JOURNAL OF ALGEBRA 83, 477–483 (1983)

Remarks on Reduction (mod p) of Finite Complex Linear Groups

GEOFFREY R. ROBINSON

Department of Mathematics, University of Chicago, 5734 University Avenue, Chicago, Illinois 60637

Communicated by Walter Feit

Received by August 31, 1982

Let G be a finite irreducible subgroup of $GL(n, \mathbb{C})$ and p be a prime divisor of $|G|$. Then it is well known that (replacing G with a suitable conjugate within $GL(n, \mathbb{C})$, if necessary) we may suppose that G is a subgroup of $GL(n, R)$, where R is the localization of the ring of algebraic integers of a cyclotomic number field at a prime ideal π containing p. This enables us to define a homomorphism from G to $GL(n, F)$, where F is the finite field of characteristic p obtained by factoring out the unique maximal ideal of R. The kernel of this homomorphism is a p-group, and the above process is known as reduction (mod p) of G.

In this paper, we will consider what can be said if a p-element x of G, acts with minimum polynomial of relatively small degree in some reduction (mod p) of G when G is quasi-primitive.

The methods of this paper are inspired by the article of Feit [3]. Indeed, Feit has obtained some of the results of our Theorem A already in unpublished work. The proof of Theorem A presented here evolved from an idea of Professor George Glauberman, and owes much to that idea. Glauberman also obtained part of our Theorem A (also in unpublished work) independently of Feit. Part of the proof of Theorem A is a special case of Theorem A 1.4 of [5].

Before we state our main theorem, we need to fix some notation. G is a finite group, p is a prime divisor of $|G|$, R is a principal ideal domain which is a local subring of $\mathbb{C}$ such that $F = R/\pi$ is a finite field of characteristic p (where π is the unique maximal ideal of R). V is a faithful RG-module such that $V \otimes_R \mathbb{C}$ is irreducible and quasi-primitive, and $\bar{V}$ is the canonical FG-module obtained from V. Also, x is an element of order p in G and k is the positive integer such that $\bar{V}(1-x)^k = 0$, $\bar{V}(1-x)^{k-1} \neq 0$. Finally, P is a Sylow p-subgroup of G containing x, and Q is the subgroup of P generated by the G-conjugates of x contained in P.

0021-8693/83 $3.00

THEOREM A. (i) *If* $k \leqslant (p-1)/2$, *then* $(V \otimes_R \mathbb{C})_{N_G(Q)}$ *is irreducible.*

(ii) *If* $1 < k \leqslant (p+1)/4$, *then* $(V \otimes_R \mathbb{C})_{N_G(Q)}$ *is irreducible and quasi-primitive, Q is extra-special of exponent p, and order* p^{2m+1} *for some integer m such that* p^m *divides* $\dim_{\mathbb{C}}(V \otimes_R \mathbb{C})$, *and each irreducible constituent of* $(V \otimes_R \mathbb{C})_M$ *has degree* p^m, *where M is the normal subgroup of G generated by the conjugates of x. Also,* $Z(Q) \leqslant Z(G)$, *so that* $O_p(G) \neq 1_G$.

(iii) *If* $k \leqslant (p+5)/8$, *then* $x \in O_p(G)$.

Proof. Let $H = N_G(Q)$. In Case (i), we let $W = V \otimes V^*$, in Case (ii) we let $W = V \otimes V^* \otimes V \otimes V^*$, and in Case (iii) we let $W = V \otimes V^* \otimes V \otimes V^* \otimes V \otimes V^* \otimes V \otimes V^*$. We first prove that $C_w(H) = C_w(G)$ in each case. Let $\bar{W} = W/\pi W$. Matters have been arranged so that $\bar{W}(1-x)^{p-2} = 0$ (for in general, if $V_1(1-x)^m = 0$ and $V_2(1-x)^n = 0$, then $V_1 \otimes V_2^*(1-x)^{m+n-1} = 0$).

We define a linear mapping $\phi: C_W(H) \to C_W(G)$ by $v\phi = \sum_{t \in T} vt$ for each $v \in C_w(H)$, where $G = \bigcup_{t \in T} Ht$ and $[G:H] = |T|$. It is easy to check that the definition of ϕ is independent of the transversal T chosen. Suppose then that $C_W(H) \neq C_W(G)$. Then there is some $w \neq 0$ in $C_W(H)$ with $w\phi = 0$. By taking a suitable multiple of w, we may suppose that $\bar{w} \neq 0$.

