Can. J. Math., Vol. XXII, No. 3, 1970, pp. 492–513

SINGER GROUPS

MARSHALL D. HESTENES

Interest in the Singer groups has arisen in various places. The name itself results from the connection Singer [**7**] made between these groups and perfect difference sets, and this is closely associated with the geometric property that a Singer group is regular on the points of a projective space. Some information about these groups appears in Huppert's book [**3**, p. 187]. Singer groups are frequently useful in constructing examples and counterexamples. Our aim in this paper is to make a systematic study of the Singer subgroups of the linear groups, with a particular view to analyzing the examples they provide of Frobenius regular groups. Frobenius regular groups are a class of permutation groups generalizing the Zassenhaus groups, and Keller [**5**] has shown recently that they provide a new characterization of A_6 and M_{11}.

In § 2 we study the properties of the Singer groups as subgroups of the linear groups. From these properties we will be able to see when the Singer subgroups may be used to obtain a representation of $\mathrm{PSL}_n(q)$ as a Frobenius regular group. Section 3 is devoted to the investigation of this representation in detail. In § 4 we determine all the cyclic self-centralizing trivial intersection (T.I.) sets in $\mathrm{PSL}_n(q)$ in order to show that the Singer groups are essentially the only cyclic T.I. sets in $\mathrm{PSL}_n(q)$ yielding a Frobenius regular representation. Then in § 5 we investigate the intersection of Singer groups with some of the other classical groups, and in particular we show that in some cases this intersection may be used to get a Frobenius regular representation of a unitary group. This result indicates that very considerable difficulties are to be expected in the problem of classifying the Frobenius regular groups.

Acknowledgement. I wish to express my deep gratitude to Professor D. G. Higman for his careful guidance, advice, and encouragement during the preparation of this work.

1. Preliminaries.

Let V be a vector space of dimension $n \geqq 2$ over the finite field F_q, where $q = p^m$, p a prime. The group of all non-singular linear transformations of V is denoted by $\mathrm{GL}(V)$, and the kernel of the determinant map $\mathrm{GL}(V) \to F_q{}^*$ is denoted by $\mathrm{SL}(V)$. Set $\mathrm{PGL}(V) = \mathrm{GL}(V)/Z$, where Z is the centre of $\mathrm{GL}(V)$, and set $\mathrm{PSL}(V) = \mathrm{SL}(V)/Z_1$, where $Z_1 = Z \cap \mathrm{SL}(V)$ is the centre of $\mathrm{SL}(V)$. Let $P(V)$ be the lattice of subspaces of V, which we may regard as an $(n - 1)$-dimensional projective

Received February 21, 1969. This research was supported in part by grants from the National Science Foundation. Most of the material in this paper appeared in the author's doctoral thesis written at the University of Michigan under the direction of Professor D. G. Higman.

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

space over F_q. Then there exists a natural homomorphism of $\mathrm{GL}(V)$ into $\mathrm{Aut}\, P(V)$, with kernel Z, so that the image of $\mathrm{GL}(V)$ is isomorphic to $\mathrm{PGL}(V)$ and the image of $\mathrm{SL}(V)$ is isomorphic to $\mathrm{PSL}(V)$.

Now we choose for V the field F_{q^n}, regarded as a vector space of dimension n over F_q. For each $\alpha \in F_{q^n}^*$, let $T_\alpha \in \mathrm{GL}(V)$ be given by T_α: $x \rightarrow \alpha x$, $x \in V$. Then $T = \{T_\alpha \in \mathrm{GL}(V) | \alpha \in F_{q^n}^*\}$ is a cyclic subgroup of $\mathrm{GL}(V)$ isomorphic to $F_{q^n}^*$, and T is regular on the vectors in $V - \{0\}$.

Definition 1.1. The conjugates of T in $\mathrm{GL}(V)$ will be called Singer groups in $\mathrm{GL}(V)$. The intersection of a Singer group in $\mathrm{GL}(V)$ with $\mathrm{SL}(V)$ will be called a Singer group in $\mathrm{SL}(V)$. The image in $\mathrm{PGL}(V)$ of a Singer group in $\mathrm{GL}(V)$ will be called a Singer group in $\mathrm{PGL}(V)$. The image in $\mathrm{PSL}(V)$ of a Singer group in $\mathrm{SL}(V)$ will be called a Singer group in $\mathrm{PSL}(V)$.

If M, SM, H, and K are Singer groups in $\mathrm{GL}(V)$, $\mathrm{SL}(V)$, $\mathrm{PGL}(V)$, and $\mathrm{PSL}(V)$, respectively, then it is evident from the definitions that they are all cyclic with orders

$$\begin{aligned} |M| &= q^n - 1, \\ |SM| = |H| &= (q^n - 1)/(q - 1), \\ |K| &= (q^n - 1)/(q - 1)(n, q - 1). \end{aligned}$$

Definition 1.2. A generator for a Singer group will be called a Singer cycle.

It is also clear that M and SM are regular and semi-regular, respectively, on the vectors in $V - \{0\}$, and H and K are regular and semi-regular, respectively, on the points of $P(V)$. The Singer groups in $\mathrm{GL}(V)$ are all conjugate as are those in $\mathrm{PGL}(V)$.

With respect to a fixed basis for V, we have isomorphisms of the groups $\mathrm{GL}(V)$, $\mathrm{SL}(V)$, $\mathrm{PGL}(V)$, and $\mathrm{PSL}(V)$ onto their matrix versions $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$, respectively. The image of a Singer group in $\mathrm{GL}(V)$ is referred to as a Singer group in $\mathrm{GL}_n(q)$, and so on.

In order to relate this study of Singer groups with Frobenius regular groups, we will need the following.

Definition 1.3. A finite permutation group G acting transitively on a set Ω will be called a Frobenius regular group if for $a \in \Omega$

(1) there exists a faithful Frobenius G_a-orbit, and

(2) every non-Frobenius orbit different from $\{a\}$ of G_a is regular.

Definition 1.4. A Frobenius regular group G such that there are α Frobenius G_a-orbits and β regular G_a-orbits is called an $[\alpha, \beta]$-group.

LEMMA 1.5. *If a finite group G has a proper subgroup N satisfying:*

(1) *N is a Frobenius group with kernel K and complement E,*

(2) $N = \mathrm{N}_G(K)$, *and*

(3) *K and E are T.I. sets in G,*

then G is faithfully represented as a Frobenius regular group on the set Ω of left cosets of G (mod N).

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

LEMMA 1.6. *Under the above hypotheses, $N{:}E$ is one plus the number of Frobenius orbits of G_a, $a \in \Omega$, and the number of self-paired Frobenius orbits of G_a is the number of involutions in N/E.*

2. Singer subgroups of the linear groups.

Let us look at our field-theoretic model of a Singer group in $\mathrm{GL}(V)$, $T = \langle T_\xi \rangle$, where ξ is a primitive $(q^n - 1)$th root of unity. Since the characteristic polynomial of ξ over F_q,

$$\prod_{i=0}^{n-1} (x - \xi^{q^i}),$$

is the same as the characteristic polynomial of T_ξ, T_ξ has only trivial eigenspaces in V. Suppose that we extend the ground field F_q to F_{q^n}; thus we have the natural embeddings:

$$\begin{aligned} V \to W &= F_{q^n} \otimes_{F_q} V, \\ P(V) &\to P(W), \\ \mathrm{GL}(V) &\to \mathrm{GL}(W), \\ \mathrm{Aut}\, P(V) &\to \mathrm{Aut}\, P(W). \end{aligned}$$

Identify V with its image in W, etc.

Definition 2.1. A vector in W but not in V will be called irrational. A point of $P(W)$ not in $P(V)$, i.e., a one-dimensional subspace of W spanned by an irrational vector, will be called an irrational point in $P(W)$.

Choose a basis $X_0, X_1, \ldots, X_{n-1}$ of W such that X_i is the irrational eigenvector of T corresponding to the eigenvalue ξ^{q^i}, $i = 0, \ldots, n-1$. Any member of T has the form $(T_\xi)^t = T_{\xi^t}$ with eigenvalues ξ^{tq^i}, $i = 0, \ldots, n-1$. What are the eigenspaces for T_{ξ^t}? X_i and X_{i+j} are in the same eigenspace for T_{ξ^t} if and only if $\xi^{tq^i} = \xi^{tq^{i+j}}$, and this equality holds if and only if $\xi^t = \xi^{tq^j}$; thus in particular the eigenspaces of T_{ξ^t} all have the same dimension. Let $\sigma: x \to x^q$, $x \in F_{q^n}{}^*$, be an automorphism of order n of F_{q^n} over F_q. Since ξ^{tq^j} is $(\xi^t)^{\sigma^j}$, X_0 and X_j are in the same eigenspace if and only if ξ^t is in the fixed field of σ^j. Hence, if $F_q(\xi^t) = F_{q^m}$ (necessarily m divides n), then X_0 and X_m are in the same eigenspace and no X_i, $0 < i < m$, is in that eigenspace. The following result is now clear for $r = q^n - 1$. The case $r = (q^n - 1)/(q - 1)$ is similar.

THEOREM 2.2. *Suppose that $r = q^n - 1$ or $r = (q^n - 1)/(q - 1)$ and η is a primitive rth root of unity, so that $\langle T_\eta \rangle$ is either T or the unimodular subgroup of T. Then for an integer t, $0 < t < r$, and a positive integer m dividing n, the following are equivalent:*

(1) *$F_q(\eta^t) = F_{q^m}$;*

(2) *The eigenspaces of $T_\eta{}^t$ are the m spaces $\langle X_i |\, i \equiv \alpha \pmod{m} \rangle$, $\alpha = 0, 1, \ldots, m-1$, each of dimension n/m;*

(3) *t is a multiple of r/s_m but not of r/s_j for any $0 < j < m$ such that j divides m, where $s_i = (q^i - 1, r)$.*

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

Given r and t, where $r = q^n - 1$ or $r = (q^n - 1)/(q - 1)$ and $0 < t < r$, write $\mu(r, t)$ for the uniquely determined m dividing n satisfying (1)–(3).

