A FIXED-POINT FORMULA FOR THE CLASSICAL GROUPS OVER A FINITE FIELD

BY
LOUIS SOLOMON(1)

1. **Introduction and statement of results.** Let K be a field of characteristic zero, let E be an n-dimensional vector space over K and let $\boldsymbol{G}$ be a finite group of linear transformations of E generated by reflections. If g_r is the number of elements of $\boldsymbol{G}$ with an $(n-r)$-dimensional fixed-point set then [9] there exist integers $m_1, \cdots, m_n$ such that

$$\sum_{r=0}^{n} g_r t^r = \prod_{i=1}^{n} (1 + m_i t), \tag{1.1}$$

where t is an indeterminate. In this paper we consider the possible existence of such formulas for the unitary, symplectic, and orthogonal groups over a finite field. The question is a natural one since we know next to nothing about reflection groups in characteristic $p > 0$, and the classical groups defined by a sesquilinear form are all generated by elements which fix a hyperplane. The results, roughly stated, are that such formulas exist if and only if the Witt index of the form is 0 or 1. Although there are similarities in the statements and proofs for the unitary, symplectic and orthogonal cases, it is awkward to try to handle them together. In the following theorems we consider n to be fixed and let q vary over the set of prime powers.

THEOREM 1. *Let E be an n-dimensional vector space over $\boldsymbol{F}_{q^2}$ with a non-singular sesquilinear form which is hermitian with respect to the automorphism $\alpha \to \alpha^q$ of $\boldsymbol{F}_{q^2}$. Let $\boldsymbol{G}(q) = \boldsymbol{U}(n, q^2)$ be the unitary group and let $g_r(q)$ be the number of elements of $\boldsymbol{G}(q)$ with an $(n-r)$-dimensional fixed-point set. There is a formula*

$$\sum_r g_r(q) t^r = \prod_i (1 + m_i(q)t), \qquad m_i(q) \in \boldsymbol{Z}, \tag{1.2}$$

for each prime power q, if and only if the index of E is 0 or 1.

For the symplectic group the index cannot be 0 and the dimension n is even.

THEOREM 2. *Let E be an n-dimensional vector space over $\boldsymbol{F}_q$ with a non-singular alternating bilinear form. Let $\boldsymbol{G}(q) = \boldsymbol{Sp}(n, q)$ be the symplectic group*

Presented to the Society, August 30, 1963; received by the editors July 29, 1963.
(1) This research was supported by the National Science Foundation under grant G-21514.

and let $g_r(q)$ be the number of elements of $G(q)$ with an $(n-r)$-dimensional fixed-point set. There is a formula (1.2) *for each prime power q, if and only if the index of E is* 1.

The theorem for the orthogonal group requires a little more care in its proof, because there are two distinct types [1] of orthogonal geometry for each pair (n, q). We assume that q is odd.

THEOREM 3. *Let E be an n-dimensional vector space over F_q with a non-singular symmetric bilinear form Φ_q, where the forms Φ_q are, for varying q, of some fixed type. Let $G(q) = O(n, q, \Phi_q)$ be the orthogonal group and let $g_r(q)$ be the number of elements of $G(q)$ with an $(n-r)$-dimensional fixed-point set. There is a formula* (1.2), *for each odd prime power q, if and only if the index of E is* 0 *or* 1.

The main tool in the proofs is a counting argument which uses an analogue for finite groups of the Möbius inversion formula. With this inversion formula and Witt's theorem we show, by computing the orders of certain subgroups of $G(q)$, that $g_r(q)$ is a monic polynomial in q with integer coefficients. The method yields the degree of $g_r(q)$. With this information and Hilbert's irreducibility theorem, we show that if the $m_i(q)$ exist, they are polynomials in q of known degree with integer coefficients. We conclude that the $m_i(q)$ can exist only in low dimensions and settle the cases in low dimensions by explicit computations. We exhibit the $m_i(q)$ when they exist.

The results are disappointing in that one has analogues of (1.1) in dimension at most four. One might hope for some substitute for (1.2) in case the index v is greater than 1. The evidence for $v = 0, 1, 2$ suggests that, in general, the polynomial $\sum_i g_r(q)t^i$ has $n - v$ linear factors of the form $1 + q^i t$, where the positive integers i are given by

$$i = 1, 3, \cdots, 2(n-v)-1, \qquad \text{if } G(q) \text{ is unitary,}$$

$$i = 1, 2, \cdots, n-v, \qquad \text{if } G(q) \text{ is symplectic,}$$

$$i = 0, 1, \cdots, n-v-1, \qquad \text{if } G(q) \text{ is orthogonal.}$$

The simple counting arguments of this paper are not strong enough to prove such a theorem(2). In characteristic zero, the integers $1 + m_i$ are the degrees of certain basic polynomial invariants [3] of G. We have shown in [10] that this information leads to a proof of (1.1). As for the groups $G(q)$, the endomorphism $x_i \to x_i^q$ of the ring $F_q[x_1, \cdots, x_n]$ of polynomial forms on E ($x_i \to x_i^{q^2}$, $F_{q^2}[x_1, \cdots, x_n]$, in the unitary case) may be used to construct, from the given invariant sesquilinear form, a set of $n-v$ algebraically independent invariant polynomial forms of the "correct" degrees $1+q$. This makes it seem plausible that information about the

(2) William Johnston has verified this conjecture on an IBM machine in case $G(q)$ is symplectic, v is 3 or 4, and q is small.

polynomial invariants of $G(q)$ may provide a substitute for (1.2) in case the index is greater than 1.

2. **Notation, and collection of known facts.** If S is a finite set we let $|S|$ denote the number of elements in S. We use $S \subseteq T$ to denote inclusion and $S \subset T$ to denote proper inclusion of sets. We let $\boldsymbol{F}_q$ denote the field of q elements, $\boldsymbol{R}$ the field of real numbers, and $\boldsymbol{Z}$ the ring of integers. If f is an $\boldsymbol{R}$-valued function, defined on the set of prime powers q, we say that $f(q)$ is a polynomial in q if f may be extended to a polynomial function on $\boldsymbol{R}$. To avoid a cluttered notation we often omit a subscript q which should be attached to spaces or forms over $\boldsymbol{F}_q$.

If E is an n-dimensional vector space over $\boldsymbol{F}_q$ we let $\boldsymbol{GL}(E) = \boldsymbol{GL}(n,q)$ denote the general linear group. Subspaces of E will be denoted $A, B, C, \cdots, V, W, X, \cdots$. If $\gamma \in \boldsymbol{GL}(E)$ and A is a subspace of E, we let $\gamma | A$ denote the restriction of γ to A. We let $\delta(A)$ denote the dimension of A and write $\nu(A)$ for the binomial coefficient $\binom{\delta(A)}{2}$. The letters $L, M, \cdots, P, Q, \cdots$ denote matrices with coefficients in $\boldsymbol{F}_q$ or $\boldsymbol{F}_{q^2}$. We let ${}^tL$ denote the transpose of L. We let $\bar{L}$ denote the conjugate of L with respect to the involutory automorphism $\alpha \to \alpha^q$ of $\boldsymbol{F}_{q^2}$.

