover, one and, hence, all ζ_j's are faithful, so since Q_1 is extraspecial we must have $\zeta_j(1) = q^7$. Since H is transitive on the $q - 1$ nonprincipal characters of U_r, each such character appears as a φ_j. Thus, $\chi(1) \geq (q-1)q^7$, 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 $q = 2^a$, $f_1(q) \geq q^6(q^3-1)(q-1)$. From this it follows that $d_1 \geq 11$ and $d_2 \geq 10$.

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. $1_{G_1}^G - 1_G - \rho$ is irreducible, where ρ is the reflection character. Since $|G:G_1| \equiv 1 \pmod q$, Table 3 shows that ρ and this character have degrees divisible by p.

It is easy to check, as in §6, that $1_{G_2}^G \supset 1_{G_1}^G$ and $1_{G_2}^G - 1_{G_1}^G$ is the sum of two irreducible characters. Let $f_1(t)$ and $f_2(t)$ be the corresponding generic degrees (see (5.2)). Then

$$f_1(q) + f_2(q) = |G:G_2| - |G:G_1|. \tag{7.20}$$

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 $8|c$ and a, b odd divisors of 48. There is obviously no solution.

(7.21) LEMMA. *If G is $Sp(2n, 2)$, $n \geq 3$, then each irreducible constituent of $1_{G_2}^G - 1_{G_1}^G$ has even degree.*

PROOF. If $n \geq 4$, 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 $4|c$, $8 \nmid c$, $(a, c) = 1$, and $a, b, c\,|\,|W| = 48$. We may thus assume that $3|b$ 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 $3|b$, $3\Phi_3(1) = 9$ divides $f_2(1)$, which is a contradiction.

We remark that the degrees of the constituents of $1_{G_2}^G$ can be found in [3] when $G = Sp(2n, 2)$, $n \geq 4$.

(7.22) PROPOSITION. *Theorem* (5.7)(i) *holds when $n = 2$. More precisely, the degrees of the irreducible constituents of 1_B^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 $1_{G_i}^G$ for precisely one i.*

(i) *For $Sp(4, q)$*: $1, \frac{1}{2}q(q+1)^2, \frac{1}{2}q(q^2+1), \frac{1}{2}q(q^2+1), q^4$.

(ii) *For* $PSU(4, q)$: $1, q^2(q^2+1), q^3(q^2-q+1), q(q^2-q+1), q^6$.

(iii) *For* $PSU(5, q)$: $1, q^3(q^2+1)(q^2-q+1), q^2(q^5+1)/(q+1), q^4(q^5+1)/(q+1), q^{10}$.

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

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

(vi) *For* ${}^2F_4(q)$: 1,

$q^2(q+1)(q^2+1)(q^9+q^6+q^3+1)/4(q+\sqrt{2q}+1)(q^3-q\sqrt{2q}+1)$, $q(q^3+1)(q^6+1)/(q+1)(q^2+1)$, $q^5(q^3+1)(q^6+1)/(q+1)(q^2+1)$,

$q^2(q+1)(q^2+1)(q^9+q^6+q^3+1)/4(q-\sqrt{2q}+1)(q^3+q\sqrt{2q}+1)$, $\frac{1}{2}q^2(q^2+1)(q^6+1), q^{12}$.

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), 1_B^G 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 $1_{G_i}^G$ for $i = 1$ and 2; of the characters occurring in 1_B^G with multiplicity 1, each of the ones discussed in [12, §10] appears in $1_{G_i}^G$ for precisely one i.

Thus, consider $1_{G_1}^G$. 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 ξ_{s_2} be the corresponding element of the Hecke algebra $H(G, G_1)$. Then, with respect to the standard basis $\xi_1, \xi_{s_2}, \xi_{s_2s_1s_2}, \xi_{s_2(s_1s_2)^2}, \xi_{s_2(s_1s_2)^3}$, right multiplication by ξ_{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 $q^2(q+1), -(q+1), q^2-1$, and $q^2 \pm \sqrt{2q} - 1$. Now the proof can be completed as in (6.1)(ii).

8. **Proof of Theorem (5.8).** Replace G by the corresponding linear group $G = Sp(2n, q), SO^+(l, q)'$, 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.

$$(8.1)\qquad \begin{aligned} &(1_{G_1}^G, 1_{G_1}^G) = 3, \quad (1_{G_2}^G, 1_{G_2}^G) = 6, \quad (1_{G_{12}}^G, 1_{G_{12}}^G) = 17; \\ &(1_{G_1}^G, 1_{G_2}^G) = 3, \quad (1_{G_1}^G, 1_{G_{12}}^G) = 5, \quad (1_{G_2}^G, 1_{G_{12}}^G) = 9. \end{aligned}$$