COROLLARY 1. *Suppose that A is a Singer cycle in* $\mathrm{GL}(V)$ (*so that* $r = q^n - 1$) *or A is a Singer cycle in* $\mathrm{SL}(V)$ (*so that* $r = (q^n - 1)/(q - 1)$). *Then for* $0 < t < r$, *the eigenspaces of A^t are all of dimension $n/\mu(r, t)$. Consequently, n is a prime if and only if each non-scalar element of $\langle A \rangle$ has the same eigenspaces as A.*

COROLLARY 2. *n is a prime if and only if all the non-identity elements of a Singer group in* $\mathrm{PGL}(V)$ (*or in* $\mathrm{PSL}(V)$) *have the same fixed point set in $P(W)$.*

We have determined the eigenspaces of the elements of a Singer group in $\mathrm{GL}(V)$ and in $\mathrm{SL}(V)$. Certainly the eigenspaces of a Singer group itself are well-defined. We will now show that no two distinct Singer groups in $\mathrm{GL}(V)$ or in $\mathrm{SL}(V)$ have a non-zero eigenvector in common. Here we will use the matrix versions since the result is an easy consequence of the following general matrix proposition.

THEOREM 2.3. *Let E be a field, let L be a finite cyclic extension of E of degree $n \geqq 2$, and let σ be a generator of the automorphism group of L over E. Then there is an inner automorphism of L_n (the $n \times n$ matrices over L) which maps E_n onto the set of all matrices in L_n of the form*

$$(*) \qquad \begin{bmatrix} x_1 & x_2 & \cdot & \cdot & \cdot & x_n \\ x_n^{\sigma} & x_1^{\sigma} & \cdot & \cdot & \cdot & x_{n-1}^{\sigma} \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ x_2^{\sigma^{n-1}} & \cdot & \cdot & \cdot & x_n^{\sigma^{n-1}} & x_1^{\sigma^{n-1}} \end{bmatrix}.$$

Proof. Suppose that α is a primitive element of L over E. If

$$P = \begin{bmatrix} 1 & 1 & \cdot & \cdot & \cdot & 1 \\ \alpha & \alpha^{\sigma} & \cdot & \cdot & \cdot & \alpha^{\sigma^{n-1}} \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ \cdot & & & & & \cdot \\ \alpha^{n-1} & \alpha^{(n-1)\sigma} & \cdot & \cdot & \cdot & \alpha^{(n-1)\sigma^{n-1}} \end{bmatrix},$$

then one can easily check that the map $X \to P^{-1}XP$, $X \in L_n$, is the desired inner automorphism of L_n.

In the present context, we obtain the following theorem.

THEOREM 2.4. *There is an inner automorphism of* $\mathrm{GL}_n(q^n)$ *which maps* $\mathrm{GL}_n(q)$ *onto the set $C_n(q)$ of all matrices of* $\mathrm{GL}_n(q^n)$ *of the form* $(*)$. *Furthermore, there is a Singer cycle A in* $\mathrm{GL}_n(q)$ *whose image under this inner automorphism is diagonal.*

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

Proof. If $F_{q^n} = F_q(\xi)$, ξ a primitive $(q^n - 1)$-root of unity, and the minimum polynomial for ξ is $m(x) = a_0 + a_1x + \ldots + x^n$, (coefficients in F_q), then the corresponding companion matrix A is a Singer cycle in $\mathrm{GL}_n(q)$ whose image under the inner automorphism is $\mathrm{diag}\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$.

COROLLARY 3. *No two distinct Singer groups in* $\mathrm{GL}_n(q)$, *and hence in* $\mathrm{SL}_n(q)$, *have a common non-zero eigenvector in* W. *Thus, no two distinct Singer groups in* $\mathrm{PGL}_n(q)$ *or in* $\mathrm{PSL}_n(q)$ *have a common fixed point in* $P(W)$.

Proof. The eigenspaces of the Singer group in $C_n(q)$ generated by $A = \mathrm{diag}\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$ are spanned by $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0,1)$, respectively. If any Singer cycle B in $C_n(q)$ has one of these unit vectors as an eigenvector, then it is easy to check that B generates the same Singer group as A.

Our next goal is to determine the possible intersections of a Singer group with a conjugate. We would particularly like to know when a Singer group is a T.I. set.

Definition 2.5. A subgroup D of a group G is a trivial intersection (T.I.) set if $D \cap D^g = 1$ or D for all $g \in G$.

THEOREM 2.6. *Suppose that S is a Singer group in G and S^* is a distinct conjugate of S. Then for some positive proper divisor r of n, $|S^* \cap S|$ divides*

(i) $q^r - 1$ *if* $G = \mathrm{GL}_n(q)$,

(ii) $(q^r - 1)/(q - 1)$ *if* $G = \mathrm{PGL}_n(q)$,

(iii) $(q^r - 1, (q^n - 1)/(q - 1))$ *if* $G = \mathrm{SL}_n(q)$,

(iv) $(q^r - 1, (q^n - 1)/(q - 1))/(n, q - 1)$ *if* $G = \mathrm{PSL}_n(q)$,

and intersections of these orders exist for every positive proper divisor r of n.

Proof. We prove (i). The proof of (iii) is similar, and (ii) and (iv) are immediate consequences of (i) and (iii), respectively. By Theorem 2.4, S is similar in $\mathrm{GL}_n(q^n)$ to the group M generated by $A = \mathrm{diag}\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$, where ξ is a primitive $(q^n - 1)$-root of unity. Suppose that $M^x \cap M = \langle A^t \rangle$ for some $t > 1$ dividing $|M|$. A^t cannot have all its diagonal entries distinct since x does not normalize M. By Theorem 2.2, Corollary 1, t must be such that $\mu(q^n - 1, t) = r$ for some positive proper divisor r of n. By Theorem 2.2 (3), t is a multiple of $(q^n - 1)/(q^r - 1)$. Hence $|M^x \cap M|$ divides $q^r - 1$.

COROLLARY 4. *If n is a prime, the Singer groups in* $\mathrm{PGL}_n(q)$ *and* $\mathrm{PSL}_n(q)$ *are T.I. sets.*

On the other hand, let $t = (q^n - 1)/(q^r - 1)$ so that A^t has order $q^r - 1$ and A^t has every rth diagonal entry equal. Let x be a member of $C_n(q)$ (the group of all matrices of $\mathrm{GL}_n(q^n)$ of the form $(*)$) such that the only non-zero entries in the first row are x_1 and x_{r+1}. Then x normalizes $\langle A^t \rangle$ but does not normalize any larger subgroup of M; thus $|M^x \cap M| = q^r - 1$.

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

Let us turn our attention to the normalizers of the Singer groups. Higman and McLaughlin [**2**] have determined the normalizers of M in GL and H in PGL. They pointed out that if σ generates the automorphism group of F_{q^n} over F_q, then each member of $\langle\sigma\rangle$ may be considered as a non-singular linear transformation of the vector space $V = F_{q^n}$ over F_q, and hence induces a collineation of the projective space $P(V)$. If we denote this induced collineation group by $\langle\tau\rangle$, then $\langle\sigma\rangle$ and $\langle\tau\rangle$ are isomorphic, $\mathrm{N}_{\mathrm{GL}}(M) = M\langle\sigma\rangle$ and $\mathrm{N}_{\mathrm{PGL}}(H) = H\langle\tau\rangle$.

THEOREM 2.7.

$$\mathrm{N}_{\mathrm{SL}}(SM) = \mathrm{N}_{\mathrm{GL}}(M) \cap \mathrm{SL} \qquad \textit{and} \qquad \mathrm{N}_{\mathrm{PSL}}(K) = \mathrm{N}_{\mathrm{PGL}}(H) \cap \mathrm{PSL}.$$

Proof. Certainly $\mathrm{N}_{\mathrm{GL}}(M) \cap \mathrm{SL} \leqq \mathrm{N}_{\mathrm{SL}}(SM)$ since M is cyclic. If $x \in \mathrm{N}_{\mathrm{SL}}(SM)$, then $SM \leqq M^x \cap M$ and by Theorem 2.6 (i), $M^x \cap M = M$. The projective case is similar.

If $\sigma \in \mathrm{SL}$, then $\mathrm{N}_{\mathrm{SL}}(SM) = SM\langle\sigma\rangle$; thus the question arises, when is $\sigma \in \mathrm{SL}$? σ maps x to x^q, and so with respect to a normal basis,

$$\sigma = \begin{bmatrix} 0 & 1 & & & & \\ & \cdot & \cdot & & & \\ & & \cdot & \cdot & & \\ & & & \cdot & \cdot & \\ & & & & \cdot & 1 \\ 1 & & & & & 0 \end{bmatrix}$$

and this has determinant $(-1)^{n+1}$. Thus $\sigma \in \mathrm{SL}$ if and only if n is odd or n is even and q is a 2-power. Similarly, $\tau \in \mathrm{PSL}$ if and only if n is odd or n is even and there is a $\lambda \in F_q$ such that $\lambda^n = -1$. Using this and a coset decomposition when $\sigma \notin \mathrm{SL}$ or $\tau \notin \mathrm{PSL}$, one can easily see that the orders are as they should be.