Let E be an n-dimensional vector space with a nonsingular sesquilinear form Φ. We write $A \perp B$ for a Witt sum of two subspaces A, B of E, that is, a direct sum in which A, B are orthogonal with respect to Φ. We let rad A denote the singular part of A, the subspace of all $\xi \in A$ such that $\Phi(\xi, \eta) = 0$ for all $\eta \in A$. The subspace A is isotropic if and only if rad $A \neq 0$ and totally isotropic if and only if rad $A = A$. The Witt index of Φ is the dimension of a maximal totally isotropic subspace of E. The restriction Φ_A of Φ to A defines a geometry in A. We let $\boldsymbol{U}(A), \boldsymbol{Sp}(A), \boldsymbol{O}(A)$ denote, in the three cases, the subgroups of $\boldsymbol{GL}(A)$ which leave Φ_A invariant. Since Φ_A may be singular these need not be the unitary, symplectic, and orthogonal groups in the usual sense.

We collect here some information about the classical groups over a finite field. The group $\boldsymbol{GL}(E) = \boldsymbol{GL}(n,q)$ has order

$$|\boldsymbol{GL}(n,q)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1), \tag{2.1}$$

which is a polynomial in q of degree n^2 with coefficients in $\boldsymbol{Z}$. In the unitary case there exists a nonsingular hermitian form on E which is unique up to equivalence under the natural action of $\boldsymbol{GL}(E) = \boldsymbol{GL}(n, q^2)$. The index of E is $n/2$ if n is even and $(n-1)/2$ if n is odd. The group $\boldsymbol{U}(E) = \boldsymbol{U}(n, q^2)$ has order

$$|\boldsymbol{U}(n,q^2)| = q^{n(n-1)^2} \prod_{i=1}^{n} (q^i - (-1)^i), \tag{2.2}$$

which is a polynomial in q of degree n^2. In the symplectic case there exists, for even n, a nonsingular alternating bilinear form on E which is unique up to equivalence. The index of E is $n/2$. The group $\boldsymbol{Sp}(E) = \boldsymbol{Sp}(n,q)$ has order

$$|Sp(n,q)| = q^{(n/2)^2} \prod_{i=1}^{n/2} (q^{2i}-1), \tag{2.3}$$

which is a polynomial in q of degree $n(n+1)/2$. For given (n,q) with q odd, the inequivalent nonsingular symmetric bilinear forms Φ on E may be separated into four types according to the following scheme:

Type	n	Discriminant	Index
I	odd	$(-1)^{(n-1)/2}$	$(n-1)/2$
II	odd	$(-1)^{(n-1)/2}\omega$	$(n-1)/2$
III	even	$(-1)^{n/2}$	$n/2$
IV	even	$(-1)^{n/2}\omega$	$n/2-1$,

where ω is a nonsquare in F_q. The group $O(E) = O(n,q,\Phi)$ has order

$$\begin{aligned} |O(n,q,\Phi)| &= 2q^{(n-1)^2/4} \prod_{i=1}^{(n-1)/2} (q^{2i}-1), && \text{Types I, II} \\ |O(n,q,\Phi)| &= 2q^{n(n-2)/4} (q^{n/2}-\varepsilon) \prod_{i=1}^{(n-2)/2} (q^{2i}-1), && \text{Types III, IV,} \end{aligned} \tag{2.4}$$

where $\varepsilon = +1$ for type III and $\varepsilon = -1$ for type IV. For a given type the order $|O(n,q,\Phi)|$ is a polynomial in q of degree $n(n-1)/2$. The groups corresponding to types I, II are isomorphic. For proofs of these facts and references to the ideas which center around Witt's theorem see [1], [2], [4].

3. **The counting argument.** Let E be an n-dimensional vector space over F_q and let G be a subgroup of $GL(E)$. If A is a subspace of E we let $K(A)$ denote the subgroup of G which consists of those elements of G which fix every vector in A. We are interested in the number of elements of G which have A for fixed-point set. The following proposition allows us to compute this number in terms of the orders of subgroups $K(B)$ for the subspaces B which include A.

PROPOSITION 1. *Let E be an n-dimensional vector space over F_q and let G be a subgroup of $GL(E)$. Let A be a subspace of E. The number of elements of G which have A for fixed-point set is equal to*

$$\sum_{A \subseteq B \subseteq E} (-1)^{\delta(B/A)} q^{\nu(B/A)} |K(B)|,$$

where the sum is over all subspaces B of E which include A.

To prove Proposition 1 we use an inversion formula analogous to the Möbius inversion formula of elementary number theory. This method of enumeration was discovered by Weisner [11] and P. Hall [7]. Let E be a finite group and let ϕ

be an R-valued function which has for domain the set of subgroups of E. Let ψ be the summatory function derived from ϕ, defined for a subgroup B of E by

$$\psi(B) = \sum_{C \subseteq B} \phi(C), \tag{3.1}$$

where the sum is over the set of all subgroups C of E which are included in B. Then we have the inversion formula

$$\phi(E) = \sum_{A} \mu(E, A)\psi(A), \tag{3.2}$$

where the sum is over all subgroups A of E and the Möbius function μ is defined recursively by

$$\mu(E, E) = 1, \tag{3.3}$$

$$\sum_{B \supseteq A} \mu(E, B) = 0 \quad \text{if} \quad A \subset E. \tag{3.4}$$

In case E is an elementary abelian p-group, Weisner [11] and Hall [6] have shown that the function μ is given by

$$\mu(E, A) = (-1)^{\delta(E/A)} p^{\nu(E/A)}. \tag{3.5}$$

All the formulas (3.1)–(3.5) are valid in case E is a finite-dimensional vector space over F_q and the sums are taken over subspaces of F_q.

LEMMA 1. *Let E be a finite-dimensional vector space over F_q and let $X(E)$ be the free (additive) abelian group generated by symbols $[A]$ which are in one-to-one correspondence with the subspaces A of E. Let $V_1, \cdots, V_s$ be the one-dimensional subspaces of E. In $X(E)$ we have the formula*

$$\sum_{k=1}^{s} (-1)^k \sum_{i_1 < \cdots < i_k} [V_{i_1} + \cdots + V_{i_k}] = \sum_{A} (-1)^{\delta(A)} q^{\nu(A)} [A],$$

where the sum on the right is over all the nonzero subspaces A of E.