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 $(1_{G_{12}}^G, 1_{G_{12}}^G)$ 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) i-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 τ such that $V_1^\tau - V_1$, $V_2^\tau = V_2$, $A_1^\tau = A_1'$, and $A_2^\tau = A_2'$, 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

$$1_{G_1}^G = 1_G + \rho + \chi_1 \quad \text{and} \quad 1_{G_2}^G = 1_G + \rho + \chi_1 + \chi_2 + \chi_3 + \chi_4,$$

where ρ is the reflection character and χ_1, χ_2, χ_3, and χ_4 are distinct and irreducible. By (5.4), $(\rho, 1_{G_{12}}^G) = 2$, so by (8.1), $(\chi_1, 1_{G_{12}}^G) = 2$. Then (8.1) shows that we can choose notation so that

$$1_{G_{12}}^G = 1_G + 2\rho + 2\chi_1 + 2\chi_2 + \chi_3 + \chi_4 + \chi_5 + \chi_6,$$

where $1_G, \rho, \chi_1, \chi_2, \chi_3, \chi_4, \chi_5$, and χ_6 are distinct irreducible characters of G.

Clearly G_1 induces a classical group on $V_1^\perp/V_1$, with G_{12} corresponding to the stabilizer of an isotropic 1-space. Thus, $1_{G_{12}}^{G_1} = 1_{G_1} + \sigma_1 + \sigma_2$ with σ_1 and σ_2 distinct nonprincipal irreducible characters. Then

$$(8.2)\qquad \sigma_1^G + \sigma_2^G = (1_{G_{12}}^{G_1} - 1_{G_1})^G = \rho + \chi_1 + 2\chi_2 + \chi_3 + \chi_4 + \chi_5 + \chi_6.$$

We will decompose the characters σ_1^G and σ_2^G.

By the Mackey subgroup theorem,

$$(\sigma_1^G, \sigma_2^G) = \sum_{G_1 w G_1} (\sigma_1^{w^{-1}}, \sigma_2)_{G_1^w \cap G_1}$$

where the sum ranges over the double cosets of G_1 in G. We can choose $w \in W$ with $V_1 \neq V_1 w < V_2$, so $G_1^w \cap G_1 < G_{12}$. Since $\sigma_1 | G_{12}$ and $\sigma_2 | G_{12}$ both contain $1_{G_{12}}$, it follows that $(\sigma_1^G, \sigma_2^G) > 1$. Consequently, by (8.2) both σ_1^G and σ_2^G contain χ_2

The same calculations show that, for $i = 1, 2$,

$$(1_{G_1}^G, \sigma_i^G) > (1_{G_1^w \cap G_1}, \sigma_i)_{G_1^w \cap G_1} > 1$$

(where w is as above). We can thus number the σ_i's so that $\rho \subset \sigma_1$ and $\chi_1 \in \sigma_2$

We next consider $(1_{G_2}^G, \sigma_i^G)$. There are three (G_2, G_1)-double cosets: G_2G_1, G_2xG_1, and G_2yG_1, $V_1 + (V_2)x$ is an isotropic (or singular) 3-space and $(V_1, V_2y) \neq 0$. Then $G_2^x \cap G_1$ fixes V_1 and $(V_2)x$. Since $V_1 + (V_2)x$ is an isotropic (or singular) 3-space, it follows that $G_2^x \cap G_1$ is conjugate in G_1 to a subgroup of G_{13}. Note that σ_1 and σ_2 are constituents of $1_{G_{13}}^{G_1}$, just as χ_1 and χ_2 are constituents of $1_{G_2}^G$. Thus, $(1_{G_2^x \cap G_1}, \sigma_i)_{G_2^x \cap G_1} \geq 1$ 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 $V_1 + (V_1^\perp \cap (V_2)y)$, so it is conjugate in G_1 to a subgroup of G_{12}. As before, we find that, for $i = 1, 2$,

$$(1_{G_2}^G, \sigma_i^G) = (1, \sigma_i)_{G_2 \cap G_1} + (1, \sigma_i)_{G_2^x \cap G_1} + (1, \sigma_i)_{G_2^y \cap G_1} \geq 3.$$

We can thus number the χ_i's so that $\sigma_1^G \supseteq \rho + \chi_2 + \chi_3$ and $G_2^G \supseteq \chi_1 + \chi_2 + \chi_4$.

Finally, consider $(1_{G_{12}}^G, \sigma_i^G)$. The (G_1, G_{12})-double cosets are $G_{12}G_1$, $G_{12}xG_1$, $G_{12}yG_1$, $G_{12}wG_1$, and $G_{12}zG_1$, where

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

(ii) $V_1 \nleqslant (V_2)y$ and $(V_1, (V_2)y) = 0$,

(iii) $V_1 \nleqslant (V_2)w$ and $\mathrm{rad}(V_1 + (V_2)w) = (V_1)w$, and

(iv) $V_1 \nleqslant (V_2)z$ and $\mathrm{rad}(V_1 + (V_2)z)$ is a 1-space (of $(V_2)z$) other than $(V_1)w$.

