Can. J. Math., Vol. XXX, No. 5, 1978, pp. 1092–1102

PROJECTIVE REPRESENTATIONS OF MINIMUM DEGREE OF GROUP EXTENSIONS

WALTER FEIT AND JACQUES TITS

1. Introduction. Let G be a finite simple group and let $\mathbf{F}$ be an algebraically closed field. A faithful projective $\mathbf{F}$-representation of G of smallest possible degree often cannot be lifted to an ordinary representation of G, though it can of course be lifted to an ordinary representation of some central extension of G. It is a natural question to ask whether by considering non-central extensions, it is possible in some cases to decrease the smallest degree of a faithful projective representation. In other words, is it possible to find a finite group H which involves G (as a quotient of a subgroup) such that H has a faithful $\mathbf{F}$-representation whose degree is strictly smaller than the degree of any faithful projective $\mathbf{F}$-representation of G.

Let G and $\mathbf{F}$ be as above, let

$$\langle 1\rangle \rightarrow N \rightarrow H \xrightarrow{\gamma} G \rightarrow \langle 1\rangle$$

be an exact sequence and let $\lambda : H \rightarrow PGL_m(\mathbf{F})$ be a projective representation. We say that the system (H, γ, λ) is *minimal with respect to* G *and* $\mathbf{F}$ if the following conditions are satisfied:

i) no proper subgroup of H maps onto G;

ii) m is the smallest degree of a nontrivial projective representation of H.

In studying the question formulated above, it is clearly sufficient to consider systems (H, γ, λ) having these properties. This is done in the following theorem.

THEOREM. *Let* $\mathbf{F}$ *be an algebraically closed field.*

I) *Suppose* char $\mathbf{F} \neq 2$. *For every integer* $n \geqq 1$ *there exists an exact sequence*

$$(*)_n \quad \langle 1\rangle \rightarrow (\mathbf{Z}/2\mathbf{Z})^{2n} \rightarrow A_n \xrightarrow{\alpha_n} \mathrm{Sp}_{2n}(2) \rightarrow \langle 1\rangle$$

and a projective representation $\rho_n : A_n \rightarrow PGL_{2^n}(\mathbf{F})$ *such that* $\alpha_n(\mathrm{Ker}\, \rho_n) \neq \mathrm{Sp}_{2n}(2)$. *If* $n \geqq 4$, *this property characterizes uniquely* $(*)_n$ *and the pair* $\{\rho_n, \rho_n^*\}$, *where* ρ_n^* *denotes the contragredient of* ρ_n. *Furthermore,* (A_n, α_n, ρ_n) *is minimal with respect to* $\mathrm{Sp}_{2n}(2)$ *and* $\mathbf{F}$; *in particular,* ρ_n *is irreducible and the sequence* $(*)_n$ *does not split.*

II) *Let* G *be a finite non-abelian simple group and let* (H, γ, λ) *be minimal with respect to* G *and* $\mathbf{F}$. *Then one of the following holds:*

Received June 22, 1977. The work on this paper was begun while the second author was visiting Yale University and concluded while the first author was visiting the IHES. We wish to thank both institutions for their hospitality. The authors were partially supported by NSF contracts GP-33591 and MCS 76-06153.

(i) $\operatorname{Ker} \gamma = \operatorname{Ker} \lambda$; *in other words* λ *factorizes through* G.

(ii) $\operatorname{Char} \mathbf{F} \neq 2$ *and* $m = 2^n$ *for some integer* $n \geqq 4$. *There exists an irreducible representation* $\mu : G \rightarrow \mathrm{Sp}_{2n}(2)$ *and an epimorphism* $\nu : H \rightarrow \alpha_n^{-1}(\mu(G))$ *such that* $\alpha_n \circ \nu = \mu \circ \gamma$ *and* λ *is equivalent to* $\rho_n \circ \nu$ *or* $\rho_n^* \circ \nu$.

Assertion (ii) is summarized in the following commutative diagram

$$
\begin{tikzcd}
G \arrow[d, "\mu"'] & H \arrow[l, "\gamma"'] \arrow[d, "\nu"] \arrow[dr, "\lambda"] & \\
\mathrm{Sp}_{2n}(2) & A_n \arrow[l, "\alpha_n"] \arrow[r, "\rho_n \text{ or } \rho_n^*"'] & PGL_{2^n}(\mathbf{F})
\end{tikzcd} .
$$

The existence of the non-split extension $(*)_n$ and of the representation ρ_n has been established by R. Griess [**2**] but will be proved again here.