Proof. If A is a finite-dimensional vector space over F_q, let $\rho(A)$ be the number of one-dimensional subspaces of A. Let $\tau_k(A)$ be the number of sets $\{W_1, \cdots, W_k\}$ of k distinct one-dimensional subspaces of A such that $A = W_1 + \cdots + W_k$. Then

$$\sum_{B \subseteq A} \tau_k(B) = \binom{\rho(A)}{k},$$

and from the inversion formula (3.2) it follows that

$$\tau_k(A) = \sum_{B \subseteq A} \mu(A, B) \binom{\rho(B)}{k}.$$

Set

$$\zeta = \sum_{k=1}^{s} (-1)^k \sum_{i_1 < \cdots < i_k} [V_{i_1} + \cdots + V_{i_k}].$$

Then

$$\zeta = \sum_{k=1}^{s} (-1)^k \sum_{0 \subset A \subseteq E} \tau_k(A)[A]$$

$$= \sum_{k=1}^{s} (-1)^k \sum_{0 \subset A \subseteq E} \sum_{B \subseteq A} \mu(A,B) \binom{\rho(B)}{k} [A].$$

Since $s = \rho(A) \geqq \rho(B)$ it follows that

$$\sum_{k=1}^{s} (-1)^k \binom{\rho(B)}{k} = \begin{cases} 0 & \text{if } B = 0, \\ -1 & \text{if } B \neq 0. \end{cases}$$

Thus

$$\zeta = - \sum_{0 \subset A \subseteq E} \sum_{0 \subset B \subseteq A} \mu(A,B)[A].$$

Now from (3.4) and (3.5) we have

$$- \sum_{0 \subset B \subseteq A} \mu(A,B) = \mu(A,0) = (-1)^{\delta(A)} q^{\nu(A)},$$

so that

$$\zeta = \sum_{0 \subset A \subseteq E} (-1)^{\delta(A)} q^{\nu(A)} [A],$$

and this proves the lemma.

LEMMA 2. *Let E be a finite-dimensional vector space over F_q and let A be a subspace of E. Let $V_1, \cdots, V_s$ be the subspaces of E such that $V_i \supset A$ and $\delta(V_i / A) = 1$. Let ϕ be an R-valued function which has for domain the set of subspaces of E. Then*

$$\sum_{k=1}^{s} (-1)^k \sum_{i_1 < \cdots < i_k} \phi(V_{i_1} + \cdots + V_{i_k}) = \sum_{A \subset B \subseteq E} (-1)^{\delta(B/A)} q^{\nu(B/A)} \phi(B),$$

where the sum on the right is over all subspaces B of E which include A properly.

Proof. We have a one-to-one correspondence $B \leftrightarrow \tilde{B}$ between subspaces B of E which include A and subspaces $\tilde{B}$ of $\tilde{E} = E / A$. The subspaces $\tilde{V}_i$ are the one-dimensional subspaces of $\tilde{E}$. Define $\tilde{\phi}$, an R-valued function on the set of subspaces of $\tilde{E}$, by $\tilde{\phi}(\tilde{B}) = \phi(B)$. The function $\tilde{\phi}$ may be extended uniquely to a Z-linear function on the free abelian group $X(\tilde{E})$ and Lemma 2 follows at once from Lemma 1.

To prove Proposition 1 we apply Lemma 2 to the function ϕ defined by $\phi(A) = |\, \boldsymbol{K}(A)\,|$. Let $V_1, \cdots, V_s$ be the subspaces of E such that $V_i \supset A$ and such that $\delta(V_i/A) = 1$. An element $\gamma \in G$ has A for fixed-point set if and only if γ lies in $\boldsymbol{K}(A)$ but not in any $\boldsymbol{K}(V_i)$. Thus the number of elements which have A for fixed-point set is

$$
\begin{aligned}
&|\, \boldsymbol{K}(A)\,| - \Big|\, \bigcup_{k=1}^{s} \boldsymbol{K}(V_i)\,\Big| \\
&\quad = |\, \boldsymbol{K}(A)\,| - \sum_{k=1}^{s} (-1)^{k+1} \sum_{i_1 < \cdots < i_k} |\, \boldsymbol{K}(V_{i_1}) \cap \cdots \cap \boldsymbol{K}(V_{i_k})\,| \\
&\quad = |\, \boldsymbol{K}(A)\,| + \sum_{k=1}^{s} (-1)^{k} \sum_{i_1 < \cdots < i_k} |\, \boldsymbol{K}(V_{i_1} + \cdots + V_{i_k})\,| \\
&\quad = |\, \boldsymbol{K}(A)\,| + \sum_{A \subset B \subseteq E} (-1)^{\delta(B/A)} q^{\nu(B/A)} |\, \boldsymbol{K}(B)\,|,
\end{aligned}
$$

which is equivalent to the statement of Proposition 1.

4. **The Hilbert irreducibility theorem.** We need this theorem in a form proved by Dörge [5], [8]. Let x, t be indeterminates and let $g(x,t) \in \boldsymbol{Z}[x,t]$. Let Δ be the set of those positive integers n such that $g(n,t)$ is reducible in $\boldsymbol{Z}[t]$. If n is a positive integer, let $\Delta(n)$ be the number of elements in Δ which are $\leqq n$. Dörge has shown that, if $g(x,t)$ is irreducible in $\boldsymbol{Z}[x,t]$, then there exists a positive real number α, such that $\Delta(n)/n^{1-\alpha} \to 0$ as $n \to \infty$.

Suppose Δ includes the set of primes. Since the number of primes $\leqq n$ is at least $cn/\log n$ for some positive c, we have $\Delta(n)/n^{1-\alpha} \geqq cn^{\alpha}/\log n$, so that $\Delta(n)/n^{1-\alpha} \to \infty$ for all positive α. We conclude that if $g(q,t)$ is reducible in $\boldsymbol{Z}[t]$ for all prime powers q, then $g(x,t)$ is reducible in $\boldsymbol{Z}[x,t]$. Hence we have the following.

LEMMA 3. *Let x, t be indeterminates and let*

$$g(x,t) = t^n + g_1(x)t^{n-1} + \cdots + g_n(x) \in \boldsymbol{Z}[x,t].$$

Suppose that for each prime power q the roots of $g(q,t)$ are integers. Then there exist polynomials $m_1(x), \cdots, m_n(x) \in \boldsymbol{Z}[x]$ such that $g(x,t) = \prod_i (t + m_i(x))$.

5. **The unitary group; degree of $g_r(q)$.** Let E be a nonsingular n-dimensional unitary space over F_{q^2} and let $G(q)$ be the unitary group. Let $\Omega = \Omega(q)$ be the set of all pairs (B, A) where $B \supseteq A$ are subspaces of E.