Then $G_{12}^x \cap G_1$ fixes the orthogonal 1-spaces V_1 and $(V_1)x$, so $G_{12}^x \cap G_1$ is conjugate in G_1 to a subgroup of G_{12}. Similarly, $G_{12}^w \cap G_1$ and $G_{12}^z \cap G_1$ are conjugate in G_1 to subgroups of G_{12}. Since $G_{12}^y \cap G_1$ fixes the isotropic (or singular) subspaces V_1, $V_1 + (V_1)y$, and $V_1 + (V_2)y$, it is conjugate in G_1 to a subgroup of G_{123}. Considering the group induced by G_1 on $V_1^\perp/V_1$, we find that σ_i occurs with multiplicity 2 in $1_{G_{123}}^{G_1}$ just as χ_1 and χ_2 occur with multiplicity 2 in $1_{G_{12}}^G$. (In fact, all that was needed for this was $(1_{G_{12}}^G, 1_{G_1}^G) = 5$, and this holds so long as isotropic or singular 3-spaces exist.) Consequently,

$$(1_{G_{12}}^G, \sigma_i^G) \geq 4(1, \sigma_i)_{G_{12}} + (1, \sigma_i)_{G_{123}} \geq 6.$$

We can thus number the χ_i's so that

$$\sigma_1^G = \rho + \chi_2 + \chi_3 + \chi_5 \quad \text{and} \quad \sigma_2^G = \chi_1 + \chi_2 + \chi_4 + \chi_6. \tag{8.3}$$

By (5.7), p divides $\rho(1)$, $\chi_i(1)$ for $i = 1, 2, 3, 4$, $\sigma_1(1)$ and $\sigma_2(1)$. Consequently, by (8.3) we have $p | \chi_5(1), \chi_6(1)$, 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.

$$\begin{aligned} &(1_{G_1}^G, 1_{G_1}^G) = 3, \quad (1_{G_2}^G, 1_{G_2}^G) = 5, \quad (1_{G_{12}}^G, 1_{G_{12}}^G) = 16; \\ &(1_{G_1}^G, 1_{G_2}^G) = 5, \quad (1_{G_1}^G, 1_{G_{12}}^G) = 5, \quad (1_{G_2}^G, 1_{G_{12}}^G) = 8. \end{aligned} \tag{8.4}$$

This time

$$1_{G_1}^G = 1_G + \rho + \chi_1, \quad 1_{G_2}^G = 1_G + \rho + \chi_1 + \chi_2 + \chi_3,$$

and

$$1_{G_{12}}^G = 1_G + 2\rho + 2\chi_1 + 2\chi_2 + \chi_3 + \chi_4 + \chi_5,$$

with $1_G, \rho$, and the χ_i's distinct irreducible characters of G. Define σ_1 and σ_2 as before. Then $(\sigma_1^G, \sigma_2^G) \geq 1$, so $\chi_2 \in \sigma_1^G, \sigma_2^G$. Also, $(1_{G_1}^G, \sigma_i^G) \geq 1$ for $i = 1, 2$, so we may assume that $\sigma_1^G \supset \rho + \chi_2$ and $\sigma_2^G \supset \chi_1 + \chi_2$.

Since G_1 induces a group on $V_1^\perp/V_1$ having a rank 2 (B, N)-pair, $1_{G_{13}}^{G_1}$ contains just one of σ_1, σ_2, namely, the reflection character of G_1. Let $\sigma_i \in 1_{G_{13}}^{G_1}$ and let $\sigma_j \neq \sigma_i$. As before, we find that $(1_{G_{12}}^G, \sigma_i^G) \geq 3, (1_{G_2}^G, \sigma_j^G) \geq 2, (1_{G_{12}}^G, \sigma_i^G) \geq 6$, and $(1_{G_{12}}^G, \sigma_j^G) \geq 5$. If $\sigma_i = \sigma_1$ we can renumber so that $\sigma_1^G = \rho + \chi_2 + \chi_3 + \chi_4$ and $\sigma_2^G = \chi_1 + \chi_2 + \chi_5$. If $\sigma_i = \sigma_2$, then we renumber so that $\sigma_1^G = \rho + \chi_2 + \chi_3$ and $\sigma_2^G = \chi_1 + \chi_2 + \chi_4 + \chi_5$. In either case we obtain the desired divisibility, completing the proof of (5.8).

PART II. 2-TRANSITIVE REPRESENTATIONS

9. Counting lemmas.

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 Ω, with corresponding permutation character θ. Let $\alpha \in \Omega$. Set $m = |\Omega| = \theta(1)$.

