Can. J. Math., Vol. XXIII, No. 1, 1971, pp. 90–102

ON THE SMALLEST DEGREES OF PROJECTIVE REPRESENTATIONS OF THE GROUPS PSL(n, q)

MORTON E. HARRIS AND CHRISTOPH HERING

Introduction. In this paper, we obtain information about the minimal degree δ of any non-trivial projective representation of the group PSL(n, q) with $n \geqq 2$ over an arbitrary given field K. Our main results for the groups PSL(n, q) (Theorems 4.2, 4.3, and 4.4) state that, apart from certain exceptional cases with small n, we have the following rather surprising situation: if $q = p^f$ (where p is a prime integer) and char $K = p$, then $\delta = n$, but if $q = p^f$ and char $K \neq p$, then δ is of a considerably higher order of magnitude, namely, δ is at least $q^{n-1} - 1$ or $\frac{1}{2}(q - 1)$ if $n = 2$ and q is odd. Note that for $n = 2$, this lower bound for δ is the best possible. However, for $n \geqq 3$, this lower bound can conceivably be improved. But, since the classical (doubly transitive) permutation representation of PSL(n, q) on the projective points of the underlying vector space provides us with an ordinary representation of degree $q^{n-1} + q^{n-2} + \ldots + q$ over any field, δ must in any case be essentially of the same magnitude as our lower bound.

As an application, we present a new method for the determination of the so-called exceptional isomorphisms between the groups PSL(n, q) (cf. Theorem 4.5).

The main motivation for this work lies in certain applications to problems about doubly transitive permutation groups (cf. [**5**]).

The lower bounds for the degrees of projective representations that we obtain actually apply to a much wider class of groups than the groups PSL(n, q) (see Theorems 3.1 and 3.2). Moreover, the methods of proof require certain results which appear in §§ 1 and 2 and are of independent interest. For example, in § 1, a very useful result of Brauer (Lemma 1.1) is extended to splitting fields of prime characteristic (Lemma 1.2) and then used to obtain Lemmas 1.3 and 1.4 which are used in § 3 and to generalize certain results on Frobenius groups. Also, § 2 contains homological results on group algebras which are used to prove Lemma 2.6 needed in the proof of Theorem 3.2 and are also of independent interest.

Our notation is fairly standard and tends to follow that of [**6**].

1. Lemmas in group representation theory. In this section, the analogue for fields of prime characteristic of a very useful result of Brauer is derived by means of modular character theory. This analogue is then applied to obtain

Received March 10, 1970. This research was supported in part by NSF grants GP-6539 and GP-9584.

https://doi.org/10.4153/CJM-1971-010-1 Published online by Cambridge University Press

results (Lemmas 1.3 and 1.4) needed in § 3, and to extend to fields of arbitrary characteristic, some basic results on representations of Frobenius groups over fields of characteristic not dividing the order of the Frobenius group.

Let $\mathscr{G}$ denote a finite group and let L denote a splitting field of characteristic zero of $\mathscr{G}$. Let $\mathbf{K} = \{K_1 = \{E\}, K_2, \ldots, K_k\}$ denote the set of conjugacy classes of $\mathscr{G}$, let $X = \{\mathfrak{X}_1 = 1, \mathfrak{X}_2, \ldots, \mathfrak{X}_k\}$ denote a full set of representatives for the equivalence classes of L-(absolutely) irreducible representations of $\mathscr{G}$ and let $\operatorname{ch} X = \{\chi_1 = 1, \chi_2, \ldots, \chi_k\}$ denote the corresponding characters of X (i.e., $\chi_i = \operatorname{tr} \mathfrak{X}_i$).

A very useful result of Brauer (cf. [**6**, *Kapitel* V, *Satz* 13.5]) is the following.

LEMMA 1.1 (Brauer). *Assume that the finite group $\mathscr{A}$ has permutation representations on:* (1) *the set* $\operatorname{ch} X$, *denoted by* $\chi \to \chi^A$ *for all* $A \in \mathscr{A}$ *and* $\chi \in \operatorname{ch} X$, *and* (2) *the set* $\mathbf{K}$, *denoted by* $K \to K^A$ *for all* $A \in \mathscr{A}$ *and* $K \in \mathbf{K}$, *such that if* $\operatorname{ch} X$ *is viewed as a set of L-valued functions on* $\mathbf{K}$, *then* $\chi^A(K) = \chi(K^A)$ *for all* $\chi \in \operatorname{ch} X$, $K \in \mathbf{K}$ *and* $A \in \mathscr{A}$. *If the (complex) permutation characters of the permutation representations of* $\mathscr{A}$ *in* (1) *and* (2) *are denoted by* π_1 *and* π_2, *respectively, then* $\pi_1 = \pi_2$.

A similar result holds for splitting fields of $\mathscr{G}$ of prime characteristic. Thus let $\mathscr{G}$ denote a finite group, let F denote a splitting field of $\mathscr{G}$ of characteristic p and let $|\mathscr{G}| = p^a g'$, where $a \geqq 0$ and $p \nmid g'$. Let $\mathbf{K}^* = \{K_1 = \{E\}, K_2, \ldots, K_u\}$ denote the set of p-regular conjugacy classes of $\mathscr{G}$. A well-known theorem of Brauer (cf. [**1**, *Satz* (3B)]) states that a full set of representatives for the equivalence classes of F-(absolutely) irreducible representations of $\mathscr{G}$ consists of u representations; let $\mathfrak{F} = \{\mathfrak{F}_1 = 1, \mathfrak{F}_2, \ldots, \mathfrak{F}_u\}$ denote such a set and let $\operatorname{ch} \mathfrak{F} = \{\varphi_1^* = 1, \varphi_2^*, \ldots, \varphi_u^*\}$ denote the corresponding characters of $\mathfrak{F}$ (i.e., $\varphi_i^* = \operatorname{tr} \mathfrak{F}_i$). The "modular analogue" of Lemma 1.1 is the following.

LEMMA 1.2. *Assume that the finite group $\mathscr{A}$ has permutation representations on:* (1) *the set* $\operatorname{ch} \mathfrak{F}$ *denoted by* $\varphi^* \to \varphi^{*A}$ *for all* $A \in \mathscr{A}$ *and* $\varphi^* \in \operatorname{ch} \mathfrak{F}$, *and* (2) *the set* $\mathbf{K}^*$ *denoted by* $K \to K^A$ *for all* $A \in \mathscr{A}$ *and* $K \in \mathbf{K}^*$ *such that if* $\operatorname{ch} \mathfrak{F}$ *is viewed as a set of F-valued functions on* $\mathbf{K}^*$, *then* $\varphi^{*A}(K) = \varphi^*(K^A)$ *for all* $\varphi^* \in \operatorname{ch} \mathfrak{F}$, $K \in \mathbf{K}^*$ *and all* $A \in \mathscr{A}$. *If the (complex) permutation characters of the permutation representations of* $\mathscr{A}$ *in* (1) *and* (2) *are denoted by* π_1 *and* π_2, *respectively, then* $\pi_1 = \pi_2$.

Proof. Let Ω denote an algebraic number field containing a primitive g'th root of unity, let $\mathfrak{o}$ denote the ring of algebraic integers of Ω and let $\mathfrak{p}$ denote a fixed prime ideal of $\mathfrak{o}$ such that $p \in \mathfrak{p}$. Set $\Omega^* = \mathfrak{o}/\mathfrak{p}$ (a field) and let ν be any exponential valuation of Ω associated with $\mathfrak{p}$. Finally, let $\mathfrak{o}_\nu$ denote the ring of $\mathfrak{p}$-local integers of Ω and let $\mathfrak{p}_\nu$ denote the unique prime ideal of $\mathfrak{o}_\nu$. We may identify $\mathfrak{o}_\nu/\mathfrak{p}_\nu$ with Ω^*. Since Ω^* is a splitting field for $\mathscr{G}$ of characteristic p, we may assume that $F = \Omega^*$. Let θ: $\mathfrak{o} \to \Omega^*$ denote the residue class mapping; then there exists a set $\Phi = \{\varphi_1 = 1, \varphi_2, \ldots, \varphi_u\}$ of $\mathfrak{o}$-valued functions (the Brauer characters) defined on the p-regular elements of $\mathscr{G}$ which are constant on the

https://doi.org/10.4153/CJM-1971-010-1 Published online by Cambridge University Press

p-regular classes of $\mathcal{G}$ such that $\theta(\varphi_i(G)) = \varphi_i^*(G)$ for all p-regular elements $G \in \mathcal{G}$ and all $1 \leqq i \leqq u$ (cf. [**1**, § 3]). Moreover, $\varphi_i = \varphi_j$ if and only if $i = j$ and hence $\mathcal{A}$ has an obvious permutation representation on Φ which is equivalent to (1) above. If Φ is viewed as a set of functions on $\mathbf{K}^*$, then (obviously) $\varphi^A(K) = \varphi(K^A)$ for all $\varphi \in \Phi$, $K \in \mathbf{K}^*$, $A \in \mathcal{A}$, and the $u \times u$ $\mathfrak{o}$-valued matrix $(\varphi_i(K_j))$ is non-singular (cf. [**1**, *Satz* (3E)]). Now the same argument used to prove Lemma 1.1 applies to the permutation representations of $\mathcal{A}$ on $\mathbf{K}^*$ and Φ, and the lemma follows.