LEMMA 4. *Let (B_i, A_i), $i = 1, 2$, be pairs in Ω and let $Z_i = A_i \cap \operatorname{rad} B_i$. Suppose $\theta: A_1 \to A_2$ is an isometry which maps Z_1 onto Z_2. If B_1, B_2 are isometric, then θ may be extended to an isometry $B_1 \to B_2$.*

Proof. In case the B_i are nonisotropic this is Witt's theorem. Suppose first that $Z_i = 0$. Then we may write $B_i = \operatorname{rad} B_i \perp B_i'$, where $B_i' \supseteq A_i$ and B_1', B_2' are

isometric and nonisotropic. Then $\theta: A_1 \to A_2$ may be extended by Witt's theorem to an isometry $B_1' \to B_2'$ which, since $\delta(\text{rad}\, B_1) = \delta(\text{rad}\, B_2)$, may be extended to an isometry $B_1 \to B_2$. In the general case write $A_i = Z_i \perp A_i''$, $B_i = Z_i \perp B_i''$ where $B_i'' \supseteq A_i''$ and $A_2'' = \theta A_1''$. Since $A_i'' \cap \text{rad}\, B_i'' = 0$, the map $\theta \mid A_1'' : A_1'' \to A_2''$ may be extended to an isometry $B_1'' \to B_2''$ and the Witt sum of this extension with the map $\theta \mid Z_1 : Z_1 \to Z_2$ gives the desired extension. One has analogous lemmas for a symplectic or orthogonal geometry.

The group $G(q)$ acts naturally as a permutation group on Ω. Let $G(E, B, A)$ denote the group of all $\gamma \in G(q)$ such that $\gamma B \subseteq B$ and $\gamma A \subseteq A$, let $G(B, A)$ denote the group of all $\gamma \in U(B)$ such that $\gamma A \subseteq A$, and let $H(B, A)$ denote the group of all elements of $G(B, A)$ which fix every vector in A. We have a natural homomorphism $G(E, B, A) \to G(B, A)$ defined by restriction of an element of $G(E, B, A)$ to B. Witt's theorem states that this is an epimorphism. The kernel is $H(E, B)$. Thus

$$|G(E, B, A)| = |G(B, A)|\,|H(E, B)|.$$

Since $G(E, B, A)$ is the stability group for the pair (B, A) in the permutation representation of $G(q)$ on Ω, the number of elements in the orbit of (B, A) under $G(q)$ is $|G(q)|\,|G(B, A)|^{-1}$. Let $\Lambda_r = \Lambda_r(q)$ be a set of representatives for those orbits of Ω under $G(q)$ which contain pairs (B, A) such that $\delta(A) = r$. Then from Proposition 1 we have

$$\begin{aligned} g_{n-r}(q) &= \sum_{(B,A)\in\Omega,\,\delta(A)=r} (-1)^{\delta(B/A)} q^{2\nu(B/A)} |H(E, B)| \\ &= \sum_{(B,A)\in\Lambda_r} |G(q)|\,|G(E, B, A)|^{-1} (-1)^{\delta(B/A)} q^{2\nu(B/A)} |H(E, B)|. \end{aligned}$$

Thus

$$g_{n-r}(q) = |G(q)| \sum_{(B,A)\in\Lambda_r} (-1)^{\delta(B/A)} q^{2\nu(B/A)} |G(B, A)|^{-1}. \tag{5.1}$$

For the symplectic and orthogonal groups we define $G(B, A)$, $H(B, A)$, Ω, and Λ_r in the analogous way and we have practically the same formula for $g_{n-r}(q)$. The only difference is that $2\nu(B/A)$ is replaced by $\nu(B/A)$.

Our problem is thus to find a set of representatives (B, A) for the orbits and to compute $|G(B, A)|$. It is easy to find a set of representatives. If $(B, A) \in \Omega$ we set $X = \text{rad}\, A$, $Y = \text{rad}\, B$, $Z = A \cap \text{rad}\, B$. To the pair (B, A) we let correspond the quintuple (a, b, x, y, z), where a, b, x, y, z are the dimensions of A, B, X, Y, Z. It follows from Lemma 4, Witt's theorem, and the fact that there is a unique nonsingular unitary geometry for each dimension and prime power q, that two pairs (B,A), (B',A') are in the same orbit if and only if $(a, b, x, y, z) = (a', b', x', y', z')$.

In the next lemma we state several formulas which help us to compute $|G(B, A)|$.

LEMMA 5. *Let $A \perp X$, $B \perp X$ be subspaces of E, where $B \supseteq A$ and where X is totally isotropic. Then*

(1) $|\boldsymbol{G}(B \perp X, X)| = |\boldsymbol{GL}(X)|\,|\operatorname{Hom}(B, X)|\,|\boldsymbol{U}(B)|$,

(2) $|\boldsymbol{H}(B \perp X, A \perp X)| = |\operatorname{Hom}(B/A, X)|\,|\boldsymbol{H}(B, A)|$,

(3) $|\boldsymbol{H}(B \perp X, A)| = |\boldsymbol{GL}(X)|\,|\operatorname{Hom}(B/A, X)|\,|\boldsymbol{H}(B, A)|$ *if B is nonisotropic,*

(4) $|\boldsymbol{U}(B \perp X)| = |\boldsymbol{GL}(X)|\,|\operatorname{Hom}(B, X)|\,|\boldsymbol{U}(B)|$ *if B is nonisotropic.*

Proof. If $\sigma \in \boldsymbol{U}(B), \tau \in \operatorname{Hom}(B, X)$, and $\rho \in \boldsymbol{GL}(X)$, we may, since X is totally isotropic, define an element $\gamma \in \boldsymbol{G}(B \perp X, X)$ as follows: $\gamma e = \sigma e + \tau e$ if $e \in B$, $\gamma e = \rho e$ if $e \in X$. Every element of $\boldsymbol{G}(B \perp X, X)$ has this form. This proves (1). If $\sigma \in \boldsymbol{H}(B, A)$ and $\tau \in \operatorname{Hom}(B, X)$ annihilates A, then we may define an element $\gamma \in \boldsymbol{H}(B \perp X, A \perp X)$ as follows: $\gamma e = \sigma e + \tau e$ if $e \in B$, $\gamma e = e$ if $e \in X$. Every element of $\boldsymbol{H}(B \perp X, A \perp X)$ has this form. This proves (2). If $\sigma \in \boldsymbol{H}(B, A)$, $\rho \in \boldsymbol{GL}(X)$, and $\tau \in \operatorname{Hom}(B, X)$ annihilates A, then we may define an element $\gamma \in \boldsymbol{H}(B \perp X, A)$ as follows: $\gamma e = \sigma e + \tau e$ if $e \in B$, $\gamma e = \rho e$ if $e \in X$. Since B is nonisotropic, $X = \operatorname{rad}(B \perp X)$ is globally invariant under $\boldsymbol{H}(B \perp X, A)$ so that every element of $\boldsymbol{H}(B \perp X, A)$ has this form. This proves (3). Now (4) is just (3) with $A = 0$; it is also a special case of (1).