THEOREM 2.8.

$$|\mathrm{N}_{\mathrm{SL}}(SM)| = |\mathrm{N}_{\mathrm{GL}}(M)|/(q-1) \quad \textit{and} \quad |\mathrm{N}_{\mathrm{PSL}}(K)| = |\mathrm{N}_{\mathrm{PGL}}(H)|/(n, q-1).$$

Remark. From this theorem and Corollary 3, it follows that when $n = 2$, every irrational point in $P(W)$ is a fixed point for some Singer group in $\mathrm{PSL}_2(q)$, for there are $(q^2 + 1) - (q + 1)$ irrational points, and there are $\mathrm{PSL}_2(q)\colon \mathrm{N}_{\mathrm{PSL}}(K) = q(q-1)/2$ distinct Singer groups each fixing two points, no two fixing the same point.

THEOREM 2.9. *The Singer groups are all self-centralizing.*

Proof. The normalizer of a Singer group in $\mathrm{GL}_n(q)$ is conjugate in $\mathrm{GL}_n(q^n)$ to $\langle A\rangle\langle\sigma\rangle$, where $A = \mathrm{diag}\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$, ξ is a primitive $(q^n - 1)$-root of unity, and σ is the above cyclic matrix. Then $1 \leqq i \leqq n$ and σ^i centralizes A (even up to a scalar) implies $i = n$; thus the Singer groups in GL and PGL are self-centralizing. The unimodular case is similar.

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

THEOREM 2.10. $\mathrm{N}_{\mathrm{PSL}}(K)$ *is a Frobenius group with Frobenius kernel* K *if and only if* n *is an odd prime or* $n = 2$ *and* $4 \nmid (q+1)$.

Proof. Set $N = \mathrm{N}_{\mathrm{PSL}}(K)$. We determine when $1 \neq x \in K$ implies $\mathrm{C}_N(x) \leqq K$ by determining when the elements which fix all non-scalar members of SM up to a scalar are contained in SM. Let $SM = \langle A \rangle$, where $A = \mathrm{diag}\{\lambda, \lambda^q, \ldots, \lambda^{q^{n-1}}\}$, λ a primitive $(q^n - 1)/(q-1)$ root of unity. Then $\mathrm{N}_{\mathrm{SL}}(SM) = \langle A \rangle \langle \gamma \rangle$, where $\gamma = \sigma$ if $\sigma \in \mathrm{SL}_n(q)$ and $\gamma = g\sigma$ otherwise, where $g \in M$ and $\det g = -1$.

If n is not a prime, then for a divisor r of n, $1 < r < n$, there is a t such that A^t has every rth diagonal entry equal. γ^r centralizes A^t, and hence N is not Frobenius. Assume that n is a prime. If A^t is not scalar, then A^t has no two diagonal entries equal; thus for N not to be Frobenius there must be some s less than n such that γ^s fixes A^t up to a scalar different from I. However, this only happens when $n = 2$ and 4 divides $q+1$.

The normalizer of a Singer group in GL, SL, or PGL cannot be Frobenius unless there is an isomorphism with PSL. It should be mentioned that the image of the normalizer in $\mathrm{SL}_2(q)$ of the diagonal subgroup is a Frobenius subgroup of $\mathrm{PSL}_2(q)$ in case $4|(q+1)$.

In the next two theorems, $\mathrm{G}_n(q)$ will denote any of $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, or $\mathrm{PSL}_n(q)$. These theorems give conditions for a subgroup of $\mathrm{G}_n(q)$ to be contained in a Singer group.

THEOREM 2.11. *Given a Singer group* S *in* $\mathrm{G}_n(q)$, *suppose that* U *is an abelian subgroup of* $\mathrm{G}_n(q)$ *of order dividing* $|S|$, *and that there is a prime* r *dividing* $|U|$ *such that* $(r, \mathrm{G}_n(q): S) = 1$. *Then* $U^x \leqq S$ *for some* $x \in \mathrm{G}_n(q)$.

Proof. Suppose that $\mathrm{G}_n(q) = \mathrm{GL}_n(q)$. Let R be the r-Sylow subgroup of $\mathrm{GL}_n(q)$ contained in S. Then there is an $x \in \mathrm{GL}_n(q)$ such that $U^x \cap R \neq 1$. In $\mathrm{GL}_n(q^n)$, S is similar to the group S' generated by $A = \mathrm{diag}\{\xi, \xi^q, \ldots, \xi^{q^{n-1}}\}$, ξ a primitive $(q^n - 1)$-root of unity. Let R' and U' denote the images of R and U^x, respectively, under this similarity. Now $(r, \mathrm{GL}_n(q) : S) = 1$ implies $(r, q^i - 1) = 1$ for all i, $1 \leqq i < n$; thus by Theorem 2.2 and Corollary 1, the non-identity matrices in R' have distinct diagonal entries. Since U is abelian, $U^x \leqq \mathrm{C}(U^x \cap R)$; thus the matrices in U' are diagonal. Therefore they centralize S', a self-centralizing group, and hence $U^x \leqq S$.

Since $(r, q-1) = 1$, R is in $\mathrm{SL}_n(q)$; thus the result holds when $\mathrm{G}_n(q) = \mathrm{SL}_n(q)$. The projective cases are similar.

THEOREM 2.12. *Given a Singer group in* $\mathrm{G}_n(q)$ *and an abelian subgroup* U *of* $\mathrm{G}_n(q)$ *of the same order, then* U *is conjugate to the Singer group except possibly for* $\mathrm{G}_6(2)$ *or* $\mathrm{G}_2(p)$, *where* $p + 1 = 2^a$ *for some* a.

Proof. By the previous theorem, we need only show that there is a prime r dividing $|U|$ but $(r, \mathrm{G}_n(q): U) = 1$. Such an r exists by the following result [**1**, p. 358, Corollary 2].

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

If p is a prime and s, t are positive integers, then there is a prime r such that $r|(p^t - 1)$ but $r \nmid (p^s - 1)$, $s < t$, except for

(1) *$t = 2$ and $p + 1 = 2^a$ for some a, or*

(2) $p^t = 64$.

A simple calculation shows that the only exception (2) gives in our case is $n = 6$ and $q = 2$.

$\mathrm{PSL}_2(11)$ demonstrates that the abelian hypothesis cannot be dropped, since $|K| = 6$ and $|\mathrm{N}_{\mathrm{PSL}}(K)| = 12$, and thus there is also a dihedral subgroup of order 6.

By considering orders, we have the following result.

THEOREM 2.13. *A Singer group K is a Hall subgroup of* $\mathrm{PSL}_n(q)$ *if and only if n is an odd prime or $n = 2$ and $4 \nmid (q + 1)$.*

Much of our attention will be focused on this case. Here Theorems 2.11 and 2.12 with $\mathrm{G}_n(q) = \mathrm{PSL}_n(q)$ can be obtained without the abelian assumption just by citing a theorem of Wielandt [**6**, p. 230], but this powerful theorem seems out of character with the previous discussion.

In closing this section we mention the following: Suppose that π is a finite Desarguesian projective space of dimension $n - 1$. A question which arises naturally is exactly what are the subgroups G of the collineation group of π which are regular on the points of π? (π, G) is then a projective incidence group in the sense of Karzel [**4**]. He showed that if $n \geqq 3$, then there exists a unique normal nearfield (F, L) (L is a sub-skewfield of F coordinating π) such that G is isomorphic to F^*/L^*. Since π is finite, G is cyclic; thus by Theorem 2.12, G is a Singer group in $\mathrm{PGL}_n(q)$. There are some exceptions when $n = 2$, but at least the normalizer of G is not Frobenius in any of the exceptional cases.

3. Some Frobenius regular representations of $\mathrm{PSL}(q)$.

In this section we study in detail some Frobenius regular representations of $\mathrm{PSL}_n(q)$ afforded by the Singer groups. A Singer group K in $\mathrm{PSL}_n(q)$ is a T.I. set in $\mathrm{PSL}_n(q)$ when n is a prime (by Corollary 4). By Theorem 2.10, $\mathrm{N}(K) = \mathrm{N}_{\mathrm{PSL}}(K)$ is a Frobenius group with Frobenius kernel K if and only if n is an odd prime or $n = 2$ and $4 \nmid (q + 1)$. When $\mathrm{N}(K)$ is a Frobenius group, a Frobenius complement E in $\mathrm{N}(K)$ is a cyclic group of prime order n; thus E is certainly a T.I. set in $\mathrm{PSL}_n(q)$. Hence by Lemma 1.5, we have the following result.

THEOREM 3.1. $\mathrm{PSL}_n(q)$ *is faithfully represented as a Frobenius regular group on the set Ω of left cosets of* $\mathrm{PSL}_n(q)$ (mod $\mathrm{N}(K)$) *if and only if n is an odd prime or $n = 2$ and $4 \nmid (q + 1)$.*

In order to apply Lemma 1.6, we need to know the structure of $\mathrm{N}(E)$. Let us first consider the case $n = 2$ and $4 \nmid (q + 1)$. Since there is only one class of involutions in $\mathrm{PSL}_2(q)$, we may pick any involution that is convenient and it will generate a complement E for some Singer group K.

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

LEMMA 3.2. *If* $n = 2$ *and* $q = 2^m$, *then* $\mathrm{C}(E)$ *is elementary abelian of order* q.

Proof. $\mathrm{PSL}_2(q)$ is isomorphic to $\mathrm{SL}_2(q)$; thus assume that $E = \langle\tau\rangle$, where

$$\tau = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

The matrices which centralize τ have the form

$$\begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}, \qquad a \in F_q,$$

and the set of all such matrices form an elementary abelian group of order q.