For given G and $\mathbf{F}$, let d be the minimum degree of a nontrivial projective $\mathbf{F}$-representation of G and let s be the smallest integer such that G can be embedded in $\mathrm{Sp}_{2s}(2)$. Conclusion (i) of the theorem fails to hold for any choice of (H, γ) precisely when $2^s < d$. In that case conclusion (ii) holds and H is of course necessarily a nonsplit extension of G.

In Section 4 it is verified that conclusion (i) holds for all known simple groups which are not of Lie type in characteristic 2, in particular for all known sporadic groups.

The group $\mathrm{Sp}_{2n}(2^k)$ contains $O_{2n}^+(2^k)$ and $O_{2n}^-(2^k)$ and can be embedded in the group $\mathrm{Sp}_{2nk}(2)$. Thus it follows from the results of V. Landazuri and G. M. Seitz [**4**] that conclusion (i) of the theorem does not hold (for any choice of (H, γ)) for the following classes of simple groups and any algebraically closed field $\mathbf{F}$ with $\operatorname{char} \mathbf{F} \neq 2$.

$\mathrm{Sp}_{2n}(2^k)$ for $n \geqq 2$ except for $\mathrm{Sp}_4(2)$ and $\mathrm{Sp}_6(2)$;

$O_{2n}^+(2^k)'$ for $n \geqq 4$ except for $O_8^+(2)'$;

$O_{2n}^-(2^k)'$ for $n \geqq 4$.

In particular, this proves the (probably known) fact that for each of these subgroups G of $\mathrm{Sp}_{2nk}(2)$, the group $\alpha_n^{-1}(G)$ is a nonsplit extension.

2. Generalities on extraspecial and related groups. In this section we recall some known facts and fix notation.

2.1. Let p be a prime number, d a positive integer and V a d-dimensional vector space over $\mathbf{F}_p$. The additive group of $\mathbf{F}_p$ will also be denoted by $\mathbf{F}_p$. Let $f : V \times V \rightarrow \mathbf{F}_p$ be an alternating form whose radical will be denoted by V^0. If $p = 2$ let $q : V \rightarrow \mathbf{F}_2$ be a quadratic form whose associated bilinear form is f. It is well known (and easy to see) that there is a central extension

$$\langle 0 \rangle \rightarrow \mathbf{F}_p \rightarrow E \xrightarrow{\pi} V \rightarrow \langle 0 \rangle,$$

https://doi.org/10.4153/CJM-1978-092-5 Published online by Cambridge University Press

unique up to isomorphism, such that for $x, y \in E$ one has

(1) $[x, y] = f(\pi(x), \pi(y))$,

(2) $x^p = 1$ or $q(\pi(x))$ according to whether $p \neq 2$ or $p = 2$.

Furthermore,

(3) *If B is a subset of E mapped bijectively by π onto a basis of V, the group E is generated by $B \cup \mathbf{F}_p$ and defined by any set of relations defining $\mathbf{F}_p$ together with the relations* (1), (2) *for x, y in B.*

The center $\pi^{-1}(V^0)$ of E will be denoted by Z. If f or q needs to be specified we will use the notation $E(f)$ or $E(q)$ in place of E.

2.2. From now on we will assume that Z is cyclic. If $p \neq 2$ this means that f is nondegenerate, i.e. $V^0 = \{0\}$. If $p = 2$, q is nondegenerate and of defect at most one, i.e. $\dim V^0 \leqq 1$ and $q(V^0) \neq \{0\}$ if $\dim V^0 = 1$.

Let $A(= A(f)$ or $A(q))$ be the group of all automorphisms of E which centralize Z. Let $I(= I(f)$ or $I(q))$ be the group of inner automorphisms of E. It is readily seen that an element of A belongs to I if and only if it induces the identity on V. It then follows from (3) that one has an exact sequence

$$(*) \quad \langle 1 \rangle \to I \to A \to \begin{Bmatrix} \mathrm{Sp}(f) \\ O(q) \end{Bmatrix} \to \langle 1 \rangle \quad \begin{matrix} \text{if} \\ \text{if} \end{matrix} \begin{Bmatrix} p \neq 2 \\ p = 2 \end{Bmatrix}.$$

2.3. If $p \neq 2$, it is obvious (and well-known) that the sequence (*) splits: a section is provided by the centralizer of any element of A which projects onto the element -1 of $\mathrm{Sp}(f)$. (One can also observe, as J.-P. Serre pointed out to us, that $\frac{1}{2}f$ is a cocycle which is left invariant by $\mathrm{Sp}(f)$ and defines the extension E.)