Note that this lemma is valid even if $a = 0$ (i.e., if $p \nmid |\mathcal{G}|$) and hence Lemma 1.1 is generalized to splitting fields of $\mathcal{G}$ of arbitrary characteristic.

These lemmas clearly apply to the case in which $\mathcal{A}$ is a subgroup of $\mathrm{Aut}(\mathcal{G})$, and then $\mathcal{A}$ induces the obvious permutation representations on $\mathbf{K}$ and $\mathbf{K}^*$ and induces the permutation representations on $\mathrm{ch}\, X$ and on $\mathrm{ch}\, \mathfrak{F}$ defined by $\chi \to \chi^A$, where $\chi^A(K) = \chi(K^A)$, and $\varphi^* \to \varphi^{*A}$, where $\varphi^{*A}(K^*) = \varphi^*((K^*)^A)$ for all $A \in \mathcal{A}$, $\chi \in \mathrm{ch}\, X$, $\varphi^* \in \mathrm{ch}\, \mathfrak{F}$, $K \in \mathbf{K}$, and $K^* \in \mathbf{K}^*$. In this situation, the hypotheses of both lemmas are trivially satisfied.

For our later work we need the following two lemmas.

LEMMA 1.3. *Let $\mathcal{G}$ be a finite group with a proper normal nilpotent subgroup $\mathfrak{N}$. Let p be a prime integer such that $O_p(\mathfrak{N}) \neq (1)$. Suppose that $\mathcal{G}/O_{p'}(\mathfrak{N})$ is a Frobenius group with Frobenius kernel $\mathfrak{N}/O_{p'}(\mathfrak{N})$ ($\cong O_p(\mathfrak{N})$) and suppose that $\mathfrak{F}$ is a representation of $\mathcal{G}$ in a field F with characteristic not p. If* $\mathrm{Ker}(\mathfrak{F}) \not\supseteq O_p(\mathfrak{N})$, *then* $\deg \mathfrak{F} \geqq |\mathcal{G} : \mathfrak{N}|$.

Proof. By extending the field if necessary, we may assume that F is algebraically closed. Since $\mathfrak{F}|_{O_p(\mathfrak{N})}$ is completely reducible, we may also assume that $\mathfrak{F}$ is irreducible. Since $\mathrm{Ker}(\mathfrak{F}) \not\supseteq O_p(\mathfrak{N})$, Clifford's theorem implies that there exists a positive integer e and a non-trivial irreducible F-representation Ψ of $O_p(\mathfrak{N})$ such that $\mathfrak{F}|_{O_p(\mathfrak{N})}$ is equivalent to $e(\oplus_{H \in \mathcal{H}} \Psi^H)$, where $\mathcal{H}$ is a full set of representatives for the left cosets of the subgroup $\mathfrak{I}(\Psi) = \{G \in \mathcal{G} \mid \Psi^G$ and Ψ are equivalent F-representations of $O_p(\mathfrak{N})\}$ in $\mathcal{G}$. Thus $\deg \mathfrak{F} \geqq |\mathcal{G} : \mathfrak{I}(\Psi)|$. Let $\mathfrak{L}$ be a subgroup of $\mathcal{G}$ such that $\mathfrak{L} \supset O_{p'}(\mathfrak{N})$ and $\mathfrak{L}/O_{p'}(\mathfrak{N})$ is a complement to $\mathfrak{N}/O_{p'}(\mathfrak{N})$ in $\mathcal{G}/O_{p'}(\mathfrak{N})$. Clearly $C_{\mathfrak{L}}(O_p(\mathfrak{N})) = O_{p'}(\mathfrak{N})$ and $\mathfrak{L}/O_{p'}(\mathfrak{N})$ acting by conjugation induces a fixed-point free group of automorphisms on $O_p(\mathfrak{N})$. By [**6**, *Kapitel* V, *Satz* 8.9], $\mathfrak{L}/O_{p'}(\mathfrak{N})$ has a faithful semi-regular permutation representation on the set of non-identity conjugacy classes of $O_p(\mathfrak{N})$. Now Lemmas 1.1 and 1.2 imply that $\mathfrak{L}/O_{p'}(\mathfrak{N})$ has a faithful semi-regular permutation representation on the set of non-trivial irreducible F-representations of $O_p(\mathfrak{N})$. Thus $\mathfrak{L}/O_{p'}(\mathfrak{N})$ has orbits of length $|\mathfrak{L}/O_{p'}(\mathfrak{N})| = |\mathcal{G} : \mathfrak{N}|$ on this set. Consequently, $|\mathcal{G} : \mathfrak{I}(\Psi)| \geqq |\mathcal{G} : \mathfrak{N}|$ and the result follows.

LEMMA 1.4. *Let $\mathcal{G}$ be a finite group with a proper normal abelian p-subgroup $\mathfrak{N}$ such that $\mathcal{G}$ acting by conjugation on $\mathfrak{N}$ is transitive on $\mathfrak{N}^\#$. Suppose that $\mathfrak{F}$ is a representation of $\mathcal{G}$ in a field F of characteristic not p. If* $\mathrm{Ker}(\mathfrak{F}) \not\supseteq \mathfrak{N}$, *then* $\deg \mathfrak{F} \geqq |\mathfrak{N}| - 1$.

Proof. Again it suffices to assume that F is algebraically closed. Since $\mathscr{G}$ acting by conjugation is transitive on $\mathfrak{N}^{\#}$, Lemmas 1.1 and 1.2 and [**6**, *Kapitel* V, *Satz* 20.2] imply that $\mathscr{G}$ has two orbits on the F-irreducible characters of $\mathfrak{N}$ namely the 1 character and the other $|\mathfrak{N}| - 1$ characters. Thus if Ψ is any non-trivial F-irreducible character of $\mathfrak{N}$, then $|\mathscr{G}: \mathfrak{J}(\Psi)| = |\mathfrak{N}| - 1$. An appropriate modification of the proof of Lemma 1.3 yields the desired result.

Lemma 1.2 has various other applications. For example, [**6**, *Kapitel* V, *Satz* 16.13] which characterizes the irreducible representations of a Frobenius group $\mathscr{G}$ over an algebraically closed field F such that char $F \nmid |\mathscr{G}|$ can be generalized to hold for arbitrary algebraically closed fields. To prove this generalization, we require the following result.

LEMMA 1.5. *Let $\mathscr{G} = \mathfrak{N}\mathfrak{H}$ be a Frobenius group with Frobenius kernel $\mathfrak{N}$ and complement $\mathfrak{H}$. If F is a splitting field for $\mathfrak{N}$ and if $\mathfrak{F}$ is a non-trivial irreducible F-representation of $\mathfrak{N}$, then the induced representation $\mathfrak{F}^{\mathscr{G}}$ is an absolutely irreducible F-representation of $\mathscr{G}$ with kernel not containing $\mathfrak{N}$ and such that $\mathfrak{F}^{\mathscr{G}}|_{\mathfrak{N}} = \bigoplus_{H\in\mathfrak{H}} \mathfrak{F}^H$.*

Proof. First assume that F has prime characteristic p. As in Lemma 1.3, $\mathfrak{H}$, acting by conjugation, has a faithful semi-regular permutation representation on the p-regular classes of $\mathfrak{N}$. Now Lemma 1.2 applies, and we conclude that $\mathfrak{H}$ acts semi-regularly on the non-trivial irreducible F-representations of $\mathfrak{N}$. Let $F*$ be the algebraic closure of F and let $\mathfrak{X}$ be an (absolutely) irreducible constituent of $(\mathfrak{F}^{\mathscr{G}})_{F*}$ such that $\mathfrak{F}$ is equivalent to a constituent of $\mathfrak{X}|_{\mathfrak{N}}$. Now Clifford's theorem implies that $\mathfrak{X}|_{\mathfrak{N}}$ is equivalent to $e(\bigoplus_{H\in\mathfrak{H}} \mathfrak{F}^H)$, where e is a positive integer.