(9.1) LEMMA. *Let $P \leq G$ be transitive on Ω, and let $1 \neq Q \lhd P$. Suppose Q intersects l 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*

$$m(|Q_\alpha| - 1) = \sum_1^l c_i \theta(x_i).$$

PROOF. Each orbit of Q has size $|Q : Q_\alpha|$, while Q has $(\theta|Q, 1_Q) = |Q|^{-1}\Sigma_{x \in Q}\theta(x)$ orbits. Consequently,

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

Simplification yields the lemma.

(9.2) LEMMA. *Suppose G is 2-transitive on Ω. If $x \in G$, then $m - 1 \mid |G : C_G(x)|(\theta(x) - 1)$. In particular, if $\theta(x) = 0$ then $m - 1 \mid |G : C_G(x)|$.*

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 α to β. This follows from an easy counting argument.)

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

(10.1) LEMMA. *G_α 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 $(\chi|G, 1_B^G) \neq 0$, so $p|\chi(1)$. Thus, $p \nmid m$, so G_α^* contains a Sylow p-subgroup of G^*. By (2.3) and (10.1), G_α^* 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 $n \geqslant 2$.

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

PROOF. If B^+ is transitive then $G^+ = B^+(G^+)_\alpha$. 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. *θ is a constituent of 1_B^G, (θ, θ) divides 6, each irreducible constituent of θ is G^+-invariant, and G^* acts transitively on the nonprincipal irreducible constituents of θ.*

PROOF. By (2.6), $|G^* : G^+|\,|6$. Set $\chi = \theta^* - 1_{G^*}$ and $\chi|G^+ = \zeta_1 + \cdots + \zeta_k$ with the ζ_i irreducible. Then $k|6$ and the ζ_i are conjugate characters under the action of $G^* = G^+N(B^+)$ (by the Frattini argument). Since B^+ is intransitive, some and, hence, all ζ_i's are constituents of $1_{B^+}^{G^+}$. By (2.9), each ζ_i remains irreducible when restricted to G.

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

(10.6) LEMMA. *If $p \nmid m$, then $G = A_n(q)$, G_α is conjugate to G_1 or G_n, and the Main Theorem holds.*

PROOF. Suppose $p \nmid m$. Then we may assume that $U \leqslant G_\alpha$. By (2.3) and (10.1), G_α is a maximal parabolic subgroup. Suppose $\theta - 1_G$ is irreducible. Then there are just two (G_α, G_α)-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 $G_\alpha = G_\alpha^{xy} \geqslant B^y$, $y \in G_\alpha$ 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_α, G_α)-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_α 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_P^G for each maximal parabolic subgroup P of G. Consequently, $\theta \subset 1_P^G$ for each such P. In particular, $G \neq A_n(q)$.

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

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

(10.7) LEMMA. *p does not divide the degree of any irreducible constituent of $\theta - 1_G$, where $\theta - 1_G \subset 1_B^G$.*

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

(10.8) COROLLARY. $G \neq A_n(q)$.

PROOF. (10.7) and (5.9).

(10.9) COROLLARY. *If $n \geqslant 3$, 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 Ω. 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 $(\theta, 1_{G_{12}}^G) = 1$ for (i) and $(\theta, 1_{G_i}^G) = 1$ 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 Ω.*

(ii) *If G is $PSO^{\pm}(l, q)'$, then U_r is semiregular on Ω.*

(iii) *If G is exceptional, then U_r is semiregular on Ω.*

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 Ω. Once this is known, since $C(x)$ acts on $\Omega(x)$ we will have $\Omega(x) = \emptyset$ or Ω, so since G^* is faithful on Ω the desired semiregularity will follow.

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

Next suppose that $G = PSp(2n, q)$ (with $q \neq 2$), $PSU(l, q)$, or $PSO^{\pm}(l, q)'$, 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 $G = PSp(2n, q)$ (with $q \neq 2$) or $PSU(l, q)$, and that $X = U_s$. By (3.9), each irreducible character common to 1_B^G and $1_{C(x)}^G$ is contained in $1_{G_{12}}^G$. Thus, by (10.5) and (10.10), no irreducible constituent of $\theta - 1_G$ is a constituent of $1_{C(x)}^G$, so that $(\theta, 1_{C(x)}^G) = 1$ 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 $G_i = C(X)H$. Since H is an abelian group acting irreducibly on X, it induces a fixed-point-free group of automorphisms of X. Thus, $|G_i : C(X)| \mid q - 1$, so $|G : C(X)| \mid |G : G_i|(q - 1)$. 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* $G = Sp(2n, q)$.
(ii) $k = 2n - 1$ *if* $G = PSO(2n + 1, q)'$ *with q odd.*
(iii) $k = 2l - 2$ *if* $G = PSO^{\pm}(2l, q)'$.
(iv) $k = 2l - 3$ *if* $G = PSU(l, q)$.
(v) $k = 7$ *if* $G = F_4(q)$.
(vi) $k = 9$ *if* $G = {}^2E_6(q)$.
(vii) $k = 11$ *if* $G = E_6(q)$.
(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 $y \in Z$. 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 $G = F_4(q)$, $E_8(q)$, and $PSO^{\pm}(2l, q)'$.