Suppose $p = 2$. If $\dim V = 2n + 1$ (and hence $\dim V^0 = 1$), (*) will turn out to be the sequence $(*)_n$ of our theorem. Thus the latter and the remark at the end of Section 1 show, though in a rather roundabout way, that (*) does not split for $\dim V \geqq 9$. In fact, it is known [**2**] that the non-splitting starts with $\dim V = 5$. The appendix contains a short direct proof of that fact.

2.4. Elementary computations show that the faithful irreducible complex representations τ of E are in one to one correspondence with the faithful complex linear characters χ of Z. The correspondence can be described as follows:

$\tau_{|Z}$ is a sum of copies of χ;
τ is induced by any linear character χ_1 of any maximal commutative subgroup of E such that $(\chi_1)_{|Z} = \chi$.

The latter construction shows that if $2n$ $(= d$ or $d - 1)$ is the dimension of V/V^0, then the degree of τ is p^n.

If $\mathbf{F}$ is an algebraically closed field with char $\mathbf{F} \neq p$ then the same statements are true if $\mathbf{C}$ is replaced by $\mathbf{F}$.

2.5. PROPOSITION. *Let* $\mathbf{F}$ *be an algebraically closed field with* char $\mathbf{F} \neq p$. *Let* $\tau : E \rightarrow GL_{p^n}(\mathbf{F})$ *be a faithful irreducible representation of* E. *Then the normalizer* A_τ *of* $\tau(E)$ *in* $GL_{p^n}(\mathbf{F})$ *is an extension of* A *by the group of all scalar matrices. In particular, the canonical projection* $A_\tau \rightarrow PGL_{p^n}(\mathbf{F})$ *factorizes through a faithful projective representation of* A.

Let $a \in A$. The representations τ and $\tau \circ a$ of E coincide on Z. Thus they are equivalent by 2.4. In other words, there exists an element g of $GL_{p^n}(\mathbf{F})$ such that $(\operatorname{Inn} g) \circ \tau = \tau \circ a$, which means that $g \in A_\tau$ and that $\operatorname{Inn} g$ and a induce the same automorphism on $\tau(E)$ identified with E. The proposition follows readily.

2.6. LEMMA. *Let* p *be a prime and let* F *be a non-abelian* p*-group all of whose proper characteristic subgroups are cyclic and central. Then,* F *is a group* $E(f)$ *or* $E(q)$ *of the type considered above* (*with* Z *cyclic*).

The center Y of F is cyclic and F/Y is elementary abelian (since it has no proper nontrivial characteristic subgroup). Thus F has class 2 and so $[x, y]^p = [x, y^p] = 1$ for all $x, y \in F$. Setting $p' = 4$ or p according to whether p is even or odd, we have

$$(xy)^{p'} = x^{p'}y^{p'}[y, x]^{p'(p'-1)/2} = x^{p'}y^{p'}.$$

Therefore, $\varphi : x \mapsto x^{p'}$ is an endomorphism of F. Its kernel cannot be central as its image is contained in Y, and so is cyclic, while F/Y is not cyclic. Thus $\operatorname{Ker} \varphi = F$. In other words, F has exponent p'. The lemma now follows from standard results (see e.g. [**3**], Satz 13.7 and p. 355]).

3. Proof of the theorem.

3.1. The following statement will be proved in subsections 3.2 to 3.4.

(II′) *Assertion* (II) *of the theorem holds if one takes for* $(*)_n$ *the exact sequence* $(*)$ *of* 2.2 *with* $p = 2$ *and* $\dim V = 2n + 1$ (*hence* $\dim V^0 = 1$), *and for* ρ_n *the projective representation of* $A = A_n$ *described in the last part of Proposition* 2.5.

3.2. Upon replacing H by $\lambda(H)$, we may (and will) assume that λ is faithful. Let $\tilde{H}$ be a finite central extension of H such that λ lifts to an ordinary faithful representation $\tilde{\lambda} : \tilde{H} \rightarrow GL_m(\mathbf{F})$. Let $\eta : \tilde{H} \rightarrow H$ be the extension homomorphism and let $\tilde{N}$ be the kernel of $\tilde{\gamma} = \gamma \circ \eta : \tilde{H} \rightarrow G$.