Hence deg $\mathfrak{F}^{\mathscr{G}} = |\mathfrak{H}|$ deg $\mathfrak{F} \geqq$ deg $\mathfrak{X} \geqq e|\mathfrak{H}|$ deg $\mathfrak{F}$. Thus $e = 1$, $(\mathfrak{F}^{\mathscr{G}})_{F*} = \mathfrak{X}$ and $\mathfrak{F}^{\mathscr{G}}$ is absolutely irreducible. If F has characteristic zero, the analogous argument using Lemma 1.1 applies, and the lemma follows.

The generalization of [**6**, *Kapitel* V, *Satz* 16.13] to fields of arbitrary characteristic mentioned above is the following.

THEOREM 1.6. *Let $\mathscr{G} = \mathfrak{N}\mathfrak{H}$ be a Frobenius group with Frobenius kernel $\mathfrak{N}$ and complement $\mathfrak{H}$. Let F be a field which is a splitting field for both $\mathfrak{H}$ and $\mathfrak{N}$. If* char F *is a prime p, let $h_0(\mathfrak{N})$ and $h_0(\mathfrak{H})$ denote the number of p-regular conjugate classes of $\mathfrak{N}$ and $\mathfrak{H}$ respectively. If* char $F = 0$, *let $h_0(\mathfrak{N})$ and $h_0(\mathfrak{H})$ denote the number of conjugate classes of $\mathfrak{N}$ and $\mathfrak{H}$, respectively. Then:*

(1) *F is a splitting field for $\mathscr{G}$,*

(2) *if $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are non-trivial irreducible F-representations of $\mathfrak{N}$, then $\mathfrak{F}_1^{\mathscr{G}}$ and $\mathfrak{F}_2^{\mathscr{G}}$ are absolutely irreducible F-representations of $\mathscr{G}$; also, $\mathfrak{F}_1^{\mathscr{G}}$ and $\mathfrak{F}_2^{\mathscr{G}}$ are equivalent F-representations of $\mathscr{G}$ if and only if there exists an $H \in \mathfrak{H}$ such that $\mathfrak{F}_1^H$ and $\mathfrak{F}_2$ are equivalent F-representations of $\mathfrak{N}$,*

(3) *the following list of F-representations of $\mathscr{G}$ comprises a full set of representatives for the set of equivalence classes of (absolutely) irreducible F-representations of $\mathscr{G}$:*

(a) $h_0(\mathfrak{H})$ *inequivalent F-representations of* $\mathscr{G}$ *with kernel containing* $\mathfrak{N}$ *obtained from* $\mathfrak{H}$,

(b) $(h_0(\mathfrak{N}) - 1)/|\mathfrak{H}|$ *inequivalent F-representations of* $\mathscr{G}$ *induced from non-trivial irreducible F-representations of* $\mathfrak{H}$.

(4) *if V is an irreducible* $F[\mathscr{G}]$*-module on which* $\mathfrak{N}$ *acts non-trivially, then* $V_{\mathfrak{H}}$ *is a direct sum of regular* $F[\mathfrak{H}]$*-modules (where* $F[\mathscr{G}]$ *and* $F[\mathfrak{H}]$ *denote the group rings of* $\mathscr{G}$ *and* $\mathfrak{H}$, *respectively, over F).*

Proof. We first prove (2). If there exists an $H \in \mathfrak{H}$ such that $\mathfrak{F}_1{}^H$ and $\mathfrak{F}_2$ are equivalent, then clearly $(\mathfrak{F}_1{}^H)^{\mathscr{G}}$, $\mathfrak{F}_1{}^{\mathscr{G}}$, and $\mathfrak{F}_2{}^{\mathscr{G}}$ are all equivalent representations of $\mathscr{G}$. Conversely, assume that $\mathfrak{F}_1{}^{\mathscr{G}}$ and $\mathfrak{F}_2{}^{\mathscr{G}}$ are equivalent representations of $\mathscr{G}$. But, by Lemma 1.5,

$$\mathfrak{F}_1{}^{\mathscr{G}}|_{\mathfrak{N}} = \bigoplus_{H \in \mathfrak{H}} \mathfrak{F}_1{}^H \qquad \text{and} \qquad \mathfrak{F}_2{}^{\mathscr{G}}|_{\mathfrak{N}} = \bigoplus_{H \in \mathfrak{H}} \mathfrak{F}_2{}^H,$$

and (2) follows. Since the number of p-regular classes of $\mathscr{G}$ is

$$h_0(\mathfrak{H}) + (h_0(\mathfrak{N}) - 1)/|\mathfrak{H}|,$$

(3) follows. Then (1) is immediate and (4) follows as in the proof of [**6**, *Kapitel* V, *Satz* 16.13].

Finally, we state a generalization of [**3**, Theorem 3.4.3] which follows from our lemmas and Clifford's theorem.

COROLLARY 1.7. *Let* $\mathscr{G} = \mathfrak{N}\mathfrak{H}$ *be a Frobenius group with Frobenius kernel* $\mathfrak{N}$ *and complement* $\mathfrak{H}$. *Let F be a splitting field for* $\mathfrak{N}$ *and let* $\mathfrak{F}$ *be an irreducible representation of* $\mathscr{G}$ *with* $\operatorname{Ker}(\mathfrak{F}) \not\supseteq \mathfrak{N}$. *Then* $\mathfrak{F}|_{\mathfrak{N}}$ *has exactly* $|\mathfrak{H}|$ *distinct Wedderburn components.*

2. Lemmas in homological algebra of groups. In this section, we derive a result (Lemma 2.6) which is needed in the proof of one of our main theorems (Theorem 3.2) as a consequence of various group homological results which are of independent interest.

LEMMA 2.1. *Let K denote an arbitrary field, let* $\mathscr{G}$ *denote an arbitrary finite group, and let* $\mathfrak{C}$ *denote the category of right* $K[\mathscr{G}]$*-modules (where* $K[\mathscr{G}]$ *denotes the group ring of* $\mathscr{G}$ *over K). Then, for any objects V, W in* $\mathfrak{C}$ *and any integer* $n \geqq 1$, *we have:*

$$\operatorname{Ext}_{K[\mathscr{G}]}{}^n(V, W) \cong H^n(\mathscr{G}, \operatorname{Hom}_K(V, W))$$

as abelian groups, where $\operatorname{Hom}_K(V, W)$ *is viewed as a right* $\mathscr{G}$*-module with action defined by: if* $G \in \mathscr{G}$, $v \in V$, $f \in \operatorname{Hom}_K(V, W)$, *then* $v(fG) = ((vG^{-1})f)G$.

Proof. By [**2**, XVI, § 7(6)], $\operatorname{Ext}_{K[\mathscr{G}]}{}^n(K, \operatorname{Hom}_K(V, W)) \cong \operatorname{Ext}_{K[\mathscr{G}]}{}^n(V, W)$ for all integers $n \geqq 0$, where K is viewed as a trivial $\mathscr{G}$-module. Let $\mathfrak{D}$ denote the category of right $Z[\mathscr{G}]$-modules and let $T\colon \mathfrak{C} \to \mathfrak{D}$ denote the obvious "forgetful" functor. Clearly $\{\mathrm{Ext}_{Z[\mathscr{G}]}{}^n(Z, *) \circ T \mid n \geqq 0\}$ is a connected sequence of functors in $\mathfrak{C}$ and for each object X in $\mathfrak{C}$,

$$\mathrm{Ext}_{Z[\mathscr{G}]}{}^0(Z, T(X)) \cong X^{\mathscr{G}} \cong \mathrm{Hom}_{K[\mathscr{G}]}(K, X) \cong \mathrm{Ext}_{K[\mathscr{G}]}{}^0(K, X).$$