Now let $\{g_i: 1 \leqslant i \leqslant s\}$ be a complete set of (H, Q) double coset representatives in G with $g_1 = 1_G$. We compute the contribution made to $\overline{w\phi}$ by the double coset Hg_iQ for $i > 1$.

We first remark that if a p-group A is generated by a set S and A acts transitively on a set Ω, then there is an element $s \in S$ which fixes no element of Ω if $|\Omega| > 1$ (for let B be the stabilizer of a point in Ω. Then there is a maximal subgroup D of A which contains all conjugates of B. Some element $s \in S$ must lie outside D, and this s fixes no point of Ω). Now for $i > 1$, $Hg_iQ > Hg_i$, for otherwise $g_iQg_i^{-1} \leqslant H$, so $hg_iQg_i^{-1}h^{-1} \leqslant P$ for some $h \in H$, and then $hg_iQg_i^{-1}h^{-1} = Q$ by definition of Q, so that $hg_i \in N_G(Q) = H$, and $g_i \in H$, a contradiction.

Since Q is generated by conjugates of x, by the above remarks we may write $Hg_iQ = \bigcup_{k=1}^{r} \bigcup_{j=0}^{p-1} Hy_k z^j$, where z is a conjugate of x and r is an integer which depends on i. Then the contribution to $\overline{w\phi}$ from Hg_iQ is $\sum_{k=1}^{r} \overline{wy_k}(1-z)^{p-1} = 0$, because z is conjugate to x and $\bar{W}(1-x)^{p-1} = 0$.

Hence only the coset H makes any contribution to $\overline{w\phi}$, so that $\overline{w\phi} = \bar{w}$. This contradicts the fact that $w\phi = 0$ but $\bar{w} \neq 0$. Thus we must have $C_W(H) = C_W(G)$.

Case i. In this case, we have $C_{V \otimes V^*}(H) = C_{V \otimes V^*}(G)$, and it readily follows that $(V \otimes_R \mathbb{C})_H$ is irreducible.

Case ii. In this case, $C_{V \otimes V^* \otimes V \otimes V^*}(H) = C_{V \otimes V^* \otimes V \otimes V^*}(G)$. Let χ be the character of G afforded by V. By (i), $\chi|_H$ is irreducible. In this case, we see that $(\chi\bar{\chi}, \chi\bar{\chi})_G = (\chi\bar{\chi}|_H, \chi\bar{\chi}|_H)_H$. To prove (ii) we are required to prove that whenever $N \lhd H$, $\chi|_N$ is a multiple of an irreducible character.

Let N be a normal subgroup of H. We note that each irreducible constituent of $\chi\bar{\chi}$ remains irreducible on restriction to H. Thus whenever ϕ is an irreducible constituent of $\chi\bar{\chi}$ with $(\phi|_N, 1_N) \neq 0$ we see that $N \leqslant \ker \phi$ (since $\phi|_H$ is irreducible and $N \lhd H$). It follows that $C_{V \otimes V^*}(N)$ is G-invariant.

Let $K = C_G(C_{V \otimes V^*}(N))$. Then $N \leqslant K$, so that $C_{V \otimes V^*}(K) \leqslant C_{V \otimes V^*}(N) \leqslant C_{V \otimes V^*}(K)$. Since $V \otimes_R \mathbb{C}$ is quasi-primitive, $\chi|_K = a\psi$ for some integer a, some irreducible character ψ of K (because $K \lhd G$). Since $C_{V \otimes V^*}(N) = C_{V \otimes V^*}(K)$, $\psi|_N$ remains irreducible. Thus $\chi|_N = a\psi|_N$, so is a multiple of an irreducible character, as required. In particular, every Abelian normal subgroup of H is contained in $Z(G)$, so is cyclic. Since $Z(Q) \lhd H$, $O_p(G) \neq 1_G$.

Since x acts nontrivially on $\bar{V}$, $x \notin Z(Q)$, so that Q is nonabelian. We outline the argument of Rigby [7] to show that Q is extra special of exponent p (p must be odd in this case, of course). Every characteristic Abelian subgroup of Q is normal in H, so is contained in $Z(G)$, so is cyclic. Since Q is generated by elements of order p, and is nonabelian, Q is quickly seen to be extra special and of exponent p. Thus $|Q| = p^{2m+1}$ for some integer m, and each irreducible constituent of $\chi|_Q$ has degree p^m, so that p^m divides $\dim_{\mathbb{C}}(V \otimes_R \mathbb{C})$.