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 $0 \leqslant z \in Z$. 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 $(q^7(q^3+1)-1)q^7 < (q^4+1)q^{12}$, which is impossible.

Since $q^7x - 1 | (q^4+1)(q^{12}-1)x$ implies that $q^7 x - 1 | (q^4+1)(q^5 - x)$, we can write $(q^4+1)(q^5-x) = (q^7x-1)v$ with $v \in Z$. Rewrite this $v + q^5 = (q^4+1)x + q^7(xv - q^2)$. If $xv > q^2$, then $v + q^5 \geqslant (q^4+1)x + q^7 > q^7$, so $v > q^5$ and $(q^4+1)(q^5-x) > (q^7x-1)q^5$, which is impossible. Also, since x is not a power of p, $xv \neq q^2$. Thus, $xv < q^2$, 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. $G = E_8(q)$. 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 $z \in Z$. We first show that $z > 0$. For otherwise, $z = 0$ and

$$q^{24} - q^{10} - 1 | (q^{10}+1)(q^{24}-1)(q^{30}-1).$$

However, $q^{24} - q^{10} - 1$ is relatively prime to $q^{10}+1$ and $q^{24}-1$, so $1 \equiv q^{30} \equiv q^6(q^{10}+1) \pmod{q^{24} - q^{10} - 1}$, which is clearly false. Thus, $z \geqslant 1$, and (10.14) yields $x \leqslant q^{10}$. Multiplying the right side of (10.14) by $-q^5x^2$ and taking congruences mod $q^{29}x - 1$, we find that $q^{29}x - 1 | (q^{10}+1)(-1+q^5x)(q-x)$. Then $x > q$ (since $x \neq q$ by (10.4)), and hence $q^{29}x - 1 \leqslant (q^{10}+1)q^5x^2 - 1$. It follows that $q^{29} \leqslant (q^{10}+1)q^5 x \leqslant (q^{10}+1)q^{15}$, which is impossible.

3. $G = PSO^{\pm}(2l, q)'$. Here

$$(q^{2l-2}x - 1)y = (q^l \pm 1)(q^{l-1} \mp 1)(q^{l-1} \pm 1)(q^{l-2} \mp 1)/(q^2-1).$$

Taking congruences mod q^{2l-2}, we find that $y(q^2-1) = q^{2l-2}z \mp q^l \pm q^{l-2} - 1$ with $z \in Z$. Then $z \equiv 1 \pmod{q^2-1}$, so that $z \geqslant 1$. By (10.4), $x > 1$. Thus,

$$(q^{2l-2}-1)(q^{2l-2} \mp q^l \pm q^{l-2} - 1) < (q^{2l-2}-1)(q^l \pm 1)(q^{l-2} \mp 1),$$

which is impossible.

11. **The classical groups.** The proof of the Main Theorem will be completed in §§11–13. In this section we assume that G is a classical group and W has rank $\geqslant 3$. Frequent use will be made of §3. Recall that q is a prime by (10.9).

(11.1) LEMMA. $G \neq PSp(2n, q), q > 2$.

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

By (10.11), U_r and U_s are semiregular in Ω. Again by (3.2), U_sU_r/U_r corresponds to an isotropic 1-space of Q_1/U_r, 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 Ω. Then $q^{2n-1} | m$, contradicting (10.13).

(11.2) LEMMA. $G \neq PSO^{\pm}(l, q)$.

PROOF. Suppose G is $PSO^{\pm}(l, q)$. By (11.1), q is odd if l is odd. $L_1 = SO^{\pm}(l-2, q)'$ acts on the elementary abelian group Q_1 of order q^{l-2} in the natural manner as a group of $\mathbf{F}_q$-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 $(Q_1)_\alpha$ is a nontrivial subspace of Q_1; moreover, it must be anisotropic (or nonsingular). Consequently, $|(Q_1)_\alpha| \leqslant q^2$ 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 $\Omega(v)$ of fixed points is nonempty. Since Q_1 acts on $\Omega(v)$, $q^{l-4} | |\Omega(v)|$. 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 $l \geqslant 7$, it follows that $q^{l-2} | m$. This contradicts (10.13).

(11.3) LEMMA. $G \neq PSU(l, q)$.