THEOREM 3.3. $\mathrm{PSL}_2(q)$, $q = 2^m$, *has a* $[(q - 2)/2, 0]$-*Frobenius regular representation. The Frobenius orbits are all self-paired with* $q + 1$ *points.*

Proof. By Lemma 1.6, the number of Frobenius orbits is $(\mathrm{N}(E){:}E) - 1$, and since $\mathrm{N}(E) = \mathrm{C}(E)$, this is $(q/2) - 1$. Every Frobenius orbit is self-paired since $\mathrm{C}(E)/E$ elementary abelian of order $q/2$ implies $\mathrm{C}(E)/E$ contains $(q/2) - 1$ involutions. The $q + 1$ points in each of the $(q - 2)/2$ Frobenius orbits plus the one point in the trivial orbit account for the $q(q - 1)/2$ points, and hence there are no regular orbits.

LEMMA 3.4. *If* $n = 2$ *and* $2||(q + 1)$, *then* $\mathrm{C}(E)$ *is dihedral of order* $q - 1$.

Proof. Since $4|(q - 1)$, -1 is a square in F_q, say $a^2 = -1$. Suppose that E is the image in PSL of $\langle\gamma\rangle$, $\gamma = \mathrm{diag}\{a, -a\}$. Since a and $-a$ are distinct, the diagonal subgroup of SL is the centralizer of γ in SL. The image D in PSL of this subgroup has order $(q - 1)/2$.

$$\tau = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

normalizes $\langle\gamma\rangle$, and therefore its image η in PSL centralizes E. τ inverts the diagonal matrices of SL, and hence $\mathrm{C}(E)$ is the dihedral group $\langle\eta\rangle D$ of order $q - 1$.

THEOREM 3.5. *If* $2||(q + 1)$, *then* $\mathrm{PSL}_2(q)$ *has a* $[(q - 3)/2, (q - 1)/4]$-*Frobenius regular representation. The number of points in each Frobenius and regular orbit is* $(q + 1)/2$ *and* $q + 1$, *respectively, and the number of self-paired Frobenius orbits is* $\delta + (q - 1)/4$, *where* $\delta \in \{0, 1\}$ *and* $\delta \equiv (q - 5)/4 \pmod 2$.

Proof. $\mathrm{N}(E) = \mathrm{C}(E)$, and thus $\mathrm{N}(E){:}E = (q - 1)/2$ is the number of Frobenius orbits plus one. There are $q(q - 1)/2$ points all together, and from the number of points in each Frobenius and regular orbit, the number $(q - 1)/4$ of regular orbits is easily determined. The number of self-paired Frobenius orbits is the number of involutions in D/E plus the order of D/E.

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

From now on we will assume that n is an odd prime. E is a cyclic group generated by the image τ of some matrix $\sigma \in \mathrm{SL}_n(q)$. Usually, it will be convenient to assume that σ has the form obtained by using a normal basis:

$$\sigma = \begin{bmatrix} 0 & 1 & & & & \\ & \cdot & \cdot & & & \\ & & \cdot & \cdot & & \\ & & & \cdot & \cdot & \\ & & & & \cdot & 1 \\ 1 & & & & & 0 \end{bmatrix}.$$

Lemma 3.6. $\mathrm{N}(E)/\mathrm{C}(E)$ *is cyclic of order* $n - 1$.

Proof. To show that $\mathrm{N}(E)/\mathrm{C}(E)$ is the full automorphism group of E, it suffices to show that there is an element $\rho \in \mathrm{SL}_n(q)$ such that ρ has order $n - 1$ and all the non-identity members of $\langle\rho\rangle$ normalize but do not centralize $\langle\sigma\rangle$. Let ζ be a primitive $(n - 1)$-root of unity in $\mathbf{Z}_n$. Consider the permutation matrix such that the 1 in the $(i + (n + 1)/2)$-row,

$$-(n - 1)/2 \leqq i \leqq (n - 1)/2,$$

is in the $(1 + j)$-column, where $j \equiv i\zeta + (n - 1)/2 \pmod{n}$. Set ρ equal to plus or minus the matrix, the sign chosen so that ρ has determinant one. Then $\rho^{-1}\sigma\rho = \sigma^{\zeta}$ and ρ^t, $1 \leqq t < n - 1$, normalizes but does not centralize $\langle\sigma\rangle$.

The element of order 2 in $\langle\rho\rangle$ has a desirable form. Namely, the non-zero entry in row i is $(-1)^{(n-1)/2}$ in the $(n + 1 - i)$-column. This will be useful in applying Lemma 1.5, for if J is the element of order 2 in $\mathrm{N}(E)/\mathrm{C}(E)$, then the number of involutions in $\mathrm{N}(E)/E$ is the number of involutions in $\mathrm{C}(E)/E$ plus the order of the subgroup of $\mathrm{C}(E)/E$ inverted by J.

Let us now consider the case when $q \equiv 0 \pmod{n}$.

Lemma 3.7. *If* $q = p^m$ *and* $n = p$, *where* p *is an odd prime, then* $\mathrm{C}(E)$ *is elementary abelian of order* q^{p-1}.

Proof. $\mathrm{SL}_n(q) = \mathrm{PSL}_n(q)$, and hence we work in $\mathrm{SL}_n(q)$. Instead of letting E be generated by the usual cyclic matrix σ, it is easier to look at $E = \langle\gamma\rangle$, where γ is the unipotent matrix

$$\begin{bmatrix} 1 & & & & & & \\ 1 & \cdot & & & & & \\ & \cdot & \cdot & & & & \\ & & \cdot & \cdot & & & \\ & & & \cdot & \cdot & & \\ & & & & 1 & \cdot & \\ & & & & & \alpha & 1 \end{bmatrix}, \qquad \alpha = (-1)^{(p-1)/2}.$$

Then $X \in \mathrm{C}(E)$ if and only if X has the form

$$\begin{bmatrix} 1 & & & & & & \\ x_2 & \cdot & & & & & \\ \cdot & \cdot & \cdot & & & & \\ \cdot & & \cdot & \cdot & & & \\ \cdot & & & \cdot & \cdot & & \\ x_{p-1} & \cdot & \cdot & \cdot & x_2 & 1 & \\ x_p & \alpha x_{p-1} & \cdot & \cdot & \cdot & \alpha x_2 & 1 \end{bmatrix}$$

and the set of all such matrices forms an elementary abelian group of order q^{p-1}.

Lemma 3.8. *If $q = p^m$ and $p = n$, where p is an odd prime, then a generator ρ of* $\mathrm{N}(E)/\mathrm{C}(E)$ *centralizes a subgroup of* $\mathrm{C}(E)$ *of order q. If $J = \rho^{(p-1)/2}$, then* $\mathrm{C}(E) = V \times W$, *where $|V| = |W| = q^{(p-1)/2}$, J centralizes W, and J inverts the elements of V, $E \leqq V$.*

Proof. Assume that E is generated by the usual cyclic matrix σ. Then the form of the elements in $\mathrm{C}(E)$ is

$$X = \begin{bmatrix} x_1 & x_2 & \cdot & \cdot & \cdot & x_p \\ x_p & \cdot & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \cdot & \cdot & x_2 \\ x_2 & \cdot & \cdot & \cdot & x_p & x_1 \end{bmatrix}$$

and ρ is the matrix described in the proof of Lemma 3.6. Since $\rho^{-1}[x_2\sigma]\rho = x_2\sigma^\zeta$, etc., and ζ is a primitive $(\rho - 1)$-root of unity in $\mathbf{Z}_p$, it follows that a necessary and sufficient condition for ρ to centralize X is that $x_2 = \ldots = x_p$. Hence ρ centralizes a subgroup of $\mathrm{C}(E)$ of order q.

Since $J = \rho^{(p-1)/2}$, we see that

$$J = \begin{bmatrix} \mathbf{0} & & & \alpha \\ & & \cdot & \\ & \cdot & & \\ \alpha & \cdot & & \mathbf{0} \end{bmatrix}, \quad \text{where } \alpha = (-1)^{(p-1)/2};$$

thus if we conjugate $X \in \mathrm{C}(E)$ by J we obtain the transpose of X. Hence $JXJ = X$ if and only if $x_2 = x_p$, $x_3 = x_{p-1}, \ldots, x_{(p+3)/2} = x_{(p+1)/2}$. Thus J centralizes a subgroup W of $\mathrm{C}(E)$ of order $q^{(p-1)/2}$. If we consider J acting on $\mathrm{C}(E)$ as a transformation T of period 2 acting on a vector space V_0 of dimension $m(p-1)$, then this vector space can be written as $V_0 = V_1 \oplus V_2$, where V_1 is a subspace consisting of vectors fixed by T and V_2 is a subspace consisting of vectors sent onto their negatives by T. Since $|W| = q^{(p-1)/2}$ and $q = p^m$, the dimension of V_1 is $m(p-1)/2$. Hence V_2 also has dimension

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

$m(p-1)/2$; thus J inverts a subgroup V of $\mathrm{C}(E)$ of order $q^{(p-1)/2}$. (Note that $E \leqq V$.)

THEOREM 3.9. *If $q = p^m$, p an odd prime, then $\mathrm{PSL}_p(q)$ has a $[(p-1)q^{p-1}/p - 1, \beta]$-Frobenius regular representation, where*

$$\beta = \frac{(q^{p-1}-1)q}{(q^p-1)p}\left\{\frac{q^{(p-2)(p+1)/2}}{p}(q-1)\prod_{i=1}^{p-2}(q^i-1)+1\right\} - \frac{(p-1)q^{p-1}}{p^2}.$$

The Frobenius and regular orbits have $(q^p-1)/(q-1)$ and $p(q^p-1)/(q-1)$ points, respectively. There are $q^{(p-1)/2}/p$ self-paired Frobenius orbits.