The group N (and hence $\tilde{N}$) is nilpotent; indeed, by the Frattini argument, γ maps the normalizer of any Sylow subgroup S of N onto G, but then the fact that (H, γ, λ) is minimal with respect to G and $\mathbf{F}$ implies that S is normal in N. Furthermore, if char $\mathbf{F} = p$ then p does not divide the order of $\tilde{N}$ since any normal p-subgroup of $\tilde{H}$ must be in the kernel of the irreducible representation $\tilde{\lambda}$.

3.3. We next prove that

If M is a subgroup of $\tilde{N}$ which is normal in $\tilde{H}$, then either $\tilde{\lambda}_{|M}$ is irreducible or M is cyclic and central in $\tilde{H}$.

Since $\tilde{\lambda}$ is irreducible, it follows that $\tilde{\lambda}_{|M}$ is completely reducible. Thus $\tilde{\lambda}_{|M} = \lambda_1 + \ldots + \lambda_k$, where each λ_i is a sum of equivalent irreducible representations and the irreducible components of λ_i and λ_j are not equivalent if $i \neq j$. The group $\tilde{H}$ acts transitively on the set λ_i. Therefore, calling $\tilde{H}_1$ the stabilizer of λ_1 in $\tilde{H}$, we have

$$|G : \tilde{\gamma}(\tilde{H}_1)| \leqq |\tilde{H} : \tilde{H}_1| = k \leqq m.$$

But the assumption of minimality implies that H, and a fortiori G, has no nontrivial representation of degree strictly smaller than m. Consequently, G has no proper subgroup of index smaller than m. Hence $G = \tilde{\gamma}(\tilde{H}_1)$ and, again by the minimality, $\eta(\tilde{H}_1) = H$ so that $\tilde{H}_1 = \tilde{H}$. Thus, $\tilde{\lambda}|_M$ is a direct sum of isomorphic irreducible representations of M. In other words, $\tilde{\lambda}_{|M}$ is the tensor product of a trivial representation $\lambda' : M \rightarrow GL(X)$ and an irreducible representation $\lambda'' : M \rightarrow GL(Y)$. In that decomposition, the projective spaces of X and Y are uniquely defined up to unique isomorphisms. Therefore λ induces projective representations of H into $PGL(X)$ and $PGL(Y)$, at least one of which is not trivial. By minimality it follows that either $\dim X = 1$ or $\dim Y = 1$. Consequently, either $\tilde{\lambda}_{|M}$ is irreducible or $\tilde{\lambda}(M)$ consists of scalar matrices and so M is cyclic and central in $\tilde{H}$.

3.4. From now on, we assume that condition (i) of the theorem is not satisfied. This means that $\tilde{N}$ is not central in $\tilde{H}$. If char $\mathbf{F} \neq 2$ we also assume that $\tilde{H}$ has been chosen to contain the subgroup Z_4 of order 4 of the center of $GL_m(\mathbf{F})$. By 3.3 $\tilde{\lambda}_{|\tilde{N}}$ is irreducible and so $\tilde{N}$ is not abelian.

Let E_1 be a minimal noncentral normal subgroup of $\tilde{H}$ contained in $\tilde{N}$. Clearly, E_1 is a p-group for some prime p. Set $E = E_1$ or E_1Z_4 according to whether $p \neq 2$ or $p = 2$. The assertion 3.3 and the minimality of E_1 imply that E satisfies the hypotheses of Lemma 2.6. Thus, one of the following occurs:

$p \neq 2$ and $E = E(f)$ for a nondegenerate alternating form f in a vector space $(\mathbf{F}_p)^{2n}$;

$p = 2$ and $E = E(q)$ for a nondegenerate quadratic form q of defect 1 in a vector space $(\mathbf{F}_2)^{2n+1}$.

Set $\tau = \tilde{\lambda}_{|E}$ and let Y be the centralizer of E in N. Since N is nilpotent, N/Y is a p-group. By 3.3 the representation τ is irreducible. Therefore Y is central in $GL_m(\mathbf{F})$, hence is the center of N.

Let A, I, A_τ be defined as in 2.2 and 2.5. Clearly $\tilde{\lambda}(\tilde{H}) \subseteq A_\tau$. Therefore $\lambda(H)$ is contained in the projective image of $\tilde{\lambda}(\tilde{H})$, which we will identify with A. Furthermore, $\lambda(H)$ contains the projective image of $\tilde{\lambda}(EY)$ which is nothing else but $EY/Y = I$. Thus $\lambda(H)$ is the inverse image in A of a subgroup of A/I.