Moreover, by [**8**, Corollary 2.2], every $K[\mathscr{G}]$-injective module P is weakly $K[\mathscr{G}]$-projective and hence $T(P)$ is weakly $Z[\mathscr{G}]$-projective. Thus

$$\mathrm{Ext}_{Z[\mathscr{G}]}{}^n(Z, T(P)) = 0$$

for all $n > 0$ and all $K[\mathscr{G}]$-injective modules and

$$\{\mathrm{Ext}_{Z[\mathscr{G}]}{}^n(Z, *) \circ T \mid n \geqq 0\}$$

satisfies the well-known axiomatic description of $\{\mathrm{Ext}_{K[\mathscr{G}]}{}^n(K, *) \mid n \geqq 0\}$ (cf. [**7**, Chapter III, Theorem 10.2]). Finally, for all integers $n \geqq 1$,

$$\begin{aligned}\mathrm{Ext}_{K[\mathscr{G}]}{}^n(V, W) &\cong \mathrm{Ext}_{K[\mathscr{G}]}{}^n(K, \mathrm{Hom}_K(V, W)) \\ &\cong \mathrm{Ext}_{Z[\mathscr{G}]}{}^n(Z, T(\mathrm{Hom}_K(V, W))) \\ &\cong H^n(\mathscr{G}, \mathrm{Hom}_K(V, W)).\end{aligned}$$

LEMMA 2.2. *Let V be a vector space over a field K and let $\mathscr{G}$ be a group of K-linear transformations of V (acting on the right). Let F be a subfield of K such that $|K: F|$ is finite. Then the left $K[\mathscr{G}]$-modules* $\mathrm{Hom}_F(V, F)$ *and* $\mathrm{Hom}_K(V, K)$ *are $K[\mathscr{G}]$-isomorphic.*

Proof. By means of standard isomorphisms of left $K[\mathscr{G}]$-modules we have:

$$\mathrm{Hom}_F(V, F) \cong \mathrm{Hom}_F(K \otimes_K V, F) \cong \mathrm{Hom}_K(V, \mathrm{Hom}_F(K, F)).$$

Let β: $\mathrm{Hom}_F(V, F) \rightarrow \mathrm{Hom}_K(V, \mathrm{Hom}_F(K, F))$ denote this isomorphism. Now $\mathrm{Hom}_F(K, F)$ is a vector space over K and

$$\dim_K(\mathrm{Hom}_F(K, F)) = \frac{1}{|K: F|} \dim_F(\mathrm{Hom}_F(K, F)) = \frac{|K: F|}{|K: F|} = 1.$$

Let t: $\mathrm{Hom}_F(K, F) \rightarrow K$ be a K-isomorphism; thus t induces an isomorphism t^*: $\mathrm{Hom}_K(V, \mathrm{Hom}_F(K, F)) \rightarrow \mathrm{Hom}_K(V, K)$ of left $K[\mathscr{G}]$-modules. Finally $\alpha = \beta \circ t^*$ is the required isomorphism.

COROLLARY 2.3. *Let K denote an arbitrary field, let F be a subfield of K such that $|K: F|$ is finite and let $\mathscr{G}$ denote an arbitrary finite group. If V is an arbitrary right $K[\mathscr{G}]$-module and if both F and K are viewed as trivial right $\mathscr{G}$-modules, then* $\mathrm{Ext}_{K[\mathscr{G}]}{}^n(V, K) \cong \mathrm{Ext}_{F[\mathscr{G}]}{}^n(V, F)$ *as abelian groups for any integer $n \geqq 1$.*

Proof. By Lemma 2.1, $\mathrm{Ext}_{K[\mathscr{G}]}{}^n(V, K) \cong H^n(\mathscr{G}, \mathrm{Hom}_K(V, K))$ and $\mathrm{Ext}_{F[\mathscr{G}]}{}^n(V, F) \cong H^n(\mathscr{G}, \mathrm{Hom}_F(V, F))$ for all integers $n \geqq 1$ where the actions of $\mathscr{G}$ on the right on $\mathrm{Hom}_K(V, K)$ and $\mathrm{Hom}_F(V, F)$ are as defined in Lemma 2.1. However, by Lemma 2.2, $\mathrm{Hom}_K(V, K)$ and $\mathrm{Hom}_F(V, F)$ are isomorphic under this action; hence $H^n(\mathscr{G}, \mathrm{Hom}_K(V, K)) \cong H^n(\mathscr{G}, \mathrm{Hom}_F(V, F))$ for all integers $n \geqq 1$, and the result follows.

Using the same method of proof as in [**4**, Lemma 4], we can prove the following result.

LEMMA 2.4. *Let V be a vector space of dimension $n \geqq 3$ over a field K. Let U be a subspace of V of dimension* 1 *over K. Let $\mathscr{G} = \mathrm{SL}(V/U, K)$ and suppose that σ: $\mathscr{G} \rightarrow \mathrm{GL}(V, K)$ is a monomorphism such that if $G \in \mathscr{G}$, then G^σ is trivial on U and G^σ induces G on V/U. Then, excluding the cases* (a) $n = 3$, $\mathrm{char}\, K = 2$ *and* (b) $n = 4$ *and* $|K| = 2$, *there exists a subspace W of V which is $\mathscr{G}^\sigma$-invariant such that $V = U \oplus W$.*

COROLLARY 2.5. *If X is a vector space of dimension $n \geqq 2$ over a field K, then, excluding the cases* (a) $n = 2$, $\mathrm{char}\, K = 2$ *and* (b) $n = 3$, $|K| = 2$, *we have* $\mathrm{Ext}^1_{K[\mathrm{SL}(X,K)]}(X, K) = 0$, *where the action of* $\mathrm{SL}(X, K)$ *on X is the natural action and on K is the trivial action.*

We conclude this section with a result needed in the proof of Theorem 3.2.

LEMMA 2.6. *Let K and X be as in Corollary* 2.5 *and assume also that K is a finite field. Let F be a subfield of K and let $\mathscr{G}$ be a group such that* $\mathrm{GL}(X, K) \supseteq \mathscr{G} \supseteq \mathrm{SL}(X, K)$. *Then, excluding the cases* (a) *and* (b) *above, we have* $\mathrm{Ext}_{F[\mathscr{G}]}{}^1(X, F) = 0$, *where the action of $\mathscr{G}$ on X is the natural action and on F is the trivial action.*

Proof. Since $|\mathscr{G}: \mathrm{SL}(X, K)|$ is relatively prime to char K and $H^1(\mathrm{SL}(X, K), \mathrm{Hom}_K(X, K)) = (0)$ by Lemma 2.1 and Corollary 2.5, we have

$$H^1(\mathscr{G}, \mathrm{Hom}_K(X, K)) = (0).$$

Then $\mathrm{Ext}_{K[\mathscr{G}]}{}^1(X, K) = (0)$ follows from Lemma 2.1 and $\mathrm{Ext}_{F[\mathscr{G}]}{}^1(X, F) = (0)$ follows from Corollary 2.3.

3. Lower bounds for the degrees of projective representations of two types of groups.

This section contains our basic results which give lower bounds on the degrees of non-trivial projective representations for groups containing subgroups of two specific types. These results are applied in § 4 to the groups $\mathrm{PSL}(n, q)$.

Let $\mathscr{G}$ be a finite group and let V be a finite-dimensional vector space over a field K. Let ρ: $\mathscr{G} \rightarrow \mathrm{GL}(V, K)$ be a projective representation of $\mathscr{G}$ and let ρ^*: $\mathscr{G} \rightarrow \mathrm{PGL}(V, K)$ denote the ρ-induced group homomorphism.

Definition. The projective representation ρ: $\mathscr{G} \rightarrow \mathrm{GL}(V, K)$ is said to be faithful if ρ^*: $\mathscr{G} \rightarrow \mathrm{PGL}(V, K)$ is a monomorphism.