Proof. By Lemmas 3.6 and 3.7, $\mathrm{N}(E){:}E = (p-1)q^{p-1}/p$, and this is one more than the number of Frobenius orbits. From this, the number of points in each Frobenius and regular orbit, and the fact that there are

$$(q^{p(p-1)/2}/p)\prod_{i=1}^{p-1}(q^i-1)$$

total points, β can be determined. The number of involutions in $\mathrm{N}(E)$ is just the order $q^{(p-1)/2}$ of the subgroup V of $\mathrm{C}(E)$ which is inverted by J. Since E is a subgroup of V, the number of involutions in $\mathrm{N}(E)/E$ is $q^{(p-1)/2}/p$.

Now consider the case $q \equiv 1 \pmod{n}$.

LEMMA 3.10. *If $q \equiv 1 \pmod{n}$, n an odd prime, then $\mathrm{C}(E)$ is the semi-direct product of a cyclic group of order n and a group B of order $(q-1)^{n-1}/n$, where B is the direct product of $n-2$ cyclic groups of order $q-1$ and one of order $(q-1)/n$.*

Proof. The usual cyclic matrix σ has characteristic equation $x^n - 1 = 0$. Since $n|(q-1)$, this equation has roots $1, \beta, \beta^2, \ldots, \beta^{n-1}$, where $\beta \in F_q$ and β has order n. Thus σ is similar to the matrix $\gamma = \mathrm{diag}\{1, \beta, \ldots, \beta^{n-1}\}$, and hence we can assume that E is the image of $\langle\gamma\rangle$. Since γ is diagonal with distinct entries, the centralizer of γ in SL is the diagonal subgroup D of SL. D is the direct product of $n-1$ cyclic groups of order $q-1$ with one of them containing the scalar matrices; thus the image in PSL of D is just B. On the other hand, the coset containing γ is $\{\beta^i\gamma |\, i = 1, \ldots, n\}$, and $\beta^i\gamma$ is just a cyclic permutation of the diagonal entries of γ; thus σ leaves this set invariant. Hence since σ normalizes the diagonal subgroup of SL, $\mathrm{C}(E)$ is the semi-direct product of B and the image of $\langle\sigma\rangle$.

LEMMA 3.11. *If $q \equiv 1 \pmod{n}$, n an odd prime, then a generator of $\mathrm{N}(E)/\mathrm{C}(E)$ centralizes a subgroup of $\mathrm{C}(E)$ of order $(q-1)/n$. The element of order 2 in $\mathrm{N}(E)/\mathrm{C}(E)$ centralizes a subgroup W of $\mathrm{C}(E)$ of order $(q-1)^{(n-1)/2}/n$, and inverts a subgroup V of $\mathrm{C}(E)$ of order $n(q-1)^{(n-1)/2}$ which contains E.*

Proof. Since E is the image of $\langle\gamma\rangle$ and all the non-identity members of $\langle\gamma\rangle$ just differ by permutations of the $n-1$ elements $\beta, \ldots, \beta^{n-1}$, we can assume

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

that a generator for $\mathrm{N}(E)/\mathrm{C}(E)$ is $\rho = \pm\,\mathrm{diag}\{1, \rho'\}$, where ρ' is an appropriate permutation matrix and the sign is chosen so that $\det \rho = 1$. If $X \in D\langle\sigma\rangle$, then $X = Y\sigma^i$, where $Y = \mathrm{diag}\{a_0, a_1, \ldots, a_{n-1}\}$. From the above description of ρ, it follows that ρ centralizes X if and only if $\sigma^i = I$ and $a_1 = a_2 = \ldots = a_n$. The group of all such X has order $q - 1$. Since this group includes the scalar matrices, a generator of $\mathrm{N}(E)/\mathrm{C}(E)$ centralizes a subgroup of $\mathrm{C}(E)$ of order $(q-1)/n$.

ρ can be chosen so that $\rho^{(n-1)/2}$ is

$$J = \left[\begin{array}{c|cccc} \alpha & & & & \\ \hline & & & & \alpha \\ & & & \cdot & \\ & & \cdot & & \\ & \cdot & & & \\ & \alpha & & & \end{array}\right], \qquad \text{where } \alpha = (-1)^{(n-1)/2}.$$

The matrices of $D\langle\sigma\rangle$ which are centralized by J have the form

$$\mathrm{diag}\{a_0, a_1, \ldots, a_{(n-1)/2}, a_{(n-1)/2}, \ldots, a_1\}.$$

Since the scalar matrices have this form, it follows that the involution in $\mathrm{N}(E)/\mathrm{C}(E)$ centralizes a subgroup W of $\mathrm{C}(E)$ of order $(q-1)^{(n-1)/2}/n$. The matrices of D inverted by J have the form

$$\mathrm{diag}\{1, a_1, \ldots, a_{(n-1)/2}, a_{(n-1)/2}^{-1}, \ldots, a_1^{-1}\},$$

and $\langle\sigma\rangle$ is inverted by J. Hence the involution in $\mathrm{N}(E)/\mathrm{C}(E)$ inverts a subgroup V of $\mathrm{C}(E)$ of order $n(q-1)^{(n-1)/2}$ containing E.

THEOREM 3.12. *If $q \equiv 1 \pmod{n}$, n an odd prime, then $\mathrm{PSL}_n(q)$ has an $[(n-1)(q-1)^{n-1}/n - 1, \beta]$-Frobenius regular representation, where*

$$\beta = \frac{q-1}{q^n-1}\left\{\frac{q^{n(n-1)/2}}{n}\prod_{i=1}^{n-1}(q^i-1) - 1 - \left[\frac{(n-1)(q-1)^{n-1}}{n} - 1\right]\frac{q^n-1}{n(q-1)}\right\}.$$

The Frobenius and regular orbits have $(q^n-1)/n(q-1)$ and $(q^n-1)/(q-1)$ points, respectively. There are $\delta(2^{n-1}-1) + (q-1)^{(n-1)/2}$ self-paired Frobenius orbits, where $\delta \in \{0, 1\}$ and $\delta \equiv q \pmod{2}$.

The proof of this theorem is similar to that of Theorem 3.9, and therefore is omitted.

The last case we will consider is where $q \not\equiv 0$, $q \not\equiv 1 \pmod{n}$, n is an odd prime, and in addition $(n, q^i - 1) = 1$ whenever $i \mid (n-1)$, $1 < i < n-1$.

LEMMA 3.13. *If n is an odd prime, $q \not\equiv 0$, $q \not\equiv 1 \pmod{n}$, and $(n, q^i-1) = 1$ whenever $i \mid (n-1)$, $1 < i < n-1$, then $\mathrm{C}(E)$ is cyclic of order $q^{n-1} - 1$.*

Proof. Since $q \not\equiv 1 \pmod{n}$ and n is a prime, we can again identify $\mathrm{PSL}_n(q)$ with $\mathrm{SL}_n(q)$ and assume that E is generated by the cyclic matrix σ. The characteristic equation of σ is still $x^n - 1 = 0$. If m is such that $(x-1)^m \| (x^n - 1)$, then σ is similar to

$$m\left\{\begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array}\right. \!\!\left[\begin{array}{ccccc|c} 1 & & & & & \\ 1 & \cdot & & & & \\ & \cdot & \cdot & & & \\ & & \cdot & \cdot & & \\ & & & \cdot & \cdot & \\ & & & 1 & 1 & \\ \hline & & & & & \tau \end{array}\right].$$

p divides the order of this matrix unless $m = 1$, but σ has order n and $q \not\equiv 0 \pmod{n}$, and hence $m = 1$. Thus σ is similar to $\gamma = \operatorname{diag}\{1, \tau\}$, where $\tau \in SL_{n-1}(q)$ and τ has order n; thus assume that $E = \langle\gamma\rangle$.

The matrices $X \in C(E)$ have the form $\operatorname{diag}\{a, Y\}$, where Y is in the centralizer of τ in $GL_{n-1}(q)$ and $a^{-1} = \det Y$. Thus finding $C(E)$ is reduced to finding $C_{GL_{n-1}}(\tau)$. By Fermat's theorem, $q^{n-1} \equiv 1 \pmod{n}$, and from the assumptions it follows that $n \nmid (q^i - 1)$ for $1 \leqq i < n - 1$. Hence if SM is a Singer group in $SL_{n-1}(q)$, then $|\langle\tau\rangle| = n \mid |SM|$ and $(n, SL_{n-1}(q){:}SM) = 1$; thus by Theorem 2.11, $\langle\tau\rangle$ is a subgroup of some Singer group in $SL_{n-1}(q)$. By Theorem 2.6 there is a unique Singer group M in $GL_{n-1}(q)$ containing τ, since n does not divide the order of the intersection of M with a distinct conjugate. From this it follows easily that anything centralizing τ centralizes M, which is a self-centralizing subgroup of $GL_{n-1}(q)$ (Theorem 2.9).

LEMMA 3.14. *A generator of* $N(E)/C(E)$ *centralizes a subgroup of* $C(E)$ *of order* $q - 1$. *The element of order* 2 *in* $N(E)/C(E)$ *centralizes a subgroup* W *of* $C(E)$ *of order* $q^{(n-1)/2} - 1$ *and inverts a subgroup* V *of order* $q^{(n-1)/2} + 1$ *containing* E.