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

By (10.11), $Z(U_r)$ and U_s are semiregular, but by (10.13), Q_1 is not semiregular. Take $1 \neq g \in Q_1$ with a nonempty set $\Omega(g)$ 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 $\alpha \in \Omega(g)$ we have $T_\alpha \cap Z(T) = 1$. Then T_α is abelian, so $|T_\alpha| \leqslant q^{l-3}$. Consequently, $q^{l-2} | |\Omega(g)|$. Also, $gZ(Q_1)$ is an anisotropic vector of the $\mathbf{F}_{q^2}$-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 $q^{l-1} | |L_1 : C_{L_1Q_1}(g)|$. By (9.1) (applied to $P = G_1$, which is transitive by (10.10)), $q^{l-1}q^{l-2} | m$. 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 is $E_6(q)$, $E_7(q)$, 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 Ω, where $i = 2, 1$, or 8, respectively. Consequently, for all $\alpha \in \Omega$, $(Q_i)_\alpha$ contains no nontrivial element of a root group.

By (4.4), Q_i is extraspecial of order q^{21}, q^{33}, or q^{57}, respectively. Since $(Q_i)_\alpha \cap Z(Q_i) = 1$, it follows that $(Q_i)_\alpha$ is abelian, and hence (from the theory of extraspecial groups) that $|(Q_i)_\alpha| \leqslant \sqrt{|Q_i|/q}$. Then $|Q_i : (Q_i)_\alpha|$ is divisible by q^{11}, q^{17}, or q^{29}, respectively. Since α 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 Ω by (10.11), all nontrivial isotropic vectors in R_4 are semiregular. R_4 is not semiregular, as otherwise $3^7 | m$, 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 $\langle v \rangle^\perp$, so that $C_{L_4}(v) \approx O^\pm(6, 3)$, and consequently R_4 contains $3^3 z$ conjugates of v under the action of L_4, where $z \in Z$. Clearly, R_4 centralizes v and acts on $\Omega(v)$. If v fixes α, then $(R_4)_\alpha$ contains no nonzero isotropic vector, so $|(R_4)_\alpha| \leqslant 3^2$. Thus, $3^5 \mid |\Omega(v)|$. Now (9.1) implies that $3^3 \cdot 3^5 | m$, 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 Ω. Thus, for each $\alpha \in \Omega$, $(Q_1)_\alpha$ is abelian, and consequently $|(Q_1)_\alpha| \leqslant q^{10}$. Then $q^{11} | m$, 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_B^G are $1, 3^6, 91, 91, 104$ and 168. Since $\theta - 1_G$ decomposes into 1 or 2 irreducible constituents of 1_B^G of the same degree not divisible by $q = 3$, we must have $m - 1 = \theta(1) - 1 = 91, 104$, or $2 \cdot 91$. Then $m \nmid |G_2(3)|$, which is a contradiction.

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

(13.2) LEMMA. $G \neq F_4(2)$.

PROOF. Define $f_1(t)$ as in (7.19), so $9 \leqslant \deg f_1 \leqslant 15$. As usual, let ρ be the reflection character of G. Then by Table 4, $\rho(1) + 1 \nmid |F_4(2)|$. If $1_{G_\alpha}^G = 1 + \zeta_1 + \zeta_2$ with ζ_1, ζ_2 conjugate characters, them $m = |G : G_\alpha|$ 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), $f_1(t) = \frac{1}{2} t f_1^{\#}(t)$, where $3 \leqslant \deg f_1^{\#} \leqslant 15$ and (by (5.5))

$$f_1^{\#}(t) | (t + 1)^4 (t^2 + 1)^2 (t^4 + 1)(t^2 + t + 1)^2 (t^2 - t + 1)^2 (t^4 - t^2 + 1). \tag{13.3}$$

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), χ is not contained in both $1_{G_1}^G$ and $1_{G_4}^G$, so that G_1 or G_4 is transitive on Ω. 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 $t + 1, t + 1, t^2 + 1, t^2 + 1, t^4 + 1$. In view of (13.3) and $\deg f_1^{\#} \geqslant 8$, 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 $f_1^{\#}(t) = (t^2 - t + 1)(t^2 + 1)(t^4 + 1)$. 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_α is $GO^{\pm}(2n, 2)$.*

PROOF. We may assume $n \geqslant 3$. 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 $(\theta, 1_{G_1}^G) > 1$. Since $\theta - 1_G$ is irreducible, $\theta \subset 1_{G_1}^G$.

Consequently, θ 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_α: just count the pairs (x, α) with x a transvection in G_α. Since this is also true of the representation of G on the cosets of $GO^{\pm}(2n, 2)$, G_α contains $2^{n-1}(2^n \mp 1)$ transvections.

Regard G as acting as usual on a $2n$-dimensional vector space V. The subgroup X of G_α generated by its transvections is irreducible. For suppose M is an X-invariant e-space of V with $1 \leqslant e \leqslant 2n - 1$. 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_α fixes M. Then $|G_\alpha| \leqslant |G_1|$, which is not the case.