THEOREM 3.1. *Let $\mathscr{G}$ be a finite group which contains a subgroup $\mathscr{H}$ which is a Frobenius group with elementary abelian kernel of order q^n with $n \geqq 1$ and $q = p^f$, p a prime, $f \geqq 1$, and with cyclic complement of order $(1/d)(q^n - 1)$ where $d = \gcd\{n + 1, q - 1\}$. If ρ: $\mathscr{G} \rightarrow \mathrm{GL}(V, K)$ is a projective representation of $\mathscr{G}$ such that ρ restricted to $\mathscr{H}$ is faithful, if $p \neq$* char K, *and if* $(n, q) \neq (1, 4)$, $(1, 9)$, $(2, 2)$, *and* $(2, 4)$, *then* $\deg \rho$ $(= \dim_K V) \geqq (1/d)(q^n - 1)$.

https://doi.org/10.4153/CJM-1971-010-1 Published online by Cambridge University Press

Proof. Clearly we may assume that $\mathscr{G} = \mathscr{H}$, that K is algebraically closed, and that ρ^*: $\mathscr{G} \to \mathrm{PGL}(V, K)$ is a monomorphism. Note that $(1/d)(q^n - 1) = 1$ if and only if $(n, q) = (1, 2)$ or $(n, q) = (1, 3)$; thus we may exclude $(n, q) = (1, 2)$ and $(n, q) = (1, 3)$. Since $\mathscr{G}$ has a finite representation group over K, there exists a finite subgroup $\mathfrak{F}$ of $\mathrm{GL}(V, K)$ of minimal order such that if

$$\mathfrak{Z} = Z(\mathrm{GL}(V, K)),$$

then $\mathfrak{F}/(\mathfrak{F} \cap \mathfrak{Z}) \cong \mathscr{G}$. Let $\mathfrak{K}$ be the pre-image of the Frobenius kernel in $\mathfrak{F}$. Since $\mathfrak{K}/(\mathfrak{F} \cap \mathfrak{Z})$ is abelian and $\mathfrak{F} \cap \mathfrak{Z} \subseteq Z(\mathfrak{K})$, $\mathfrak{K}$ is nilpotent. If $p \nmid |\mathfrak{F} \cap \mathfrak{Z}|$, then $\mathfrak{K} = (\mathfrak{F} \cap \mathfrak{Z}) \times \mathfrak{P}$, where $\mathfrak{P}$ is elementary abelian of order q^n and is the p-Sylow subgroup of $\mathfrak{K}$. Since $\mathfrak{F}$ is a subgroup of $\mathrm{GL}(V, K)$ and char $K \neq p$, Lemma 1.3 applies, and we conclude that deg $\rho \geqq (1/d)(q^n - 1)$. Thus for the remainder of the proof, we assume that $p \mid |\mathfrak{F} \cap \mathfrak{Z}|$. Here $\mathfrak{K} = O_{p'}(\mathfrak{K}) \times \mathfrak{P}$, where $\mathfrak{P}$ denotes the p-Sylow subgroup of $\mathfrak{K}$, $O_{p'}(\mathfrak{K}) = O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$, and where $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})$ is an elementary abelian p-group of order q^n. Since $\mathfrak{F} \cap \mathfrak{Z}$ is cyclic, let $\mathfrak{N}$ denote the unique subgroup of index p in $O_p(\mathfrak{F} \cap \mathfrak{Z})$; clearly $\mathfrak{N} \lhd \mathfrak{F}$. If $\mathfrak{P}/\mathfrak{N}$ is non-abelian, then $(\mathfrak{P}/\mathfrak{N})' = O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N} = \Phi(\mathfrak{P}/\mathfrak{N})$ since $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})$ is elementary abelian and $|O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N}| = p$. Note that $\mathscr{G}$ operates irreducibly by conjugation on its Frobenius kernel. For, the Frobenius kernel of $\mathscr{G}$ is a vector space over $\mathrm{GF}(p)$ of order q^n and a Frobenius complement has order $(1/d)(q^n - 1)$ which is relatively prime to p. By complete reducibility and the fixed-point free action of the complement on the kernel, if $\mathscr{G}$ acts reducibly on its Frobenius kernel, then $(1/d)(q^n - 1) \leqq q^{\frac{1}{2}n} - 1$. This implies that

$$(q^n - 1) \leqq (q^{\frac{1}{2}n} - 1)(q - 1) = q^{\frac{1}{2}(n+2)} - q^{\frac{1}{2}n} - q + 1 < q^{\frac{1}{2}(n+2)} - 1,$$

and hence $n < \frac{1}{2}(n + 2)$ or $n < 2$. But then $n = 1, d \leqq 2, q^2 - 1 \leqq 2(q - 1)$, and hence $q + 1 \leqq 2$ which is impossible. Consequently, $\mathfrak{F}$ acts irreducibly on $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})$, and hence $Z(\mathfrak{P}/\mathfrak{N}) = O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N}$. Thus $\mathfrak{P}/\mathfrak{N}$ is an extra-special p-group. Let $\mathfrak{H}$ be the inverse image in $\mathfrak{F}$ of a Frobenius complement of $\mathscr{G}$. Clearly $\mathfrak{H} = \mathfrak{H}_1 \times O_p(\mathfrak{F} \cap \mathfrak{Z})$, where $\mathfrak{H}_1$ is a p'-group containing $O_{p'}(\mathfrak{F} \cap \mathfrak{Z}) = O_{p'}(\mathfrak{K})$. Let $\mathfrak{H}^* = \mathfrak{H}_1 \times \mathfrak{N}$; then

$$C_{\mathfrak{H}^*}(\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})) = O_{p'}(\mathfrak{K}) \times \mathfrak{N},$$

and hence $\mathfrak{H}^*/(O_{p'}(\mathfrak{K}) \times \mathfrak{N})$ is a cyclic group of order $(1/d)(q^n - 1)$ which when operating by conjugation on $\mathfrak{P}/\mathfrak{N}$ both centralizes

$$Z(\mathfrak{P}/\mathfrak{N}) = O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N}$$

and acts fixed-point free on $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})$. Now [**6**, *Kapitel* V, *Satz* **17.13**] applies, and we conclude that $(1/d)(q^n - 1) \leqq (q^{\frac{1}{2}n} + 1)$. However, $q^n = p^{fn}$ and since $\mathfrak{P}/\mathfrak{N}$ is extra-special, $2 \mid fn$. Thus

$$p^{fn} - 1 \leqq (p^{\frac{1}{2}fn} + 1)(p^f - 1) = p^{\frac{1}{2}f(n+2)} + p^f - p^{\frac{1}{2}fn} - 1.$$

If $n \geqq 2$, then $p^{fn} - 1 \leqq p^{\frac{1}{2}f(n+2)} - 1$ and hence $n \leqq \frac{1}{2}(n + 2)$ and then $n = 2$. But if $n = 2$, $d | 3$ and $(q^2 - 1) \leqq d(q + 1)$; thus $q - 1 \leqq d$ which implies that $q = 2$, $q = 3$ or $q = 4$. Since $(n, q) \neq (2, 2)$ and $(n, q) \neq (2, 4)$, we must have $q = 3$. But then $d = 1$ and $3^2 - 1 \leqq 3 + 1$ which is a contradiction. Hence assume that $n = 1$. If q is even, $d = 1$ and $q - 1 \leqq \sqrt{q} + 1$. Thus $q^2 - 4q + 4 \leqq q$, $q^2 - 4q < q$, $q - 4 < 1$, and $q = 2$ or $q = 4$. Since the cases $(n, q) = (1, 2)$ and $(n, q) = (1, 4)$ have been excluded, we may assume that q is odd and then $d = 2$ and $q - 1 \leqq 2(\sqrt{q} + 1)$. Hence $q^2 - 10q < 0$ and $q < 10$. Since $2 | f$, we see that $q = 9$ but $(n, q) = (1, 9)$ has also been excluded. Thus we may assume that $\mathfrak{P}/\mathfrak{N}$ is abelian. If

$$\Omega_1(\mathfrak{P}/\mathfrak{N}) = O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N},$$