Proof. If E and $C(E)$ are as above, when we pass to the extension field $F_{q^{n-1}}$, a generator $\operatorname{diag}\{a, Y\}$ of $C(E)$ is similar to $X = \operatorname{diag}\{a, Z\}$, where $Z = \operatorname{diag}\{\xi, \xi^q, \ldots, \xi^{q^{n-2}}\}$ and ξ is a primitive $(q^{n-1} - 1)$-root of unity. Set $\gamma = X^{(q^{n-1}-1)/n}$ and assume that $E = \langle\gamma\rangle$. It follows from the discussion of intersections of Singer groups that γ has distinct diagonal entries; thus

$$\rho = (-1)\left[\begin{array}{c|cccccc} 1 & & & & & & \\ \hline & 0 & 1 & & & & \\ & & \cdot & \cdot & & & \\ & & & \cdot & \cdot & & \\ & & & & \cdot & \cdot & \\ & & & & & \cdot & 1 \\ & 1 & & & & & 0 \end{array}\right]$$

is isomorphic to a generator of $N(E)/C(E)$. ρ centralizes X^t if and only if

$\xi^t = \xi^{tq} = \ldots = \xi^{tq^{n-2}}$; hence ρ centralizes a subgroup of $C(E)$ of order $q - 1$.
The element of order 2 in $\langle \rho \rangle$ is

$$J = (-1)^{(n-1)/2} \begin{bmatrix} 1 & & \\ & 0 & I \\ & I & 0 \end{bmatrix}.$$

From this it is easy to check that J centralizes a subgroup W of $C(E)$ of order $q^{(n-1)/2} - 1$ and inverts a subgroup V of order $q^{(n-1)/2} + 1$.

THEOREM 3.15. *If n is an odd prime, $q \not\equiv 0$, $q \not\equiv 1 \pmod{n}$, and $(n, q^i - 1) = 1$ whenever $i | (n-1)$, $1 < i < n - 1$, then* $\mathrm{PSL}_n(q)$ *has an* $[(n-1)(q^{n-1}-1)/n - 1, \beta]$*-Frobenius regular representation, where*

$$\beta = \frac{q-1}{n(q^n-1)} \left\{ \frac{q^{n(n-1)/2}}{n} \prod_{i=1}^{n-1} (q^i - 1) - 1 - \left[\frac{(n-1)(q^{n-1}-1)}{n} - 1 \right] \frac{q^n - 1}{q-1} \right\}.$$

The Frobenius and regular orbits have $(q^n - 1)/(q-1)$ *and* $n(q^n-1)/(q-1)$ *points, respectively. The number of self-paired Frobenius orbits is*

$$\delta + (q^{(n-1)/2} + 1)/n,$$

where $\delta \in \{0, 1\}$ *and* $\delta \equiv q \pmod{2}$.

The proof is omitted.

4. Cyclic self-centralizing T.I. sets. It has been shown that when n is an odd prime or $n = 2$ and $4 \nmid (q + 1)$, a Singer group K in $\mathrm{PSL}_n(q)$ may be used to obtain a Frobenius regular representation of $\mathrm{PSL}_n(q)$. Now we would like to determine all the cyclic subgroups of $\mathrm{PSL}_n(q)$ affording such a representation. It is evident from Lemma 1.5 that such a subgroup must at least be a cyclic self-centralizing T.I. set in $\mathrm{PSL}_n(q)$, and there are very few of these.

THEOREM 4.1. *Suppose that $n \geqq 3$ and G is a cyclic self-centralizing T.I. set in* $\mathrm{PSL}_n(q)$. *Then one of the following holds:*

(i) *n is a prime and $G = K_n(q)$,*

(ii) *$n - 1$ is a prime, $(q - 1) | n$, and G is conjugate to some $K_{n-1}(q)$,*

(iii) *$n = 3$, $q = 2$, and G is conjugate to $\langle A \rangle$, where*

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Proof. The cyclic subgroups G of $\mathrm{PSL}_n(q)$ are the images of the subgroups $D\langle A \rangle$ of $\mathrm{SL}_n(q)$, where D is the diagonal subgroup of $\mathrm{SL}_n(q)$ and $A \in \mathrm{SL}_n(q)$. As A runs through the possible classical canonical forms, we will attempt to show that the corresponding G is not a self-centralizing T.I. set either by showing that $D\langle A \rangle$ is not self-centralizing in $\mathrm{SL}_n(q)$, or by producing a distinct conjugate of $\langle A \rangle$ whose intersection with $\langle A \rangle$ is non-scalar. When this attempt fails, we will show that the corresponding G is a self-centralizing T.I. set.

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

$xI - A$ is similar to $\operatorname{diag}\{1, \ldots, 1, \delta_1, \ldots, \delta_r\}$, where the δ_i are monic polynomials in x, and $\delta_i | \delta_{i+1}$, $i = 1, \ldots, r - 1$. We will investigate the various possibilities for these invariant factors. In what follows, $f(x)$, $g(x)$, etc., will always denote irreducible functions, and the notation $f^s(x)$ will always carry the tacit assumption that $s > 0$.

Assume that $f^s(x) \| \delta_i$ and $f^s(x) \| \delta_{i+1}$ for some $i < r$. Then A contains two identical blocks C along the diagonal corresponding to the elementary divisors $f^s(x)$. Certainly there is an $X \in \mathrm{SL}_n(q)$ which interchanges the two blocks and fixes everything else; thus G is not self-centralizing. Hence,

(1) If $f^s(x) \| \delta_i$, $i < r$, then $f^t(x) \| \delta_{i+1}$, where $t > s$.

Assume that $\deg f(x) > 1$, $s > 1$, and $f^s(x) \| \delta_i$ for some i. Then the block C on the diagonal of A corresponding to the elementary divisor $f^s(x)$ has the form

$$C = \begin{bmatrix} B & & & & \\ N & B & & & \\ \cdot & \cdot & & & \\ & \cdot & \cdot & & \\ & & \cdot & \cdot & \\ & & & N & B \end{bmatrix}, \qquad \text{where } N = \begin{bmatrix} & \mathbf{0} \\ 1 & \end{bmatrix},$$

and B is the companion matrix for $f(x)$. The group generated by all matrices of the form

$$\begin{bmatrix} I & & & & & & \\ & \cdot & & & & & \\ & & \cdot & & & & \\ & & & \cdot & & & \\ & & & & \cdot & & \\ & & & & & \cdot & \\ & & & & & & \cdot \\ B^j & & & & & & I \end{bmatrix}, \qquad j = 1, \ldots, |B|,$$

is a non-cyclic group which commutes with C. Hence,

(2) If $\deg f(x) > 1$ and $s > 1$, then $f^s(x) \nmid \delta_i$, $i = 1, \ldots, r$.

Assume that $\deg f(x) = 1$, $s > 1$, and $f^s(x) \| \delta_i$ for some i. The block C of A corresponding to $f^s(x)$ has the same form as above (of course $B = b$ and $N = 1$). C is centralized by the group of matrices of the form

$$\begin{bmatrix} 1 & & & & \\ a_2 & \cdot & & & \\ \cdot & \cdot & \cdot & & \\ \cdot & & \cdot & \cdot & \\ \cdot & & & \cdot & \cdot \\ a_s & \cdot & \cdot & \cdot & a_2 & 1 \end{bmatrix}.$$

This group is not cyclic unless $s = 2$ and $q = p$ or $s = 3$ and $q = 2$. Hence,

(3) If $\deg f(x) = 1$, $s > 1$, and $f^s(x)||\delta_i$ for some i, then $s = 2$ and $q = p$ or $s = 3$ and $q = 2$.

If (3) holds for some $i > 1$ and $f(x)|\delta_{i-1}$, it is easy to show that $D\langle A\rangle$ is not self-centralizing. Hence,

(4) If $\deg f(x) = 1$ and $f^s(x)||\delta_i$ for some $i > 1$, where $s = 2$ and $q = p$ or $s = 3$ and $q = 2$, then $f(x) \nmid \delta_{i-1}$.

Combining (1) through (4), we have:

(5) There is a single invariant factor δ, and the only possible reducible elementary divisors are described in (3).

Assume that $f(x)||\delta$ and $g(x)||\delta$, where $f(x) \neq g(x)$ but

$$\deg f(x) = \deg g(x) = r > 1.$$

Then the blocks U and V of A corresponding to $f(x)$ and $g(x)$, respectively, are both matrices from Singer groups in $\mathrm{GL}_r(q)$. Suppose that $A = \mathrm{diag}\{U, V, W\}$ and X generates the unimodular subgroup of the Singer group containing U. Then $\mathrm{diag}\{X, I, I\}$ centralizes A but is not in $D\langle A\rangle$. If $f^s(x)||\delta$ and $g^s(x)||\delta$, where $f(x) \neq g(x)$ but $\deg f(x) = \deg g(x) = 1$ and $s = 1$ or $q = p$ and $s = 2$, then it is also possible to find a matrix not in $D\langle A\rangle$ which centralizes A.

(6) The following possibilities for δ remain:

$$\begin{aligned} \delta &= f_1(x)\ldots f_l(x) && \text{if } q = p^m,\\ &= g^2(x)f_1(x)\ldots f_l(x) && \text{if } q = p,\\ &= (x-1)^3 f_1(x)\ldots f_l(x) && \text{if } q = 2,\end{aligned}$$

where $\deg g(x) = 1$ and $\deg f_i(x) < \deg f_{i+1}(x)$.

Assume that $f(x)||\delta$ and $\deg f(x) = r > 1$. Then the block C of A corresponding to $f(x)$ is contained in a Singer group in $\mathrm{GL}_r(q)$. Certainly C must generate the largest Singer group consistent with the circumstances in order that G be self-centralizing. However, if r is not a prime, the Singer group in $\mathrm{PGL}_r(q)$ corresponding to $\langle C\rangle$ is not a T.I. set by Theorem 2.6. Hence,

(7) If $f(x)||\delta$, then the degree of $f(x)$ is 1 or a prime.