LEMMA 6. *For each prime power q let E_q be a nonsingular n-dimensional unitary space over $\boldsymbol{F}_{q^2}$ and let (B_q, A_q) be a pair of subspaces of E_q with $B_q \supseteq A_q$. Suppose these subspaces are chosen so that the corresponding quintuple $(a_q, b_q, x_q, y_q, z_q) = (a, b, x, y, z)$ is independent of q. Then $|\boldsymbol{G}(q)|q^{2\nu(B/A)}|\boldsymbol{G}(B_q, A_q)|^{-1}$ is a monic polynomial in q of degree at most $n^2 - a^2$ with integer coefficients which depend only on n and the quintuple (a, b, x, y, z). The degree is $n^2 - a^2$ if and only if A_q is nonisotropic and $A_q = B_q$.*

Proof. We shall sometimes omit the subscript q. Choose spaces V, W such that $X = Z \perp V$, $Y = Z \perp W$. Choose a nonisotropic subspace C of A such that $A = X \perp C$. Since $(V \perp C) \cap Y = 0$ and C is a nonisotropic subspace of B, we may choose a nonisotropic subspace D of B such that $D \supseteq V$ and $B = Y \perp C \perp D$. We thus have decompositions

$$A = Z \perp V \perp C, \quad B = Z \perp W \perp C \perp D, \tag{5.2}$$

where V, W, Z are totally isotropic and C, D are nonisotropic, and where $D \supseteq V$. Each of the spaces C, D, V, W is provided with a subscript q, but the corresponding dimensions c, d, v, w are independent of q. We have

$$v = x - z, \quad w = y - z, \quad c = a - x, \quad d = (b - a) + (x - y).$$

There is a homomorphism $\boldsymbol{G}(B, A) \to \boldsymbol{G}(A, Z)$ defined by restriction of an element of $\boldsymbol{G}(B, A)$ to A. By Lemma 4 this is an epimorphism. The kernel is $\boldsymbol{H}(B, A)$. Thus

$$|\boldsymbol{G}(B, A)| = |\boldsymbol{H}(B, A)|\,|\boldsymbol{G}(A, Z)|.$$

Now from Lemma 5 we have

$$\begin{aligned}|G(A,Z)| &= |G(Z\perp V\perp C,Z)| \\ &= |GL(Z)|\,|\mathrm{Hom}(V\perp C,Z)|\,|U(V\perp C)| \\ &= |GL(Z)|\,|\mathrm{Hom}(V\perp C,Z)|\,|GL(V)|\,|\mathrm{Hom}(C,V)||U(C)|.\end{aligned}$$

Thus from (2.1) and (2.2) we see that $|G(A_q,Z_q)|$ is a monic polynomial in q with integer coefficients which depend only on (a,b,x,y,z) of degree

$$2z^2+2vz+2cz+2v^2+2cv+c^2=z^2+v^2+a^2.$$

Again, using Lemma 5,

$$\begin{aligned}|H(B,A)| &= |H(Z\perp W\perp C\perp D,Z\perp V\perp C)| \\ &= |\mathrm{Hom}(B/A,Z)|\,|H(W\perp C\perp D,V\perp C)| \\ &= |\mathrm{Hom}(B/A,Z)|\,|GL(W)|\,|\mathrm{Hom}(D/V,W)|\,|H(C\perp D,V\perp C)| \\ &= |\mathrm{Hom}(B/A,Z)|\,|GL(W)|\,|\mathrm{Hom}(D/V,W)|\,|H(D,V)|.\end{aligned}$$

The last equality $|H(C\perp D,V\perp C)|=|H(D,V)|$ is valid because C and D are nonisotropic, so that an element of $U(C\perp D)$ which fixes C leaves D globally invariant. Since V is a totally isotropic subspace of the nonisotropic space D, we have a Witt decomposition $D=(V+V')\perp F$, where V' is totally isotropic, $V+V'$ is nonisotropic, $\delta(V)=\delta(V')$, the sum $V+V'$ is direct, and F is nonisotropic. The dimension of F is $f=b-a+2z-x-y$. In a suitable basis adapted to this decomposition of D, the hermitian form Φ_D defining the geometry in D is given by

$$\Phi_D=\begin{bmatrix}0 & I & 0\\ I & 0 & 0\\ 0 & 0 & I\end{bmatrix},$$

where I denotes an identity matrix of an appropriate degree, v or f. In this basis the matrix for an element of $H(D,V)$ has the form

$$\begin{bmatrix}I & 0 & 0\\ P & I & Q\\ R & 0 & S\end{bmatrix},$$

where Q is an arbitrary v-by-f matrix with coefficients in F_{q^2} and P,R,S are subject to the conditions

$$S\in U(F),\quad P+{}^t\bar{P}+Q\,{}^t\bar{Q}=0,\quad \bar{R}+Q\,{}^t\bar{S}=0.$$

The number of possibilities for Q is q^{2vf}. R is determined by Q and S. For given Q the number of possibilities for P is the number of v by v skew-hermitian-matrices with coefficients in F_{q^2}. This number is q^{v^2}. Thus $|H(B_q,A_q)|$ is a monic polynomial in q with integer coefficients which depend only on (a,b,x,y,z) of degree

$$2(b-a)z + 2w^2 + 2(d-v)w + v^2 + 2vf + f^2 = 2(b-a)z + w^2 + (b-a)^2.$$

Thus $|G(q)|q^{2\nu(B_q/A_q)}|G(B_q, A_q)|^{-1}$ is a monic polynomial in q of degree

$$n^2 - a^2 - (b-a)(1+2z) - z^2 - v^2 - w^2.$$

This is at most $n^2 - a^2$ with equality if and only if $b = a$ and $z = v = w = 0$. Hence equality holds if and only if $A = B$ is nonisotropic. This proves the lemma.

Let $\Gamma_r(q)$ denote the set of all quintuples $(a_q, b_q, x_q, y_q, z_q)$ with $a_q = r$, which correspond to the pairs (B_q, A_q) in $\Lambda_r(q)$. Since there is a unique nonsingular unitary geometry for each dimension and prime power q, the set $\Gamma_r(q)$ depends only on r and n and is independent of q. We conclude from (5.1) and Lemma 6 the following.

PROPOSITION 2. *Let $G(q)$ be the unitary group of degree n. Then $g_{n-r}(q)$ is a monic polynomial in q of degree $n^2 - r^2$ with integer coefficients which depend only on n and r.*

We shall need more explicit information about $g_1(q)$, the number of elements of $G(q)$ distinct from the identity, which fix an $(n-1)$-dimensional subspace.

LEMMA 7. *Let $G(q)$ be the unitary group of degree n. Then*

$$g_1(q) = Q_n(q^n + Q_{n-1})/Q_1$$

where we set $Q_k = q^k - (-1)^k$.