then $\mathfrak{P}/\mathfrak{N}$ is cyclic and hence $fn = 1$. Since $(n, q) = (1, 2)$ has been excluded, we may assume that $f = n = 1$, $p \neq 2$, and $\mathfrak{P}/\mathfrak{N}$ is cyclic. But $\mathfrak{F}$ acts trivially on $\Omega_1(\mathfrak{P}/\mathfrak{N}) = O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N}$, and hence $\mathfrak{F}$ acts trivially on $\mathfrak{P}/\mathfrak{N}$ which is impossible. By the same argument above, $\mathfrak{F}$ acts irreducibly on $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})$, and hence $\Omega_1(\mathfrak{P}/\mathfrak{N}) = \mathfrak{P}/\mathfrak{N}$. Thus $\mathfrak{P}/\mathfrak{N}$ is elementary abelian. However, $O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N}$ is centralized by $\mathfrak{F}$ and $|\mathfrak{F}:\mathfrak{P}|$ is relatively prime to p. Also $C_{\mathfrak{F}}(\mathfrak{P}/\mathfrak{N}) \supseteq \mathfrak{P}$ and hence $\mathfrak{P}/\mathfrak{N}$ is a completely reducible $\mathfrak{F}/C_{\mathfrak{F}}(\mathfrak{P}/\mathfrak{N})$-module over $\mathrm{GF}(p)$. Thus there exists a subgroup $\mathfrak{R}$ of $\mathfrak{P}$ such that $\mathfrak{R} \supset \mathfrak{N}$, $\mathfrak{R} \lhd \mathfrak{F}$, and $\mathfrak{P}/\mathfrak{N} = O_p(\mathfrak{F} \cap \mathfrak{Z})/\mathfrak{N} \times \mathfrak{R}/\mathfrak{N}$. As before, if $\mathfrak{H}$ is the inverse image in $\mathfrak{F}$ of a Frobenius complement of $\mathscr{G}$, then $\mathfrak{H} = \mathfrak{H}_1 \times O_p(\mathfrak{F} \cap \mathfrak{Z})$, where $\mathfrak{H}_1$ is a p' subgroup containing $O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$. Then $\mathfrak{H}_1/O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$ is cyclic of order $(1/d)(q^n - 1)$ and $\mathfrak{H}_1\mathfrak{R}$ is a proper subgroup of $\mathfrak{F}$ such that

$$O_p(\mathfrak{F} \cap \mathfrak{Z}) \cap (\mathfrak{H}_1\mathfrak{R}) = O_p(\mathfrak{F} \cap \mathfrak{Z}) \cap \mathfrak{R} = \mathfrak{N}.$$

It is now clear that $\mathfrak{Z} \cap (\mathfrak{H}_1\mathfrak{R}) = (\mathfrak{F} \cap \mathfrak{Z}) \cap (\mathfrak{H}_1\mathfrak{R}) = \mathfrak{N} \times O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$ and $\mathfrak{H}_1\mathfrak{R}(\mathfrak{F} \cap \mathfrak{Z}) \supseteq \mathfrak{H}\mathfrak{P} = \mathfrak{F}$. Hence $\mathfrak{H}_1\mathfrak{R}/(\mathfrak{Z} \cap (\mathfrak{H}_1\mathfrak{R})) \cong \mathfrak{F}/\mathfrak{F} \cap \mathfrak{Z} \cong \mathscr{G}$, which contradicts the minimal choice of $\mathfrak{F}$ and so this case does not occur. This completes the proof.

Now let F denote a finite field of $q = p^f$ elements, where p is a prime integer and $f \geqq 1$ is an integer. Let W denote a vector space of dimension $n \geqq 1$ over F, let $d = \gcd\{n + 1, q - 1\}$ and let $\mathfrak{L} = \{X \in \mathrm{GL}(W, F) | \det X \in (F^\times)^d\}$. We shall denote by $W\mathfrak{L}$ the obvious semi-direct product.

The final result of this section is the following.

THEOREM 3.2. *Let $\mathscr{G}$ be a finite group containing a subgroup $\mathscr{H}$ isomorphic to $W\mathfrak{L}$ with $n \geqq 2$. If $\rho: \mathscr{G} \to \mathrm{GL}(V, K)$ is a projective representation of $\mathscr{G}$ such that ρ restricted to $\mathscr{H}$ is faithful, if $p \neq \mathrm{char}\, K$, and if the cases* (a) $n = 2$, $p = 2$ *and* (b) $n = 3$, $q = 2$ *are excluded, then* $\deg \rho$ $(= \dim_K V) \geqq q^n - 1$.

Proof. As in Theorem 3.1, we may assume that $\mathscr{G} = \mathscr{H}$, that K is algebraically closed, and that $\rho^*: \mathscr{G} \to \mathrm{PGL}(V, K)$ is a monomorphism. Moreover, there exists a finite subgroup $\mathfrak{F}$ of $\mathrm{GL}(V, K)$ of minimal order such that $\mathfrak{F}/(\mathfrak{F} \cap \mathfrak{Z}) \cong W\mathfrak{L}$. Let $\mathfrak{K}$ be the pre-image of W in $\mathfrak{F}$; as above, $\mathfrak{K}$ is nilpotent. If $p \nmid |\mathfrak{F} \cap \mathfrak{Z}|$, then $\mathfrak{K} = (\mathfrak{F} \cap \mathfrak{Z}) \times \mathfrak{P}$, where $\mathfrak{P}$ is the p-Sylow subgroup of $\mathfrak{K}$ and is isomorphic as a group to W and where $O_{p'}(\mathfrak{K}) = \mathfrak{F} \cap \mathfrak{Z}$. Since $\mathfrak{F}$ is a subgroup of GL(V, K) and $p \neq \operatorname{char} K$, Lemma 1.4 applies, and we conclude that $\deg \rho \geqq q^n - 1$. Thus for the remainder of the proof, we assume that $p \,|\, |\mathfrak{F} \cap \mathfrak{Z}|$. Here $\mathfrak{K} = \mathfrak{P} \times O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$, where $\mathfrak{P}$ is the p-Sylow subgroup of $\mathfrak{K}$, $O_{p'}(\mathfrak{K}) = O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$, and $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z}) \cong W$. Suppose that there exists an elementary abelian subgroup $\mathfrak{E}$ of $\mathfrak{P}$ such that $\mathfrak{E} \lhd \mathfrak{F}$, $\mathfrak{E} \cong W$, and $\mathfrak{E} \cap O_p(\mathfrak{F} \cap \mathfrak{Z}) = (1)$. Then $\mathfrak{P} = \mathfrak{E} \times O_p(\mathfrak{F} \cap \mathfrak{Z})$ and $\mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z}) \cong \mathfrak{E}$ over $\mathfrak{F}$. Again, since $\mathfrak{L}$ is transitive on $W^{\#}$, $\mathfrak{F}$ acting by conjugation on $\mathfrak{E}$ is transitive on $\mathfrak{E}^{\#}$, and the proof can be completed as above. In order to demonstrate the existence of such a subgroup $\mathfrak{E}$ of $\mathfrak{P}$, let $\mathfrak{D}$ be a subgroup of $\mathfrak{P}$ of minimal order such that $\mathfrak{D}$ is a normal subgroup of $\mathfrak{F}$ and $\mathfrak{P} = \mathfrak{D}O_p(\mathfrak{F} \cap \mathfrak{Z})$. Set $\mathfrak{Y} = \mathfrak{D} \cap O_p(\mathfrak{F} \cap \mathfrak{Z})$; if $\mathfrak{Y} = (1)$, our proof is complete and so we assume that $\mathfrak{Y} \neq (1)$. Note that $\mathfrak{D}/\mathfrak{Y} \cong \mathfrak{P}/O_p(\mathfrak{F} \cap \mathfrak{Z})$ over $\mathfrak{F}$ and hence $C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{Y}) = \mathfrak{K}$. Since $\mathfrak{Y}$ is cyclic, let $\mathfrak{N}$ denote the unique subgroup of $\mathfrak{Y}$ of index p; clearly $\mathfrak{N} \lhd \mathfrak{F}$. If $\mathfrak{D}/\mathfrak{N}$ is non-abelian, then

$$(\mathfrak{D}/\mathfrak{N})' = \mathfrak{Y}/\mathfrak{N} = \Phi(\mathfrak{P}/\mathfrak{N})$$