This yields a faithful representation $\mu : \tilde{H}/EY \to A/I \cong \mathrm{Sp}_{2n}(p)$. The inverse image in E_1 of any subgroup of $I = EY/Y$ which is invariant under $\lambda(H)$ is normal in $\tilde{H}$. Thus it follows from 3.3 and the minimality of E_1 that such a subgroup must be central in E_1. Hence $\mu(\tilde{H}/EY)$ acts irreducibly on I. Since it acts faithfully, $\tilde{H}/EY$ cannot have a proper normal p-subgroup. Consequently, $\tilde{N} = EY$ and μ is an irreducible representation of G in $\mathrm{Sp}_{2n}(p)$.

If $p \neq 2$, the extension

$$\langle 1 \rangle \to I \to \lambda(H) \to \mu(G) \to \langle 1 \rangle$$

splits (cf. 2.3), contrary to the fact that (H, γ, λ) is minimal with respect to G and $\mathbf{F}$.

Thus $p = 2$. Therefore char $F \neq 2$ since $GL_m(\mathbf{F})$ contains an irreducible 2-group $\bar{\lambda}(E)$. One cannot have $n = 2$, otherwise $\mu \circ \gamma$ would map H onto a nontrivial subgroup of $\mathrm{Sp}_4(2)' = \mathscr{A}_6$, which has a projective representation of degree 3 (cf. [**1**]), contradicting the minimality of (H, γ, λ). Similarly, $n \neq 3$ because $\mathrm{Sp}_6(2)$ has a projective representation of degree 7 (cf. [**1**]). Thus $n \geqq 4$. To finish the proof of (II$'$) it now suffices to remember that E has only two inequivalent faithful irreducible representations and they are contragredient to each other (cf. 2.4).

3.5. In order to prove (I), let now

$$(*)' \quad \langle 1 \rangle \to (\mathbf{Z}/2\mathbf{Z})^{2n'} \to A' \xrightarrow{\alpha'} \mathrm{Sp}_{2n'}(2) \to \langle 1 \rangle,$$

with $n' \geqq 4$, be an exact sequence, A'' a subgroup of A' such that $\alpha'(A'') = \mathrm{Sp}_{2n'}(2)$ and minimal with that property and $\rho' : A'' \to PGL_{m'}(\mathbf{F})$ a nontrivial projective representation of smallest possible degree of A''. Suppose that $m' \leqq 2^{n'}$. Since the Schur multiplier of $\mathrm{Sp}_{2n'}(2)$ is trivial, $\mathrm{Sp}_{2n'}(2)$ has no projective $\mathbf{F}$-representation of degree $\leqq 2^{n'}$ (cf. [**4**]). Therefore, assertion (II$'$) applied to $G = \mathrm{Sp}_{2n'}(2)$, $H = A''$ and $\lambda = \rho'$ implies the existence of an integer n such that $m' = 2^n$ and a commutative diagram

$$\begin{array}{ccc} A'' & \xrightarrow{\alpha'} & \mathrm{Sp}_{2n'}(2) \\ \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \mu} \\ A_n & \xrightarrow{\alpha_n} & \mathrm{Sp}_{2n}(2) \end{array}$$

where μ is irreducible, $\nu(A'') = \alpha_n^{-1}(\mu(\mathrm{Sp}_{2n'}(2)))$ and $\rho' = \rho_n \circ \nu$ or $\rho' = \rho_n^* \circ \nu$. We have $2^n = m' \leqq 2^{n'}$, hence $n \leqq n'$. Since μ is not trivial it follows that $n = n'$ and that μ is an isomorphism. Furthermore, A' and A_n have the same order, whereas $\nu(A'') = \alpha_n^{-1}(\mathrm{Sp}_{2n}(2)) = A_n$; therefore ν also is an isomorphism and $A'' = A'$. This establishes the uniqueness of $(*)_n$ and $\{\rho_n, \rho_n^*\}$ satisfying the conditions of (I) (if $(*)_n'$, $\{\rho_n', \rho_n'^*\}$ is any other such system apply the above to $(*)' = (*)_n'$ and $\rho' = \rho_n'|_{A''})$, as well as the minimality of (A_n, α_n, ρ_n) (take $(*)' = (*)_n$ and $\rho' = \rho_{n|A''})$. The proof is complete.

4. The known simple groups.

4.1. PROPOSITION. *If G is a known simple group*† *for which conclusion* (ii) *of the theorem holds (for a suitable choice of H, γ) then G is a group of Lie type in characteristic* 2.