Proof. The set $\Gamma_1(q)$ consists of four quintuples, two of them corresponding to pairs (B, A) for which A is nonisotropic and two for which $\delta(\operatorname{rad} A) = 1$. To each A correspond two pairs (B, A), one with $B = A$ and the other with $B = E$. We use the argument of Lemma 6 to compute the polynomials

$$|G(q)|q^{2\nu(B/A)}|G(B, A)|^{-1}.$$

These are given by the following table:

(a, b, x, y, z)	$\lvert G(q)\rvert q^{2\nu(B/A)}\rvert G(B,A)\rvert^{-1}$
$(n-1, n-1, 0, 0, 0)$	$q^{n-1}Q_n$
$(n-1, \ n, \ 0, 0, 0)$	$q^{n-1}Q_n/Q_1$
$(n-1, n-1, 1, 1, 1)$	qQ_nQ_{n-1}/Q_2
$(n-1, \ n, \ 1, 0, 0)$	Q_nQ_{n-1}/Q_2 .

It follows from (5.1) that

$$g_1(q) = q^{n-1}Q_n - q^{n-1}Q_n/Q_1 + qQ_nQ_{n-1}/Q_2 - Q_nQ_{n-1}/Q_2$$

which, after some simplification, yields the statement of the lemma.

6. **The unitary group; proof of Theorem 1.** Suppose that for all prime powers q there exist integers $m_i(q)$ which satisfy (1.2). Since $g_r(q)$ is a polynomial in q with integer coefficients it follows from Lemma 3, with t replaced by t^{-1}, that (after renumbering the $m_i(q)$ for each q, if necessary) $m_i(q)$ is a polynomial in q with integer coefficients. Since $g_{n-r}(q)$ has degree $n^2 - r^2$ and is the $(n-r)$th elementary symmetric function of the $m_i(q)$, it follows that the degrees of the $m_i(q)$ are $1, 3, 5, \cdots, 2n-1$. Set $t = 1$ in (1.2). Then the formula (2.2) for $|G(q)|$ yields

$$q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i) = \prod_{i=1}^{n} (1 + m_i(q)). \tag{6.1}$$

From Lemma 7 it follows, for $n > 1$, that $g_1(q) \equiv -1 \bmod q$, so that

$$\sum_i m_i(q) \equiv -1 \bmod q. \tag{6.2}$$

Assume for the moment that $n > 1$. Then from (6.2) we have

$$\sum_i (1 + m_i(0)) = n - 1. \tag{6.3}$$

Since $1 + m_i(q)$ is a polynomial with coefficients in $\boldsymbol{Z}$ we see from (6.1) and the unique factorization in $\boldsymbol{Z}[x]$ that

$$1 + m_i(0) = 0, \ +1, \ -1, \tag{6.4}$$

for each $i = 1, \cdots, n$. Now (6.3) and (6.4) taken together show that the only possible distribution for the values $1 + m_i(0)$ is $0, 1, \cdots, 1$ where 1 is taken $n-1$ times. It follows that $1 + m_i(q) \equiv 0 \bmod q$ for at most one value of i and hence from (6.1) we see that some $1 + m_i(q)$ is divisible by $q^{n(n-1)/2}$. In particular, the degree of this $m_i(q)$ must be at least $n(n-1)/2$. On the other hand, we have seen that the degree of $m_i(q)$ is at most $2n-1$. Thus $n(n-1)/2 \leqq 2n-1$ and hence $n \leqq 4$. We can exclude the case $n = 4$. In this case the degrees of the hypothetical $m_i(q)$ are $1, 3, 5, 7$. We must have $1 + m_j(q) \equiv 0 \bmod q^6$ for some j. From (6.1) and the unique factorization in $\boldsymbol{Z}[x]$ if follows that we must have $m_j(q) = q^6(q \pm 1) - 1$ while the remaining $m_i(q)$ have degree at most 5. This contradicts Lemma 7, which shows that $\sum_i m_i(q) = q^7 - q^2 + q - 1$. Thus $n = 4$ is impossible. For $n = 1, 2, 3$ we compute the $g_r(q)$ directly using (5.1). The results are

n	$g_1(q)$	$g_2(q)$	$g_3(q)$
1	q		
2	q^3-1	q^4-q^2-q	
3	q^5+q-1	q^8-q^3-q	$q^9-q^7-q^4$.

From this information we see that the $m_i(q)$ exist for $n = 1,2,3$ and are given by

n	$m_i(q)$
1	q
2	$q, q^3 - q - 1$
3	$q, q^3, q^5 - q^3 - 1$.

This completes the proof of Theorem 1.

7. **The symplectic group.** We sketch those parts of the argument which differ from the unitary case. The symplectic group $G(q)$ acts on the set Ω of pairs (B, A) of subspaces of E and the orbits are again in one-to-one correspondence with certain quintuples (a, b, x, y, z). The spaces B, A may be decomposed as in (5.2). Here $|G(A_q, Z_q)|$ is a monic polynomial in q of degree

$$z^2 + vz + cz + v^2 + cv + \frac{c(c+1)}{2} = \frac{1}{2}\{z^2 + v^2 + a^2 + c\}.$$

In the decomposition $D = (V + V') \perp F$ we write the nonsingular symplectic space F as a direct sum $F = F_0 + F_0'$ of maximal totally isotropic subspaces. Set $f_0 = \delta(F_0)$ so that $f = 2f_0$. In a suitable basis adapted to this decomposition of D, the alternating form Φ_D defining the geometry in D, is given by

$$\Phi_D = \begin{bmatrix} 0 & I & 0 & 0 \\ -I & 0 & 0 & 0 \\ 0 & 0 & 0 & I \\ 0 & 0 & -I & 0 \end{bmatrix},$$

where I denotes an identity matrix of an appropriate degree, v or f_0. In this basis the matrix for an element of $H(D, V)$ has the form

$$\begin{bmatrix} I & 0 & 0 & 0 \\ L & I & M & N \\ P & 0 & Q & R \\ S & 0 & T & U \end{bmatrix},$$

where M, N are arbitrary v-by-f_0 matrices with coefficients in F_q and L,P,Q,R,S,T,U are subject to the conditions

$$L \text{ symmetric}, \quad \begin{pmatrix} Q & R \\ T & U \end{pmatrix} \text{ symplectic},$$

$${}^tP - M\,{}^tR + N\,{}^tQ = 0, \quad {}^tS - M\,{}^tU + N\,{}^tT = 0.$$

We conclude that $|H(B_q, A_q)|$ is a monic polynomial in q of degree

$$(b-a)z + w^2 + (d-v)w + \frac{v(v+1)}{2} + vf + \frac{f(f+1)}{2}$$
$$= \frac{1}{2}\{2(b-a)z + w^2 + (b-a)^2 + v + f\}.$$

It follows, after a little computation, that $|G(q)|q^{v(B_q/A_q)}|G(B_q, A)_q|^{-1}$ is a monic polynomial in q of degree

$$\frac{1}{2}\{n(n+1) - a(a+1) - (b-a)(1+2z) - (z^2 - z) - (v^2 - v) - (w^2 - w)\}.$$

This is at most $n(n+1)/2 - a(a+1)/2$. If equality holds then $b = a$ and $z = 0$ or 1. Then $A = B$ and $Z = A \cap \operatorname{rad} B = \operatorname{rad} A$ and hence $v = w = 0$. Since the dimension of a nonsingular symplectic space is even we have $z \equiv a \bmod 2$. Thus equality holds if and only if $A = B$ and one of the following is true:

$\delta(A)$ is even and A is nonisotropic,

$\delta(A)$ is odd and $\delta(\operatorname{rad} A) = 1$.