since $|\mathfrak{Y}/\mathfrak{N}| = p$. Also $Z(\mathfrak{D}/\mathfrak{N}) \supseteq \mathfrak{Y}/\mathfrak{N}$ and $\mathfrak{F}$ operates transitively on $(\mathfrak{D}/\mathfrak{Y})^{\#}$ and hence irreducibly on $\mathfrak{D}/\mathfrak{Y}$. Thus $Z(\mathfrak{D}/\mathfrak{N}) = \mathfrak{Y}/\mathfrak{N}$ and $\mathfrak{D}/\mathfrak{N}$ is an extra-special p-group. Since $C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{N}) = C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{Y}) = \mathfrak{K}$, $\mathfrak{P} = \mathfrak{D}O_p(\mathfrak{F} \cap \mathfrak{Z})$, $\mathfrak{K} = \mathfrak{P} \times O_{p'}(\mathfrak{F} \cap \mathfrak{Z})$ and $C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{N}) = O_p(\mathfrak{F} \cap \mathfrak{Z}) \times O_{p'}(\mathfrak{F} \cap \mathfrak{Z}) = \mathfrak{F} \cap \mathfrak{Z}$. Since $|\mathrm{GL}(W, F): \mathfrak{L}| = d$, the "Singer cycle" of GL(W, F) (cf. [**6**, *Kapitel* II, the proof of *Satz* 7.3]) implies that there exists an element of $\mathfrak{L}$ of order $(1/d)(q^n - 1) > 1$ (since $n \geqq 2$). Hence there exists a p'-element $\alpha \in \mathfrak{F}$ such that $\alpha(\mathfrak{F} \cap \mathfrak{Z})$ is an element of order $(1/d)(q^n - 1) > 1$ in $\mathfrak{F}/(\mathfrak{F} \cap \mathfrak{Z})$. Also $\mathfrak{F}/(\mathfrak{F} \cap \mathfrak{Z})$ can be viewed as a subgroup of Aut$(\mathfrak{D}/\mathfrak{N})$ and $\alpha(\mathfrak{F} \cap \mathfrak{Z})$ is fixed point free on $\mathfrak{D}/\mathfrak{Y}$ and centralizes $Z(\mathfrak{D}/\mathfrak{N}) = \mathfrak{Y}/\mathfrak{N}$. Consequently, [**6**, *Kapitel* V, *Satz* 17.13] applies and we conclude that $2 \,|\, fn$ and $(1/d)(p^{fn} - 1) \leqq p^{\frac{1}{2}fn} + 1$. Since $n \geqq 2$, as above, we must have $n = 2$ and $q = 2$ or 4 but both of these cases have been excluded. Thus we may assume that $\mathfrak{D}/\mathfrak{N}$ is abelian. Clearly $\Omega_1(\mathfrak{D}/\mathfrak{N}) \supseteq \mathfrak{Y}/\mathfrak{N}$ and if $\Omega_1(\mathfrak{D}/\mathfrak{N}) = \mathfrak{Y}/\mathfrak{N}$, then $\mathfrak{D}/\mathfrak{N}$ is cyclic, $|\mathfrak{D}/\mathfrak{Y}| = p$ and hence $fn = 1$; but $n = 2$. Thus $\Omega_1(\mathfrak{D}/\mathfrak{N})$ is elementary abelian and, since $C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{N}) \subseteq C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{Y}) = \mathfrak{K}$, we have $C_{\mathfrak{F}}(\mathfrak{D}/\mathfrak{N}) = \mathfrak{K}$. Let $\mathfrak{M}$ be the inverse image of $\mathfrak{L}$ in $\mathfrak{F}$. Then $\mathfrak{M}/(\mathfrak{F} \cap \mathfrak{Z})$ (acting by conjugation) is a group of automorphisms on the elementary abelian p-group $\mathfrak{D}/\mathfrak{N}$ and centralizes $\mathfrak{Y}/\mathfrak{N}$ and the action of $\mathfrak{M}/(\mathfrak{F} \cap \mathfrak{Z})$ on $\mathfrak{D}/\mathfrak{Y}$ mimics the action of $\mathfrak{L}$ on W. Now, setting $F_1 = \mathrm{GF}(p)$, Lemma 2.6 implies that $\mathrm{Ext}_{F_1[\mathfrak{L}]}{}^1(W, F_1) = (0)$. Hence there exists a subgroup $\mathfrak{D}_1$ in $\mathfrak{D}$ such that $\mathfrak{D}_1 \supset \mathfrak{N}$, $\mathfrak{D}/\mathfrak{N} = \mathfrak{D}_1/\mathfrak{N} \times \mathfrak{Y}/\mathfrak{N}$ and such that $\mathfrak{D}_1$ is invariant under $\mathfrak{M}$. But $\mathfrak{P} = \mathfrak{D}O_p(\mathfrak{F} \cap \mathfrak{Z})$ and so $\mathfrak{D}_1$ is invariant under $\mathfrak{P}$. Since $\mathfrak{F} = \mathfrak{K}\mathfrak{M} = \mathfrak{P}(\mathfrak{F} \cap \mathfrak{Z})\mathfrak{M}$, we have $\mathfrak{D}_1 \lhd \mathfrak{F}$. Also $\mathfrak{P} = \mathfrak{D}O_p(\mathfrak{F} \cap \mathfrak{Z}) = \mathfrak{D}_1\mathfrak{Y}O_p(\mathfrak{F} \cap \mathfrak{Z}) = \mathfrak{D}_1O_p(\mathfrak{F} \cap \mathfrak{Z})$. This contradicts the minimal choice of $\mathfrak{D}$, and the theorem follows.

4. Lower bounds for the degrees of projective representations of the groups PSL(n, q). We now proceed to show how the results of § 3 can be applied to obtain lower bounds for the degrees of projective representations of the finite groups PSL(n, q), and we give a new proof of a classical result (Theorem 4.5).

LEMMA 4.1. *Let $n \geqq 2$ be an integer, let $q = p^f$, where p is a prime integer and f is a positive integer, let F denote a field of q elements, and let $d = \gcd\{n, q - 1\}$. Then:*

(a) PSL(n, q) *contains a subgroup isomorphic to the "natural" semi-direct product $W\mathfrak{L}$, where W denotes a vector space of dimension $n - 1$ over F and where $\mathfrak{L} = \{X \in \mathrm{GL}(W, F) | \det X \in (F^\times)^d\}$,*

(b) *if $(n, q) \neq (2, 2)$ and $(n, q) \neq (2, 3)$, then* PSL(n, q) *contains a subgroup which is a Frobenius group of order $(1/d)q^{n-1}(q^{n-1} - 1)$ with an elementary abelian kernel of order q^{n-1} and a cyclic complement.*

Proof. Note that the inverse image of the subgroup PSL(n, q) of the group PGL(n, q) under the natural homomorphism of GL(n, q) onto PGL(n, q) is $\mathfrak{H} = \{X \in \mathrm{GL}(n, q) | \det X \in (F^\times)^d\}$. Let $\mathfrak{K}$ denote the subgroup of GL(n, K) formed by all matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ X & E \end{smallmatrix}\right)$, where E is the $(n - 1) \times (n - 1)$ identity F-matrix, 0 denotes the $1 \times (n - 1)$ zero F-matrix, and X is an arbitrary element of the set W^* of all $(n - 1) \times 1$ F-matrices. Note that the mapping of $\mathfrak{K}$ into the set W^* defined by

$$\begin{pmatrix} 1 & 0 \\ X & E \end{pmatrix} \rightarrow X$$

is an isomorphism of $\mathfrak{K}$ onto the additive group W^*. To demonstrate (a), let $\mathfrak{M}$ consist of all matrices of GL(n, K) of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & C \end{smallmatrix}\right)$, where 0 denotes a $1 \times (n - 1)$ and $(n - 1) \times 1$ zero F-matrix and C is an arbitrary matrix in $\{C \in \mathrm{GL}(n - 1, q) | \det C \in (F^\times)^d\}$. It is easy to see that $\mathfrak{K}$, $\mathfrak{M}$, and $\mathfrak{K}\mathfrak{M}$ are subgroups of $\mathfrak{H}$ and that $(\mathfrak{K}\mathfrak{M}) \cap Z(\mathrm{GL}(n, q)) = (1)$. Hence PSL$(n, q)$ contains a subgroup isomorphic to $\mathfrak{K}\mathfrak{M}$. But $\mathfrak{K} \cong W^* \cong W$ and $\mathfrak{M}$ is isomorphic to $\mathfrak{L}$. Clearly $\mathfrak{K}\mathfrak{M}$ is of the desired type.

To demonstrate (b), note that $(1/d)(q^{n-1} - 1) = 1$ if and only if $(n, q) = (2, 2)$ or $(n, q) = (2, 3)$. Hence we may assume that

$$(1/d)(q^{n-1} - 1) > 1.$$

Since $n - 1 \geqq 1$, GL$(n - 1, F)$ has a cyclic subgroup $\mathfrak{T} = \langle T \rangle$ of order $(1/d)(q^{n-1} - 1)$ such that $\det T \in (F^\times)^d$ and such that $\mathfrak{T}$ acts regularly on the non-zero F-space of $(n - 1)$ F-tuples (cf. [**6**, *Kapitel* II, *Satz* 7.3]). Now let $\mathfrak{M}$ denote the set of all matrices of GL(n, F) of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & C \end{smallmatrix}\right)$, where C is any matrix in $\mathfrak{T}$. It is easy to see that $\mathfrak{K}\mathfrak{M}$ is a Frobenius subgroup of $\mathfrak{H}$ with kernel $\mathfrak{K}$ and complement $\mathfrak{M} \cong \mathfrak{T}$. Again, $(\mathfrak{K}\mathfrak{M}) \cap Z(\mathrm{GL}(n, q)) = (1)$ and the result follows.