Let G be a finite nonabelian simple group and let c (respectively $2s'$) be the smallest degree of a faithful projective representation of G over $\mathbf{C}$ (respectively over $\mathbf{F}_2$), c' the smallest index of a proper subgroup of G and $2s$ the smallest even integer such that $\mathrm{Sp}_{2s}(2)$ possesses a subgroup isomorphic to G. Thus $c' > c$ and $s' \leqq s$. If conclusion (ii) of the theorem holds one has

(1) $s \geqq 4$ and $c \geqq 2^s$,

and, a fortiori,

(2) $c' > 2^{s'}$.

We shall examine successively the various types of known simple groups which are not of Lie type in characteristic 2.

4.2. *Alternating groups.* Suppose that $G = \mathscr{A}_r$ and that conclusion (ii) of the theorem holds. Thus $s \geqq 4$. Denoting by N_{odd} the largest odd divisor of the integer N, we have

$$(r!)_{\mathrm{odd}} = |\mathscr{A}_r|_{\mathrm{odd}} \leqq |\mathrm{Sp}_{2s}(2)|_{\mathrm{odd}} = \prod_{i=1}^{s} (2^i - 1)(2^i + 1) < ((2^s + 1)!)_{\mathrm{odd}}.$$

Therefore $r \leqq 2^s$ in contradiction to (1), since $r = c' > c$.

4.3. *Groups of Lie type in odd characteristic.*

4.3.1. Let G be a simple group of Lie type over $\mathbf{F}_q$ and d the dimension of the corresponding simple algebraic group. If G is a Suzuki or Ree group of type ${}^2B_2$, ${}^2G_2$ or ${}^2F_4$ "over $\mathbf{F}_q$" (with q an odd power of 2 or 3), we set $d = 5$, 7 or 26 respectively.

LEMMA. $|G| < q^d$.

Suppose first that G is not of type ${}^3D_4$. Writing the standard formula for the order of G (see e.g. [**6**]) as follows

$$|G| = \frac{1}{e} q^N \prod_{i=1}^{l} (q^{n_i} + \epsilon_i)$$

with e a positive integer, $\epsilon_i = \pm 1$, $N + \sum n_i = d$ and $n_1 \leqq n_2 \leqq \ldots \leqq n_l$, one checks right away that $\epsilon_1 = -1$ and that $\epsilon_i = +1$ implies $\epsilon_{i-1} = -1$.

†Known to us at the time this is written: alternating groups, groups of Lie type and the 26 sporadic groups listed in 4.4 (some of which are not yet known to exist).

Then our assertion follows from the fact that if $a \leqq b$, one has

$$(q^a - 1)(q^b + 1) < q^{a+b}.$$

If G is of type ${}^3D_4$, one uses the inequality $(q^2 - 1)(q^8 + q^4 + 1) < q^{10}$.

4.3.2. The above lemma implies the following inequality:

(3) $\quad c' < q^{d/2}$.

Indeed, it is known that G has a subgroup whose index is smaller than the square root of $|G|$. The reader who is not willing to accept this fact (for which we cannot suggest a reference) may check the above inequality case by case, using parabolic subgroups of G.

4.3.3. From now on we will assume that q is odd and that conclusion (ii) of the theorem holds for G and a suitable choice of H, γ. We suppose first that G is not of one of the following types: PSL_n with $n \leqq 4$, PSU_n, $PSO_7(3)$, $P\mathrm{Sp}_{2m}$, G_2, ${}^2G_2$. Using the list of [**4**, p. 419], one easily checks, case by case, that $2s' > q^{\sqrt{d}-1}$. In view of (2) and (3) we must have

$$q^{d/2} > 2^{q^{\sqrt{d}-1}/2},$$

that is,

$$d \,.\, \log_2 q > q^{\sqrt{d}-1}.$$

Since $q \geqq 3$ it follows that $\log_2 q < 0{,}53.q$. This implies that

$$0{,}53.d > 3^{\sqrt{d}-2}.$$

Therefore $d < 16$ in contradiction to the assumption made on G.