Assume that δ contains two non-linear elementary divisors e_1 and e_2. By (6) and (7), one of e_1, e_2, say e_1, is $f_i(x)$ for some i, where $\deg f_i(x) = r$, a prime. The block B corresponding to $f_i(x)$ generates a subgroup of a Singer group $M_r(q)$ in $\mathrm{GL}_r(q)$ which at least contains the unimodular Singer group in $M_r(q)$. Hence, $(q^r - 1)/(q-1)(r, q-1)||B||(q^r - 1)$. If $e_2 = f_j(x)$, $i \neq j$, a similar condition holds for the corresponding block C, with r replaced by the prime $r' = \deg f_j(x) \neq r$. If $e_2 = g^s(x)$, where $s = 2$ or 3 and $\deg g(x) = 1$, then $p||C|$. Hence in any case there is a t such that $B^t = I$, $C^t \neq I$. Therefore if $\bar{A}$ is a matrix obtained from A by replacing B by a conjugate $B^x \notin \langle B\rangle$, then $\bar{A}$ is a conjugate of A, $\bar{A} \notin D\langle A\rangle$, but $\bar{A}^t = A^t$; thus G is not a T.I. set. Hence, since $n \geqq 3$,

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

(8) δ contains exactly one elementary divisor of degree greater than 1.

Assume that $(x - a)||\delta$, $a \neq 0$. If $q = p$ and $\delta = (x - a)(x - b)^2$, where $a \neq b$, $b \neq 0$, then

$$A = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 1 & b \end{bmatrix}.$$

$A^p = \operatorname{diag}\{a, b, b\}$ is a non-scalar matrix. If B is a conjugate of A by $X = \operatorname{diag}\{1, Y\}$, $Y \in \mathrm{SL}_2(p)$, then $B^p = \operatorname{diag}\{a, b, b\}$; thus G is not a T.I. set. Similarly, suppose that $\delta = (x - a)f(x)$, where $\deg f(x)$ is the prime $n - 1$. In order that A be self-centralizing, a must generate $F_q{}^*$ and the block B of A corresponding to $f(x)$ must generate a Singer group in $\mathrm{GL}_{n-1}(q)$. $B^{(q^{n-1}-1)/(q-1)}$ is scalar, and any conjugate of B raised to the same power will also be the same scalar matrix. Thus G will not be a T.I. set unless $A^{(q^{n-1}-1)/(q-1)}$ is also scalar, and this occurs when $(q - 1)|n$. Hence,

(9) The remaining possibilities for δ are $\delta = f(x)$; $(q - 1)|n$, and $\delta = (x - a)f(x)$, $a \neq 0$; or $q = 2$ and $\delta = (x - 1)^3$, where $\deg f(x)$ is prime.

These possibilities do correspond to self-centralizing T.I. sets in $\mathrm{PSL}_n(q)$. We already know this is the case when $\delta = f(x)$, for the image of $\langle A \rangle$ in $\mathrm{PSL}_n(q)$ is a Singer group. When $n - 1$ is a prime, $(q - 1)|n$, and $\delta = (x - a)f(x)$, $a \neq 0$, we have seen that $A = \operatorname{diag}\{a, B\}$, where B is a Singer cycle in $\mathrm{GL}_{n-1}(q)$. The corresponding G is clearly self-centralizing. In $\mathrm{GL}_n(q^{n-1})$, A is similar to $\operatorname{diag}\{a, \xi, \xi^q, \ldots, \xi^{q^{n-2}}\}$, where ξ is a primitive $(q^{n-1} - 1)$-root of unity. Since no power of this matrix has two diagonal entries equal without the matrix being scalar, G is also a T.I. set. When $q = 2$ and $\delta = (x - 1)^3$, G is conjugate to $\langle A \rangle$, where

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Under the isomorphism between $\mathrm{PSL}_3(2)$ and $\mathrm{PSL}_2(7)$, G is isomorphic to a Singer group; thus G is a self-centralizing T.I. set.

THEOREM 4.2. *The cyclic subgroups G of* $\mathrm{PSL}_n(q)$ *affording Frobenius regular representations of* $\mathrm{PSL}_n(q)$ *are as follows:*

(i) *$G = K_n(q)$, and n is an odd prime or $n = 2$ and $4 \nmid (q + 1)$;*

(ii) *G is conjugate to $K_{n-1}(q)$, $n - 1$ is a prime, and $(q - 1)|n$;*

(iii) *G is the image of the diagonal subgroup in* $\mathrm{SL}_2(q)$, *$n = 2$, and $4 \nmid (q - 1)$;*

(iv) *G is a p-Sylow subgroup, $n = 2$, and $q = p > 3$.*

Proof. We have already seen that the Singer groups of (i) afford Frobenius regular representations of $\mathrm{PSL}_n(q)$. Suppose that $n - 1$ is a prime, $(q - 1)|n$, and G is the image of the group in $\mathrm{SL}_n(q)$ generated by $A = \operatorname{diag}\{a, B\}$,

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

where B is a Singer cycle in $\mathrm{GL}_{n-1}(q)$ and $a^{-1} = \det B$. A matrix in $\mathrm{N}_{\mathrm{SL}}(\langle A\rangle)$ has the form

$$X = \begin{bmatrix} z & x \\ y & C \end{bmatrix},$$

where x is a row vector and y is a column vector. From $AX = XA^t$ it follows that $By = a^t y$ and $ax = xB^t$. But by Theorem 2.4, B and B^t have the same eigenvectors, and their non-zero eigenvectors are all irrational. Thus x and y are zero vectors. But this states that $C \in \mathrm{N}_{\mathrm{GL}_{n-1}}(\langle B\rangle)$ and $a^{-1} = \det C$; thus the normalizer of G in $\mathrm{PSL}_n(q)$ is isomorphic to the normalizer of $K_{n-1}(q)$ in $\mathrm{PSL}_{n-1}(q)$, and this latter group is a Frobenius group with kernel $K_{n-1}(q)$ and a T.I. set as complement.

When $n \geqq 3$, Theorem 4.1 tells us that the only other possibility is $n = 3$, $q = 2$, and G is conjugate to $\langle A\rangle$, where

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Under the isomorphism from $\mathrm{PSL}_3(2)$ onto $\mathrm{PSL}_2(7)$, G corresponds to a Singer group in $\mathrm{PSL}_2(7)$, and $4 | (q + 1) = 7 + 1$ implies that the normalizer of a Singer group is not Frobenius.

The proof that the groups of (iii) and (iv) are the only remaining cyclic subgroups of $\mathrm{PSL}_2(q)$ affording Frobenius regular representations is straightforward and hence is omitted.

5. Singer Groups in other classical groups.

In this section we find the maximal intersection of a Singer group with some of the other classical groups, and then in the unitary case we show that this intersection may afford a Frobenius regular representation of the group.

I would like to thank Professor J. E. McLaughlin for his helpful remarks on the field-theoretic models of the classical groups.

We give a brief description of the groups and the notation. In the orthogonal and the symplectic case, let $V = F_{q^n}$, considered as a vector space of dimension $n \geqq 2$ over F_q, while in the unitary case, let $V = F_{q^{2n}}$, considered as a vector space of dimension $n \geqq 2$ over F_{q^2}. If f is a non-degenerate Hermitian form on V, then a unitary group $\mathrm{U}(V)$ is the group of all linear transformations of V which leave f invariant. If f is a non-degenerate skew-symmetric form on V (necessarily $n = 2m$), then a symplectic group $\mathrm{Sp}(V)$ is the group of all linear transformations of V which keep f invariant. If Q is a non-degenerate quadratic form on V, then an orthogonal group $\mathrm{O}(V)$ is the group of all linear transformations of V which keep Q invariant.

If n is even and $\mathrm{O}(V)$ is an orthogonal group of maximal index, we write $\mathrm{O}(+1, V)$, while if it is of non-maximal index, we write $\mathrm{O}(-1, V)$ when the

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

distinction is important. $\mathrm{Sp}(V)$ is a subgroup of $\mathrm{SL}(V)$; denote $\mathrm{O}(V) \cap \mathrm{SL}(V)$ by $\mathrm{SO}(V)$ and $\mathrm{U}(V) \cap \mathrm{SL}(V)$ by $\mathrm{SU}(V)$. For any of the above groups, the factor group modulo the centre is denoted by prefixing a P to the notation for the group. The matrix version of an orthogonal group $\mathrm{O}(V)$ will be denoted by $\mathrm{O}_n(q)$, etc.

The unitary case is the most interesting.

THEOREM 5.1. *Suppose that n is odd, $M = M_n(q^2)$ is a Singer group in* $\mathrm{GL}_n(q^2)$, *and $U = \mathrm{U}_n(q)$ is a unitary group in* $\mathrm{GL}_n(q^2)$. *Then $|M \cap U|$ divides $q^n + 1$.*

Proof. In $\mathrm{GL}_n(q^{2n})$, a generator for M is similar to

$$A = \mathrm{diag}\{\xi, \xi^{q^2}, \ldots, \xi^{q^{2(n-1)}}\},$$

where ξ is a primitive $(q^{2n} - 1)$-root of unity. If $B = A^s$ and $r = q^{2n} - 1$, then by Corollary 1, B can be rearranged so that B has the $\mu(r, s)$ distinct $n/\mu(r, s) \times n/\mu(r, s)$ scalar matrices $\alpha I, \alpha^{q^2} I, \ldots, \alpha^{q^{2(\mu(r,s)-1)}} I$ down the diagonal, where $\alpha = \xi^s$. Suppose that B satisfies $BJ\bar{B}^t = J$ (t = transpose), where J is the matrix of a non-degenerate Hermitian form and the bar denotes the non-trivial automorphism of $F_{q^{2n}}$ over F_{q^n}. Since n is odd, $J = \bar{J}^t$, and B has the form described, it follows that J has a non-zero block on the diagonal, say it is the $(j + 1)$-block. Then $\alpha^{q^{2j}(q^n+1)} = 1$; thus $\alpha^{q^n+1} = 1$. Thus $|M \cap U|$ divides $q^n + 1$.

On the other hand, an intersection of order $q^n + 1$ does occur.