We conclude from the symplectic analogue of (5.1) the following.

PROPOSITION 3. *Let $G(q)$ be the symplectic group of degree n. Then $g_{n-r}(q)$ is a monic polynomial in q of degree $n(n+1)/2 - r(r+1)/2$ with integer coefficients.*

Suppose that for given n we have a formula (1.2) for all prime powers q. We conclude via Lemma 3, Proposition 3 and (2.3), the existence of polynomials $m_1(q), \cdots, m_n(q)$ of degrees $1, \cdots, n$ with integer coefficients, such that

$$q^{(n/2)^2} \prod_{i=1}^{n/2} (q^{2i} - 1) = \prod_{i=1}^{n} (1 + m_i(q)).$$

Compute $g_1(q) = q^n - 1$. Since $g_1(q) \equiv -1 \bmod q$, we conclude that some $m_i(q)$ has degree at least $(n/2)^2$. Hence $(n/2)^2 \leqq n$ and $n \leqq 4$. We exclude the case $n = 4$ by an argument similar to that for the unitary group. For $n = 2$ the $m_i(q)$ exist and are given by

$$m_1(q) = q, \qquad m_2(q) = q^2 - q - 1.$$

8. **The orthogonal groups.** We sketch those parts of the argument which differ from the unitary case. In this case two pairs (B, A), (B', A') lie in the same orbit under $G(q)$ if and only if $(a, b, x, y, z) = (a', b', x', y', z')$ and there exist isometries $A/\operatorname{rad} A \simeq A'/\operatorname{rad} A'$, $B/\operatorname{rad} B \simeq B'/\operatorname{rad} B'$. The analogue of Lemma 6 is the following.

LEMMA 8. *For each odd prime power q, let E_q be an n-dimensional vector space over E_q with a nonsingular orthogonal geometry of a type independent of*

q. Let (B_q, A_q) be a pair of subspaces of E_q with $B_q \supseteq A_q$. Suppose these subspaces are chosen so that $(a_q, b_q, x_q, y_q, z_q) = (a, b, x, y, z)$ is independent of q and so that the types of $A_q/\operatorname{rad} A_q$ and $B_q/\operatorname{rad} B_q$ are independent of q. Then $|G(q)|q^{\nu(B_q/A_q)}|G(B_q, A_q)|^{-1}$ is a polynomial in q of degree at most $n(n-1)/2 - r(r-1)/2$. The coefficients are integers or half-integers and depend only on n, on the quintuple (a, b, x, y, z) and on the types of $A_q/\operatorname{rad} A_q$ and $B_q/\operatorname{rad} B_q$. The degree is equal to $n(n-1)/2 - r(r-1)/2$ if and only if both A_q and B_q are nonisotropic.

Proof. The spaces B, A may be decomposed as in (5.2). Since $C \simeq A/\operatorname{rad} A$, the type of $C = C_q$ is independent of q and hence $|O(C_q)|$ is a polynomial in q. Then $|G(A_q, Z_q)|$ is a polynomial in q of degree

$$z^2 + vz + cz + v^2 + cv + \frac{c(c-1)}{2} = \frac{1}{2}\{z^2 + v^2 + a^2 - c\},$$

with integer coefficients. Since $B/\operatorname{rad} B \simeq A/\operatorname{rad} A \perp D$, the type of geometry in $D = D_q$ is independent of q. In the decomposition $D = (V + V') \perp F$, the nonisotropic space $V + V'$ has a geometry of type III and hence the type of $F = F_q$ is independent of q. Thus $|O(F_q)|$ is a polynomial in q, and by computations like those for the unitary group we see that $|H(B_q, A_q)|$ is a polynomial in q with integer coefficients of degree

$$(b-a)z + w^2 + (d-v)w + \frac{v(v-1)}{2} + vf + \frac{f(f-1)}{2}$$
$$= \frac{1}{2}\{2(b-a)z + w^2 + (b-a)^2 - v - f\}.$$

It follows that $|G(q)|q^{\nu(B_q/A_q)}|G(B_q, A_q)|^{-1}$ is a polynomial in q of degree

$$\frac{1}{2}\{n(n-1) - a(a-1) - 2(b-a)z - (z^2 - z) - v^2 - w^2 - x - y\}.$$

This is at most $n(n-1)/2 - a(a-1)/2$. Equality holds if and only if v, w, x, y, z are all 0, that is, if and only if both A and B are nonisotropic. The coefficients are half-integers if C_q and F_q are both different from zero, in which case both $|O(C_q)|$ and $|O(F_q)|$ contribute factors of 2 to the denominator. Only one of these factors of 2 is cancelled by $|G(q)|$.

PROPOSITION 4. *Let $G(q) = O(n, q, \Phi_q)$ be the orthogonal group, where the forms Φ_q are all of the same type. Then $g_{n-r}(q)$ is a monic polynomial in q of degree $n(n-1)/2 - r(r-1)/2$ with integer coefficients.*

Proof. We have

$$g_{n-r}(q) = |G(q)| \sum_{(B,A)\in\Lambda_r(q)} (-1)^{\delta(B/A)} q^{\nu(B/A)} |G(B, A)|^{-1}. \tag{8.1}$$

Two complications occur here which were not present for the unitary and symplectic groups. First, the terms in the sum may have half-integer coefficients. Second, all pairs (B, A) with nonisotropic B and A contribute to the leading term of $g_{n-r}(q)$.