4.3.3. Except for $PSU_4(3)$, $G_2(3)$ and some groups of type $P\mathrm{Sp}_{2m}$, the groups left aside in 4.3.3 can also be eliminated by means of (2), but one has to use better bounds for c' and s'. The relations to be checked are:

for $PSL_n(q)$: $2^{(q^{n-1}-1)/2} > \dfrac{q^n - 1}{q - 1}$ $\quad$ ($n \geqq 3$; note that $PSL_2 = P\mathrm{Sp}_2$);

for $PSU_{2m}(q)$: $2^{(q^{2m-1})(q+1)/2} > \dfrac{(q^{2m} - 1)(q^{2m-1} + 1)}{q^2 - 1}$

($m \geqq 2$; $(m, q) \neq (2, 3)$)

$PSU_{2m+1}(q)$: $2^{q(q^{2m-1})(q+1)/2} > \dfrac{(q^{2m+1} + 1)(q^{2m} - 1)}{q^2 - 1}$ $\quad$ ($m \geqq 2$);

for $PSU_3(q)$: $2^{(q-1)/2} > q^3 + 1$ $\quad$ ($q \neq 3$; note that $PSU_3(3)$ is isomorphic to a group of Lie type in characteristic 2);

for $PSO_7(3)'$: $2^{27/2} > \dfrac{3^6 - 1}{3 - 1}$;

for $G_2(q)$: $2^{q(q^2-1)/2} > \dfrac{q^6 - 1}{q - 1}$ $\quad$ ($q \neq 3$);

for ${}^2G_2(q)$: $2^{q(q-1)/2} > q^3 + 1$ $\quad$ ($q = 3^{2r+1}$, $r > 1$; note that ${}^2G_3(3)'$ is isomorphic to a group of Lie type in characteristic 2).

4.3.5. If $c = 2s'$, a relation satisfied by "most" groups of Lie type in odd characteristics, the inequalities (1), which imply

$$c \geqq 2^{c/2} \quad \text{and} \quad c \geqq 16$$

are clearly incompatible. This takes care of the remaining groups:

for $G_2(3)$, $c = 2s' = 14$ (for the inequality $2s' \geqq 14$, cf. [**14**]; relatively easy computations show that $c = 14$ but no written reference is known to us);

for $PSU_4(3)$, $c = 2s' = 6$ (cf. [**5**])

for $P\mathrm{Sp}_{2m}(q)$, $c = 2s' = (q^m - 1)/2$ (for the inequality $2s' \geqq (q^m - 1)/2$, cf. [**4**]; if $q = p^l$, one has $P\mathrm{Sp}_{2m}(q) \subset P\mathrm{Sp}_{2ml}(p)$ and the inequality $c \leqq (q^n - 1)/2$ is obtained by decomposing the representation of degree $p^{ml} = q^m$ of $P\mathrm{Sp}_{2m}(q)$ deduced from 2.5, 2.3).

4.4. *Sporadic groups.*

4.4.1. LEMMA. *Let p be a prime dividing the order of the simple group G and let n be the smallest integer such that $p|2^{2n} - 1$. Then one has $s \geqq n$.*

Indeed, $|G|$, and hence p, must divide

$$|\mathrm{Sp}_{2s}(2)| = 2^{s^2} \cdot \prod_{t=1}^{s} (2^{2t} - 1).$$

For the applications it is useful to observe that if $p = 2p' + 1$, where p' is an odd prime, then $n = p'$.

4.4.2. For all the known sporadic simple groups G, except Held's group HHM, there is a prime p dividing $|G|$ such that, defining n as in 4.4.1, one has $c < 2^n$, hence $c < 2^s$: one can take

$p = 7$ for HaJ $(= J_2)$;

$p = 11$ for the Mathieu groups, the Conway groups, HiS, Mc, Suz and Fi_{22};

$p = 19$ for J_1, HJM $(= J_3)$, O'Nan's group, Harada's group and Thompson's group;

$p = 23$ for Fi_{23} and Fi_{24}';

$p = 29$ for J_4 and Rudvalis' group;

$p = 47$ for the monster and its baby;

$p = 67$ for LyS.

(In all these cases, $n = (p - 1)/2$). As for HHM, it has a complex representation of degree 51 and since its order is divisible by 7^3 it is not contained in $\mathrm{Sp}_{10}(2)$.

5. Appendix. The non-splitting of the sequence (*) for $p = 2$ and dim $V \geqq 5$.

5.1. Let V be a vector space over $\mathbf{F}_2$, $q : V \to \mathbf{F}_2$ a quadratic form, f the associated alternating form, E the group $E(q)$ of 2.1, $\pi : E \to V$ the canonical projection, A the group of all automorphisms of F centralizing the center $\pi^{-1}(V^\perp)$ of E and $\alpha : A \to O(q)$ the canonical homomorphism. For $x \in q^{-1}(1)$, we denote by $r(x)$ the reflection $y \to y + f(x, y)x$ associated to x. In particular, if $x \in V^\perp$, $r(x)$ is the identity.