THEOREM 5.2. *If n is odd and $M(V)$ is a Singer group in* $\mathrm{GL}(V)$, *then there is a unitary group* $\mathrm{U}(V)$ *such that* $|M(V) \cap \mathrm{U}(V)| = q^n + 1$.

Proof. Our field-theoretic model of a Singer group is

$$T = \{T_\alpha \in \mathrm{GL}(V) | \alpha \in F_{q^{2n}}^*\},$$

where T_α: $x \to \alpha x$, $x \in V$. We now describe a field-theoretic model for a unitary group and show that this intersects T in a group of order $q^n + 1$.

For $x \in F_{q^{2n}}^*$, let $\bar{x} = x^{q^n}$, so that $x \to \bar{x}$ is the non-trivial automorphism of $F_{q^{2n}}$ over F_{q^n}. The restriction of this automorphism to F_{q^2} is the non-trivial automorphism of F_{q^2} over F_q. Using this, one can easily check that $f(x, y) = \mathrm{tr}_{F_{q^{2n}}/F_{q^2}} x\bar{y}$ is a Hermitian form. Let U be the group of all transformations in $\mathrm{GL}(V)$ leaving this form invariant. Then

$$T \cap U = \{T_\alpha \in T | f(T_\alpha x, T_\alpha y) = f(x, y) \text{ for all } x, y \in V\}.$$

From the definition of the form and the properties of the trace function, $T_\alpha \in T \cap U$ if and only if $\alpha\bar{\alpha} = 1$. But $\{\alpha \in F_{q^{2n}}^* | \alpha\bar{\alpha} = 1\}$ is just the kernel of the norm function from $F_{q^{2n}}^*$ onto $F_{q^n}^*$, and this has order $q^n + 1$. Thus $|T \cap U| = q^n + 1$.

COROLLARY 5. *If n is odd and K is a Singer group in* $\mathrm{PSL}(V)$, *then there is a unitary group* $\mathrm{PSU}(V)$ *such that* $|K \cap \mathrm{PSU}(V)| = (q^n + 1)/(q + 1)(n, q + 1)$, *and this is the maximum possible order of such an intersection.*

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press

THEOREM 5.3. *Suppose that n is odd and K and* $\mathrm{PSU}(V)$ *are as above. Then* $K \cap \mathrm{PSU}(V)$ *affords a Frobenius regular representation if and only if n is a prime.*

Proof. Let T and U be as in the previous proof, and let σ be an automorphism of order n of $F_{q^{2n}}$ over F_{q^2}. Then since $f(x, y) = \mathrm{tr}\, x\bar{y}$ and the trace function is just the sum of the conjugates, we have $f(x, y) = f(x^\sigma, y^\sigma)$; therefore $\sigma \in U$. Thus $\langle\sigma\rangle \leqq \mathrm{N}_U(U \cap T)$. On the other hand, if there is a $u \in \mathrm{N}_U(U \cap T)$ which does not normalize T, then $T \cap T^u$ contains a subgroup of order $q^n + 1$, in contradiction to Theorem 2.6. Therefore

$$\mathrm{N}_U(U \cap T) = (U \cap T)\langle\sigma\rangle.$$

Let K and PSU be the images in $\mathrm{PSL}(V)$ of $T \cap \mathrm{SL}(V)$ and $U \cap \mathrm{SL}(V)$, respectively. Suppose that n is a prime, $K\langle\sigma\rangle$ is a Frobenius group with kernel K (Theorem 2.10); thus $\mathrm{N}_{\mathrm{PSU}}(K \cap \mathrm{PSU}) = (K \cap \mathrm{PSU})\langle\sigma\rangle$ is a Frobenius group with kernel $K \cap \mathrm{PSU}$. Since K is a T.I. set in $\mathrm{PSL}(V)$ and $\langle\sigma\rangle$ has prime order n, $K \cap \mathrm{PSU}$ and $\langle\sigma\rangle$ are both T.I. sets in PSU. Thus by Lemma 1.5, PSU has a Frobenius regular representation.

Suppose that n is not a prime. A generator for the matrix version of T is similar in $\mathrm{GL}_n(q^{2n})$ to $A = \mathrm{diag}\{\xi, \xi^{q^2}, \ldots, \xi^{q^{2(n-1)}}\}$, where ξ is a primitive $(q^{2n} - 1)$-root of unity. The matrix for σ is the usual cyclic matrix. If $r|n$, then $(q^r + 1)|(q^n + 1)$ since n is odd. By Theorem 2.2, the subgroup of $\langle A\rangle$ of order $q^r + 1$ has every rth diagonal entry equal; thus σ^r centralizes this subgroup. Consequently, $\mathrm{N}_{\mathrm{PSU}}(K \cap \mathrm{PSU})$ could not be Frobenius.

In the odd-dimensional orthogonal case, a proof almost identical to that of Theorem 5.1 yields the following result.

THEOREM 5.4. *Suppose that n is odd, M is a Singer group in* $\mathrm{GL}_n(q)$ *and* $\mathrm{O}_n(q)$ *is an orthogonal group in* $\mathrm{GL}_n(q)$. *Then* $M \cap \mathrm{O}_n(q) = \{\pm I\}$.

COROLLARY 6. *If n is odd, K is a Singer group in* $\mathrm{PSL}_n(q)$, *and* $\mathrm{PSO}_n(q)$ *is an orthogonal group in* $\mathrm{PSL}_n(q)$, *then* $|K \cap \mathrm{PSO}_n(q)| = 1$.

Now let us look at some of the even-dimensional orthogonal and symplectic cases.

THEOREM 5.5. *If M is a Singer group in* $\mathrm{GL}_{2m}(q)$, *then*

$$|M \cap \mathrm{O}_{2m}(\pm 1, q)| \leqq q^m + 1 \quad \textit{and} \quad |M \cap \mathrm{Sp}_{2m}(q)| \leqq q^m + 1.$$

Proof. Once again we work in $\mathrm{GL}_{2m}(q^{2m})$ and assume that M is generated by the usual diagonal matrix A. The matrix $J = (a_{ij})$ of the form is a nonsingular symmetric (orthogonal case) or skew-symmetric (symplectic case) $2m \times 2m$ matrix. The intersections are generated by

$$B = A^r = \mathrm{diag}\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\},$$

where $\alpha = \xi^r$, ξ is a primitive $(q^{2m} - 1)$-root of unity, and B satisfies $BJB = J$. From this it follows that the order of B is related to J by

$$|B| = (q^{2m} - 1, \gcd\{q^{j-i} + 1 | 1 \leqq i \leqq j \leqq 2m \text{ and } a_{ij} \neq 0\}).$$

This is maximal when $1 \leqq i \leqq j \leqq 2m$ and $a_{ij} \neq 0$ imply $j - i = m$. Then B has order $q^m + 1$.

Intersections of this order exist with a symplectic group and with an orthogonal group of non-maximal index.

THEOREM 5.6. *Suppose that $n = 2m$ and M is a Singer group in* $\mathrm{GL}(V)$. *Then there exists a symplectic group* $\mathrm{Sp}(V)$ *and an orthogonal group of non-maximal index* $\mathrm{O}(-1, V)$ *such that* $|M \cap \mathrm{Sp}(V)| = |M \cap \mathrm{O}(-1, V)| = q^m + 1$.

Proof. We describe field-theoretic models for $\mathrm{Sp}(V)$ and $\mathrm{O}(-1, V)$ which intersect T in a subgroup of order $q^m + 1$. In the symplectic case, define a non-degenerate bilinear form $f: F_{q^{2m}} \to F_q$ by $f(x, y) = \mathrm{tr}_{F_{q^{2m}}/F_q} ax\bar{y}$, where $a \in F_{q^{2m}}{}^*$ is such that $a + \bar{a} = 0$. Set

$$\mathrm{Sp}(V) = \{S \in \mathrm{GL}(V) | f(Sx, Sy) = f(x, y) \text{ for all } x, y \in V\}.$$

In the orthogonal case, define a quadratic form $Q: F_{q^{2m}} \to F_q$ by $Q(x) = \mathrm{tr}_{F_{q^m}/F_q} x\bar{x}$. The norm function $x \to x\bar{x}$ has a kernel of order $q^m + 1$, and the kernel of the trace function from F_{q^m} onto F_q has order $q^{m-1} - 1$. Thus $|\ker Q(x)| = (q^m + 1)(q^{m-1} - 1)$, and Q has index $m - 1$. Set

$$\mathrm{O}(-1, V) = \{S \in \mathrm{GL}(V) | Q(Sx) = Q(x) \text{ for all } x \in V\}.$$

An easy consequence of these definitions is that $\alpha\bar{\alpha} = 1$ is a necessary and sufficient condition for $T_\alpha \in T$ to be either $\mathrm{Sp}(V)$ or $\mathrm{O}(-1, V)$, and the theorem follows.

REFERENCES

1. E. Artin, *The orders of the linear groups*, Comm. Pure Appl. Math. *8* (1955), 355–366.
2. D. G. Higman and J. E. McLaughlin, *Geometric* ABA-*groups*, Illinois J. Math. *5* (1961), 382–397.
3. B. Huppert, *Endliche Gruppen*, Vol. I (Springer-Verlag, New York, 1967).
4. H. Karzel, *Bericht über projektive Inzidenzgruppen*, Jber. Deutsch. Math.-Verein. *67* (1964/65), Abt. 1, 58–92.
5. G. Keller, *A characterization of A_6 and M_{11}*, J. Algebra *13* (1969), 409–421.
6. W. R. Scott, *Group theory* (Prentice-Hall, Englewood Cliffs, N. J., 1964).
7. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. *43* (1938), 377–385.

Michigan State University,
East Lansing, Michigan

https://doi.org/10.4153/CJM-1970-057-2 Published online by Cambridge University Press