THEOREM 4.2. *Using the notation above* ($n \geqq 2$), *if* $(n, q) \neq (2, 4)$, $(2, 9)$, $(3, 2)$, $(3, 4)$, *then the degree of any non-trivial projective representation* ρ *of* $\mathrm{PSL}(n, q)$ *over any field* K *with* char $K \neq p$ *is at least* $(1/d)(q^{n-1} - 1)$.

Proof. Since $(1/d)(q^{n-1} - 1) = 1$ if and only if $(n, q) = (2, 2)$ or $(n, q) = (2, 3)$, we may also assume that $(n, q) \neq (2, 2)$ and $(n, q) \neq (2, 3)$. But then $\mathrm{PSL}(n, q)$ is simple and so the ρ induced group homomorphism ρ^*: $\mathrm{PSL}(n, q) \to \mathrm{PGL}(\bar{n}, K)$, where $\bar{n} = \deg \rho$, is a monomorphism since ρ is non-trivial. The theorem now follows from Theorem 3.1 and Lemma 4.1 (b).

A similar proof using Theorem 3.2 and Lemma 4.1 (a) yields the following result.

THEOREM 4.3. *If* $n \geqq 3$ *and if the cases* $n = 3$, $p = 2$ *and* $n = 4$, $q = 2$ *are excluded, then the degree of any non-trivial projective representation* ρ *of* $\mathrm{PSL}(n, q)$ *over any field* K *with* char $K \neq p$ *is at least* $q^{n-1} - 1$.

For projective representations of $\mathrm{PSL}(n, q)$ in the characteristic p case we have the following result.

THEOREM 4.4. *Let* $n \geqq 2$ *and* $q = p^f$ *be as above. If* $(n, q) \neq (2, 2)$ *and* $(n, q) \neq (2, 3)$, *then the degree of any non-trivial projective representation of* $\mathrm{PSL}(n, q)$ *over any field of characteristic* p *is at least* n.

Proof. Let ρ denote a non-trivial projective representation of $\mathrm{PSL}(n, q)$ of degree $\bar{n}$ over a field K of characteristic p. Clearly we may assume that K is algebraically closed. Since $\mathrm{PSL}(n, q)$ has a finite representation group over K, we may assume that K is the algebraic closure of $\mathrm{GF}(p)$. Since $\mathrm{PSL}(n, q)$ is finite, we may assume that ρ takes values in $\mathrm{GL}(\bar{n}, \bar{K})$, where $\bar{K}$ is a finite field of characteristic p. Since $\mathrm{PSL}(n, q)$ is simple, ρ induces a group monomorphism ρ^*: $\mathrm{PSL}(n, q) \to \mathrm{PGL}(\bar{n}, \bar{K})$. But the p-Sylow subgroups of $\mathrm{PSL}(n, q)$ and $\mathrm{PGL}(\bar{n}, \bar{K})$ have classes $n - 1$ and $\bar{n} - 1$, respectively (cf. [**6**, *Kapitel* III, *Satz* 16.3]). Hence $\bar{n} \geqq n$.

To conclude, we give a new proof of the following well-known result (cf. [**6**, *Kapitel* II, *Satz* 6.14]).

THEOREM 4.5. *Let* $n_1 \geqq 2$ *and* $n_2 \geqq 2$ *be integers and let* $q_1 = p_1^{f_1}$ *and* $q_2 = p_2^{f_2}$, *where* p_1 *and* p_2 *are prime integers and* f_1 *and* f_2 *are positive integers. If* $\mathrm{PSL}(n_1, q_1) \cong \mathrm{PSL}(n_2, q_2)$ *with* $(n_1, q_1) \neq (n_2, q_2)$, *then we have one of the follwing two cases:*

$$\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5) \qquad \text{or} \qquad \mathrm{PSL}(2, 7) \cong \mathrm{PSL}(3, 2).$$

Proof. Since $\mathrm{PSL}(2, 2)$ and $\mathrm{PSL}(2, 3)$ are the only solvable groups under consideration and have different orders, we may assume that $(n_i, q_i) \neq (2, 2)$ and $(n_i, q_i) \neq (2, 3)$ for $i = 1, 2$. If $p_1 = p_2$, then Theorem 4.4 implies that $n_1 \geqq n_2$ and $n_2 \geqq n_1$. Hence, in this case, $n_1 = n_2$ and, comparing the orders of p-Sylow subgroups, we conclude that $q_1 = q_2$. Thus we may assume that

$p_1 \neq p_2$. First suppose that $n_1 = n_2 = n$. If $n \geqq 3$, then $p_1 \neq 2$ or $p_2 \neq 2$ and Theorem 4.3 implies that $n \geqq q^{n-1} - 1 \geqq 3^{n-1} - 1$. Since $3^{n-1} - 1 > n$ for all $n \geqq 3$, we may assume that $n = 2$. Suppose that $p_1 = 2$; then $\gcd\{2, q_1 - 1\} = 1$ and $2 \geqq q_1 - 1$ by Theorem 4.2. Hence $q_1 = 4$; but since

$$|\mathrm{PSL}(2, 4)| \neq |\mathrm{PSL}(2, 9)|,$$

we must have $q_2 \neq 9$. Applying Theorem 4.2 again, we obtain $2 \geqq \frac{1}{2}(q_2 - 1)$ or $q_2 \leqq 5$. Hence $q_2 = 5$; but, as is well known, $\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5)$ (cf. [**6**, *Kapitel* II, *Satz* 6.14]). Suppose now that $p_1 \neq 2 \neq p_2$. Then either $q_i = 9$ or $4 \geqq q_i - 1$ for $i = 1, 2$ by Theorem 4.2. But $|\mathrm{PSL}(2, 5)| \neq |\mathrm{PSL}(2, 9)|$ and so this case is excluded. Thus we may now assume that $2 \leqq n_1 < n_2$. If $p_2 \neq 2$, then $n_1 \geqq q_2^{n_2-1} - 1 \geqq 3^{n_2-1} - 1 > n_2 > n_1$ (using Theorem 4.3) and hence $p_2 = 2$ and p_1 is odd. If $n_2 = 4$, then $\gcd\{n_2, q_2 - 1\} = 1$ and Theorems 4.2 and 4.3 imply: if $n_2 \geqq 4$, then $n_1 \geqq q_2^{n_2-1} - 1 \geqq 2^{n_2-1} - 1 > n_2 > n_1$, which is impossible. Hence $n_2 = 3$ and $n_1 = 2$. If $q_2 \geqq 8$, then

$$2 \geqq \frac{1}{\gcd\{3, q_2 - 1\}} (q_2^2 - 1) \geqq q_2 + 1$$

by Theorem 4.2; thus $q_2 = 2$ or $q_2 = 4$. Since

$$|\mathrm{PSL}(3, 2)| \neq |\mathrm{PSL}(2, 9)| \neq |\mathrm{PSL}(3, 4)|,$$

we have $q_1 \neq 9$. Then $3 \geqq \frac{1}{2}(q_1 - 1)$ or $q_1 \leqq 7$. Hence $q_1 = 5$ or 7 and, by comparing orders, we must have $q_2 = 2$ and $q_1 = 7$. But, here again, $\mathrm{PSL}(2, 7) \cong \mathrm{PSL}(3, 2)$ [**6**, *Kapitel* II, *Satz* 6.14].

References

1. R. Brauer, *Zur Darstellungstheorie der Gruppen endlicher Ordnung*, Math. Z. *63* (1956), 406–444.
2. H. Cartan and S. Eilenberg, *Homological algebra* (Princeton Univ. Press, Princeton, N.J., 1956).
3. D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).
4. D. G. Higman, *Flag-transitive collineation groups of finite projective spaces*, Illinois J. Math. *6* (1962), 434–446.
5. C. Hering, *On transitive linear groups* (in preparation).
6. B. Huppert, *Endliche Gruppen*. I (Springer-Verlag, Berlin, 1967).
7. S. MacLane, *Homology* (Springer-Verlag, Berlin, 1963).
8. D. S. Rim, *Modules over finite groups*, Ann. of Math. (2) *69* (1959), 700–712.

University of Illinois at Chicago Circle,
Chicago, Illinois