5.2. Lemma. *Let $a, b \in V$ be such that $q(a) = q(b) = 1, f(a, b) = 0$, $a \notin V^\perp$ and $a + b \notin V^\perp$, and let $\varphi \in \alpha^{-1}(r(a))$ and $\psi \in \alpha^{-1}(r(b))$. Suppose that $\varphi^2 = (\varphi\psi)^2 = 1$. Then φ inverts the elements of $\pi^{-1}(a)$ and ψ centralizes them.*

One cannot have $a^\perp \supsetneqq b^\perp$ (because $a \notin V^\perp$) nor $a^\perp = b^\perp$ (because $a + b \notin V^\perp$); therefore $b^\perp$ is not contained in $a^\perp$. Let $x \in V$ be orthogonal to b and not to a, and let $x' \in \pi^{-1}(x)$. Set $\tau = \varphi$ or $\varphi\psi$, hence $\alpha(\tau) = r(a)$ or $r(a)r(b)$. We have $\pi(\tau(x')) = \alpha(\tau)(x) = x + a$, therefore $\tau(x' . \tau(x')) = a$, i.e. $x' . \tau(x') \in \pi^{-1}(a)$. On the other hand, $x'^2 = \tau(x')^2 = \tau(x')^{-2}$, we also have $\tau(x' . \tau(x')) = \tau(x') . x' = \tau(x')^{-1} . x'^{-1} = (x' . \tau(x'))^{-1}$. Thus both φ and $\varphi\psi$ invert the elements of $\pi^{-1}(a)$, and so ψ centralizes them.

5.3. Proposition. *Let Y be a two-dimensional subspace of V such that $q(Y) = \{0\}$ and $Y \cap V^\perp = \{0\}$. Let X be a three-dimensional subspace such that $Y \subset X \subset Y^\perp$ and $q(X) \neq \{0\}$. Let $T \subset O(q)$ be the elementary abelian 2-group generated by the reflections $r(a)$ with $a \in X - Y$ (note that $q(X - Y) = \{1\}$). Then the homomorphism $\alpha^{-1}(T) \to T$ admits no section.*

Suppose the contrary. Let $\sigma : T \to A$ be a section, i.e. a homomorphism such that $\alpha \circ \sigma = \mathrm{id}$, and set $X - Y = \{a_1, a_2, a_3, a_4\}$, with $a_1 \notin V^\perp$. The automorphism $\sigma(r(a_1))$ centralizes $\pi^{-1}(a_i)$ for $i = 2, 3, 4$: this follows from the definition of A if $a_i \in V^\perp$, and from the above lemma, setting $\varphi = \sigma(t(a_i))$ and $\psi = \sigma(t(a_1))$, otherwise. (Note that $a_1 + a_i \notin V^\perp$ because $a_1 + a_i \in Y$). Since $\pi^{-1}(a_1) \subset \langle \pi^{-1}(a_i) | i = 2, 3, 4\rangle$, we see that $\sigma(r(a_1))$ centralizes $\pi^{-1}(a_1)$, in contradiction with the same lemma in which one takes now $\varphi = \sigma(r(a_1))$ and $\psi = \sigma(r(a_2))$.

5.4. Corollary. *If* dim $V \geqq 5$ *and q is nondegenerate the sequence* (*) *of* 2.2 *does not split.*

Because then, there exist subspaces Y and X satisfying the hypotheses of 5.3.

References

1. W. Feit, *The current situation in the theory of finite simple groups*, Actes du Congrés International des Mathématiciens, Nice (1970), Vol. 1, 55–93.
2. R. L. Griess, Jr., *Automorphisms of extra special groups and nonvanishing degree* 2 *cohomology*, Pacific J. Math. *48* (1973), 403–422.

3. B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenshaften, Band 134 (Springer-Verlag, Berlin–New York, 1967).

4. V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra *32* (1974), 418–443.

5. J. H. Lindsey, II, *Finite linear groups of degree six*, Can. J. Math. *23* (1971), 771–790.

6. J. Tits, *Groupes simples et géométries associées*, Proc. Int. Cong. Math. Stockholm, Stockholm (1962), 197–221.

Institut des Hautes Etudes Scientifiques,
Bures sur Yvette, France