From [25] it follows that G_α is contained in an orthogonal group, so the maximality of G_α 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 ${}^2F_4(2)'$ has no faithful 2-transitive permutation representation.*

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

As $G = G'B = G'U$, $(\lambda, 1_B^G) = 0$, while $(1_{G'_\alpha}^G, 1_B^G) > 1$ by (2.10). We may assume that χ is a constituent of 1_B^G. Clearly $2|\Omega| = 2 + \chi(1)$ or $2 + 2\chi(1)$ must divide $|G|$. By (7.26), $\chi(1) = 2^{12}, 2 \cdot 5^2 \cdot 13, 3^3 \cdot 5^2, 3^3 \cdot 13, 2 \cdot 3 \cdot 13$, or $2^5 \cdot 3 \cdot 13$. It follows that $\chi(1) = 2 \cdot 3 \cdot 13$, $|\Omega| = 40$, and $1_{G'_\alpha}^G = 1_G + \lambda + \chi$. Let Ω^* be the set of right cosets of G'_α in G.

In the notation of [12], $\chi = d_{\sigma_2}(2)$. In particular, χ 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 Ω. Choose the notation so that G_1 is transitive. Then $5 \mid |G_1|$.

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 $G_1 = Q_1L_1$ is transitive on Ω, where $|\Omega^*| = 80$, so a Sylow 5-subgroup of G_1 must be semiregular on Ω^*. On the other hand, $|G : G'_\alpha| = 80$ implies that $5 \mid |G'_\alpha|$, so some element of G' of order 5 fixes α. 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 $[L_1, L_1^{s_1s_2s_1}] = 1$, where $L_1 \cap L_1^{s_1s_2s_1} = 1$. Set $M = (L_1 \times L_1^{s_1s_2s_1})\langle s_1s_2s_1\rangle$. 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 $U_2^{s_1s_2s_1}$ of $N_G(F)$ centralizes some involution $v \in C_G(F)$. According to [17, (10.3)(iii)], $U_2^{s_1s_2s_1}$ contains the central involution t of G_1, so that $G_1 = C_G(t)$ as G_1 is maximal in G. Thus, $v \in C(t) = G_1$, so $v \in C_{G_1}(F \cap G_1) = C_{G_1}(O_5(L_1))$. However, $C_{G_1}(O_5(L_1)) = O_5(L_1) \times U_2^{s_1s_2s_1}$ (this follows from [17, §10], in particular, from the paragraphs following (10.3) and (10.10)). Then $v \in U_2^{s_1s_2s_1}$, whereas $U_2^{s_1s_2s_1}$ is fixed-point-free on $F \cap L_1^{s_1s_2s_1}$.

Thus, $|C_G(F)|$ is odd. Since $|GL(2, 5)| = 2^5 \cdot 3 \cdot 5$, 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 $N_G(F) \leqslant N_G(X)$. 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 $3 \mid |C_G(F)|$. Then $C_G(F) = F \times X$. With the same notation as before, $t \in U_2^{s_1s_2s_1} \leqslant N_G(X)$ and $|U_2^{s_1s_2s_1}| = 4$ imply that $t \in C(X)$. Then $X \leqslant C_G(t) = G_1$, 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 $1 + \chi(1)$ (and $1 + 2\chi(1)$ in the case $G_2(3)$) does not divide $|G|$, whenever χ is an irreducible constituent of $1_B^G - 1_G$ such that $p \nmid \chi(1)$. Finally, handle $Sp(2n, 2)$ as in (13.4).

REFERENCES

1. E. Artin, *Geometric algebra*, Interscience, New York and London, 1957. MR 18, 553.

2. E. Bannai, *Doubly transitive permutation representations of the finite projective special linear groups* PSL(n, q), Osaka J. Math. 8 (1971), 437–445. MR 47 #1966.

3. ———, *On some subgroups of the group* Sp($2n$, 2), Proc. Japan Acad. 47 (1971), 769–773. MR 46 #5472.

4. ———, *On some subgroups of the group* $\mathrm{PS_p}(2n, q)$, Proc. Japan Acad. 48 (1972), 43–48.

5. C. T. Benson and C. W. Curtis, *On the degrees and rationality of certain characters of finite Chevalley groups*, Trans. Amer. Math. Soc. 165 (1972) 251–273. MR 46 #3608.

6. D. M. Bloom, *The subgroups of* PSL(3, q) *for odd* q, Trans. Amer. Math. Soc. 127 (1967), 150–178. MR 35 #5520.

7. A. Borel and J. Tits (unpublished manuscript).

8. N. Bourbaki, *Éléments de mathématique. Fasc.* XXXIV, *Groupes et algèbres de Lie*, Chaps. 4, 5, 6, Actualités Sci. Indust., no. 1337, Hermann, Paris, 1968. MR 39 #1590.