To eliminate the half-integer coefficients, suppose (B, A) is a pair such that C, F are both nonzero. In this case the leading coefficient of

$$|G(q)|\, q^{v(B/A)} |G(B, A)|^{-1}$$

is $1/2$. To the orbit of (B, A) under $G(q)$ we associate a second orbit containing a pair $(B, \tilde{A})$ such that the corresponding $\tilde{C}, \tilde{F}$ are both nonzero, such that $\tilde{A} \approx A$, and such that the polynomial $|G(q)|\, q^{v(B/A)}(|G(B, A)|^{-1} + |G(B, \tilde{A})|^{-1})$ has integer coefficients. This will be enough to show that $g_{n-r}(q)$ has integer coefficients. We use the decompositions

$$A = Z \perp V \perp C, \quad B = Z \perp W \perp C \perp D, \quad D = (V + V') \perp F,$$

Since C, F are nonzero, we may choose in the nonisotropic space $C \perp F$, subspaces $\tilde{C}, \tilde{F}$ such that $C \perp F = \tilde{C} \perp \tilde{F}$, $\delta(C) = \delta(\tilde{C})$, $\delta(F) = \delta(\tilde{F})$, and such that $C, \tilde{C}$ have different types of geometry. We use here the fact that a space E over F_q with a nonsingular orthogonal geometry, contains nonisotropic subspaces of both types, for any dimension δ such that $0 < \delta < \delta(E)$. Then $F, \tilde{F}$ have different types of geometry. Set

$$\tilde{A} = Z \perp V \perp \tilde{C}, \quad \tilde{B} = Z \perp W \perp \tilde{C} \perp \tilde{D} = B, \quad \tilde{D} = (V + V') \perp \tilde{F}.$$

The computations of Lemma 5 are valid for the orthogonal group, almost without change. These computations show that

$$\frac{|G(B, A)|}{|G(B, \tilde{A})|} = \frac{|H(B, A)|}{|H(B, \tilde{A})|} = \frac{|H(D, V)|}{|H(\tilde{D}, V)|} = \frac{|O(F)|}{|O(\tilde{F})|},$$

so that

$$|G(q)|\, q^{v(B/A)}(|G(B, A)|^{-1} + |G(B, \tilde{A})|^{-1}) = |G(q)|\, q^{v(B/A)} |G(B, A)|^{-1} \left(1 + \frac{|O(F)|}{|O(\tilde{F})|}\right). \tag{8.2}$$

If f is odd we have $|O(F)| = |O(\tilde{F})|$ so that we acquire a factor of 2 in the numerator and (8.2) is a monic polynomial in q with integer coefficients. If f is even, then from (2.4) we see that, interchanging F and $\tilde{F}$ if necessary,

$$1 + \frac{|O(F)|}{|O(\tilde{F})|} = 1 + \frac{q^{f/2} - 1}{q^{f/2} + 1} = \frac{2q^{f/2}}{q^{f/2} + 1},$$

so that (8.2) is, in this case too, a monic polynomial in q with integer coefficients.

We must show that the leading coefficient of $g_{n-r}(q)$ is 1. In view of Lemma 8 we need consider in (8.1) only those orbits which contain pairs (B, A) for which B, A are nonisotropic. If $r = n$ we must compute the leading coefficient of

$$|G(q)| \sum_{B \in \Lambda} (-1)^{\delta(B)} q^{\nu(B)} |O(B)|^{-1},$$

where the sum is over a set Λ of subspaces of E such that every subspace of E is isometric to a unique element of Λ. Since there are, up to isometry, two possibilities for B in each dimension k with $0 < k < n$, this leading coefficient is

$$2 + \sum_{0<k<n} (-1)^k(1+1) + (-1)^n = 1.$$

If $0 < r < n$, there are, up to isometry, two subspaces $A, \tilde{A}$ of dimension r, and then (8.2) shows in the same way that the leading coefficient is 1 here too. This completes the proof of Proposition 4.

Suppose now that for given n and given type we have a formula (1.2) for all odd prime powers q. We conclude via Lemma 3, Proposition 4, and (2.4) the existence of polynomials $m_i(q)$ of degrees $0, 1, \cdots, n-1$, with integer coefficients, such that

$$\begin{aligned} 2q^{(n-1)^2/4} \prod_{i=1}^{(n-1)/2} (q^{2i} - 1) &= \prod_{i=1}^{n} (1 + m_i(q)), && \text{Types I, II,} \\ 2q^{n(n-2)/4}(q^{n/2} - \varepsilon) \prod_{i=1}^{(n-2)/2} (q^{2i} - 1) &= \prod_{i=1}^{n} (1 + m_i(q)), && \text{Types III, IV.} \end{aligned} \tag{8.3}$$

We compute $g_1(q)$ and find that

$$g_1(q) = \begin{cases} q^{n-1}, & \text{Types I, II,} \\ q^{n-1} - \varepsilon q^{n/2-1}, & \text{Types III, IV.} \end{cases}$$

Thus $g_1(q) \equiv 0 \bmod q$ if $n > 2$. Assume for the moment that $n > 2$. Since one of the $m_i(q)$, say $m_1(q)$, has degree 0 and since $g_n(q) = \prod_i m_i(q)$ is a monic polynomial in q with integer coefficients it follows that $m_1(q) = 1$. We may thus cancel a factor of 2 on both sides of (8.3). Now, observing that

$$\sum_{i=2}^{n} m_i(q) \equiv -1 \bmod q,$$

we may argue as in the case of the unitary group, to conclude that some $m_i(q)$ is divisible by the full power of q which divides $|G(q)|$. Thus

$$\begin{aligned} (n-1)^2/4 &\leqq n-1, && \text{for Types I, II,} \\ n(n-2)/4 &\leqq n-1, && \text{for Types III, IV,} \end{aligned}$$

so that $n \leqq 5$ for types I, II and $n \leqq 4$ for types III, IV. We exclude $n = 5$ by an argument similar to that for the unitary group. We exclude $n = 4$, type III, by

explicitly computing the $g_r(q)$. The remaining cases are enumerated in the following table:

n	Type	$g_1(q)$	$g_2(q)$	$g_3(q)$	$g_4(q)$
1	I,II	1			
2	III	$q-1$	$q-2$		
2	IV	$q+1$	q		
3	I,II	q^2	q^3-q-1	q^3-q^2-q	
4	IV	q^3+q	$q^5+q^3-q^2-1$	$q^6-q^3-q^2-q$	$q^6-q^5-q^3$.

From this information we see that the $m_i(q)$ exist in these cases and are given by

n	Type	$m_i(q)$
1	I,II	1
2	III	$1, q-2$
2	IV	$1, q$
3	I,II	$1, q, q^2-q-1$
4	IV	$1, q, q^2, q^3-q^2-1$

This completes the proof of Theorem 3.

References

1. E. Artin, *Geometric algebra*, Interscience, New York, 1957.
2. N. Bourbaki, *Algèbre, Formes sesquilinéaires et formes quadratiques*, Hermann, Paris, 1959.
3. C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.
4. J. Dieudonné, *La géométrie des groupes classiques*, Springer, Berlin, 1955.
5. K. Dörge, *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*, Math. Ann. **96** (1927), 176–182.
6. P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. **36** (1934), 29–95.
7. ———, *The Eulerian functions of a group*, Quart. J. Math. Oxford Ser. **7** (1936), 34–51.
8. S. Lang, *Diophantine geometry*, Interscience, New York, 1962.
9. G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.
10. L. Solomon, *Invariants of finite reflection groups*, Nagoya Math. J. **22** (1963), 57–64.
11. L. Weisner, *Some properties of prime power groups*, Trans. Amer. Math. Soc. **38** (1935), 485–492.

Institute for Advanced Study,
Princeton, New Jersey
Haverford College,
Haverford, Pennsylvania