9. R. Carter, *Simple groups and simple Lie algebras*, J. London Math. Soc. 40 (1965), 193–240. MR 30 #4855.

10. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. (2) 7 (1955), 14–66. MR 17, 457.

11. R. J. Clarke, Ph.D. Thesis, University of Warwick, 1965.

12. C. W. Curtis, N. Iwahori, and R. Kilmoyer, *Hecke algebras and characters of parabolic type of finite groups with* (B, N)*-pairs*, Publ. Math. 40 (1972), 81–116.

13. C. W. Curtis and T. V. Fossum, *On centralizer rings and characters of representations of finite groups*, Math. Z. 107 (1968), 402–406. MR 38 #5946.

14. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. 11, Interscience, New York and London, 1962. MR 26 #2519.

15. J. Dieudonné, *La géométrie des groupes classiques*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Heft 5, Springer-Verlag, Berlin, 1955. MR 17, 236.

16. W. Feit and G. Higman, *The nonexistence of certain generalized polygons*, J. Algebra 1 (1964), 114–131. MR 30 #1189.

17. P. Fong and G. M. Seitz, *Groups with a* (B, N)*-pair of rank* 2. I, II, Invent. Math. 21 (1973), 1–57; 24 (1974), 191–239.

18. D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968. MR 38 #229.

19. J. A. Green, *On the Steinberg characters of finite Chevalley groups*, Math. Z. 117 (1970), 272–288. MR 43 #6331.

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

21. D. G. Higman, *Intersection matrices for finite permutation groups*, J. Algebra **6** (1967), 22–42. MR **35** #244.

22. N. Itô, *Über die Gruppen* $PSL_n(q)$, *die eine Untergruppe von Primzahlindex enhalten*, Acta.Sci. Math. (Szeged) **21** (1960), 206–217. MR **26** #184.

23. R. Kilmoyer, *Some irreducible complex representations of a finite group with a* (B, N)*-pair*, Ph.D. Thesis, M. I. T., 1969.

24. H. Lüneburg, *Charakterisierungen der endlichen desarguesschen projektiven Ebenen*, Math. Z. **85** (1964), 419–450. MR **29** #5153.

25. J. McLaughlin, *Some subgroups of* $SL_n(F_2)$, Illinois J. Math. **13** (1969), 108–115. MR **38** #5941.

26. H. H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911), 207–242.

27. E. T. Parker, *A simple group having no multiply transitive representation*, Proc. Amer. Math. Soc. **5** (1954), 606–611. MR **16**, 110.

28. D. Perin, *On collineation groups of finite projective spaces*, Math. Z. **126** (1972), 135–142. MR **47** #5715.

29. F. C. Piper, *On elations of finite projective spaces of odd* (*even*) *order*, J. London Math. Soc. **41** (1966), 641–648; ibid., **43** (1968), 459–464. MR **34** #1912; **37** #2082.

30. R. Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc. **84** (1957), 392–400. MR **19**, 247.

31. F. Richen, *Modular representations of split B, N pairs*, Trans. Amer. Math. Soc. **140** (1969), 435–460. MR **39** #4299.

32. G. M. Seitz, *Flag-transitive subgroups of Chevalley groups*, Ann. of Math. **97** (1973), 27–56.

33. R. Steinberg, *A geometric approach to the representations of the full linear group over a Galois field*, Trans. Amer. Math. Soc. **71** (1951), 274–282. MR **13**, 317.

34. ———, *Variations on a theme of Chevalley*, Pacific J. Math. **9** (1959), 875–891. MR **22** #79.

35. ———, *Automorphisms of finite linear groups*, Canad. J. Math. **12** (1960), 606–615. MR **22** #12165.

36. ———, *Lectures on Chevalley groups*, Lecture Notes, Yale Univ., 1967.

37. M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962), 105–145. MR **25** #112.

38. J. H. Walter, *Finite groups with abelian Sylow* 2*-subgroups of order* 8, Invent. Math. **2** (1967), 332–376. MR **36** #1531.

39. H. N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89. MR **33** #5752.

40. H. Wielandt, *Finite permutation groups*, Lectures, Univ. of Tübingen, 1954/55; English transl., Academic Press, New York and London, 1964. MR **32** #1252.

ADDED IN PROOF

41. C. T. Benson and D. A. Gay, *On dimension functions of the generic algebra of type* D_n (to appear).

42. C. T. Benson, L. C. Grove and D. B. Surowski, *Semilinear automorphisms and dimension functions for certain characters of finite Chevalley groups*, Math. Z. **144** (1975), 149–159.

43. P. N. Hoefsmit, *Representations of Hecke algebras of finite groups with BN-pairs of classical type*, Ph.D. Thesis, University of British Columbia, 1974.

44. R. B. Howlett, *On the degrees of Steinberg characters of Chevalley groups*, Math. Z. **135** (1974), 125–135.

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