Let $X = C_G(C_{V \otimes V^*}(Q))$. Then $X \lhd G$, and all irreducible constituents of $\chi|_X$ are equal, and of degree p^m, by an earlier argument. Let M be the normal subgroup of G generated by the conjugates of x. Then $Q \leqslant M \leqslant X$, so each irreducible constituent of $\chi|_M$ has degree p^m also (and all are equal). The proof of part (ii) is complete.

Case iii. Suppose that $x \notin O_p(G)$. Then by part (ii), Q is extra special of exponent p. In this case, we also have $C_w(H) = C_w(G)$, where $W = V \otimes V^* \otimes V \otimes V^* \otimes V \otimes V^* \otimes V \otimes V^*$.

An argument similar to that used in part (ii) shows that whenever $N \lhd H$, $C_{V \otimes V^* \otimes V \otimes V^*}(N)$ is G-invariant, and that there is a normal subgroup K of G having the same fixed points on $V \otimes V^* \otimes V \otimes V^*$ as N does, so that each irreducible constituent of $\chi\bar{\chi}|_K$ remains irreducible on restriction to N.

Let R be the normal subgroup of G which corresponds to Q in the above way. By part (ii), $\chi\bar{\chi}|_Q$ is a multiple of the regular character of Q/Q', so that all irreducible constituents of $\chi\bar{\chi}|_Q$ are linear. Hence all irreducible constituents of $\chi\bar{\chi}|_R$ are linear also, so that $R' \leqslant \ker(\chi\bar{\chi}) = Z(G)$. Thus R is nilpotent. Since $Q \leqslant R$, and $x \in Q$, x lies in $O_p(G)$, contrary to hypothesis. The proof of part (iii) is complete.

COROLLARY 1. *Let G, x be as in Theorem* A. *Then if $x \notin Z(G)$, x has at least $(p+3)/4$ distinct eigenvalues on $V \otimes_R \mathbb{C}$.*

Proof. Suppose that x has $(p+1)/4$ or fewer eigenvalues, but that $x \notin Z(G)$. Then x has a minimum polynomial of degree $\leqslant (p+1)/4$ on $\bar{V}$. If x acts nontrivially on $\bar{V}$ we see from part (ii) that Q is extra special and that $\chi|_Q = a\psi$ for some faithful irreducible character ψ of Q. Since $x \in Q \backslash Z(Q)$ (for $Z(Q) \leqslant Z(G)$ and $x \notin Z(G)$) we have $\chi(x) = 0$, a contradiction, as x has $(p+1)/4$ or fewer eigenvalues. Thus $x \in O_p(G)$, so $O_p(G) \nleqslant Z(G)$.

Since V is quasi-primitive, $O_p(G)$ is the central product of an extra special group of exponent p and a cyclic group contained in $Z(G)$, so again we have $\chi(x) = 0$, a contradiction. Thus if $x \notin Z(G)$, x must have at least $(p+3)/4$ distinct eigenvalues.

COROLLARY 2. *Suppose that $O_p(G) = 1_G$ and that $P^{(n)} \neq 1_G$. Then $\chi|_P$ has at least $(p-1)/4$ distinct irreducible constituents of degree p^n or more. In particular,* $\dim_C(V \otimes_R \mathbb{C}) \geqslant p^n((p-1)/4)$.

Proof. An easy induction argument shows that $P^{(n)} \leqslant \ker \psi$ whenever ψ is an irreducible constituent of $\chi|_p$ of degree p^{n-1} or less. Since $P^{(n)} \neq 1_G$, there is an element x of order p in $P^{(n)} \cap Z(P)$. Since x has at least $(p+3)/4$ distinct eigenvalues, there must be at least $(p-1)/4$ inequivalent irreducible constituents of $\chi|_p$ of degree p^n or more.

Remark. We can conclude from the above argument that $\dim_{\mathbb{C}}(V \otimes_R \mathbb{C}) > p^n((p-1)/4)$ and if $p \equiv 3 \pmod 4$ that $\dim_{\mathbb{C}}(V \otimes_R \mathbb{C}) > p^n((p+1)/4)$.

COROLLARY 3. *Let $\varepsilon = 1$ if $p \equiv -1 \pmod 4$ and $\varepsilon = -1$ if $p \equiv 1 \pmod 4$. Then if $\dim_{\mathbb{C}}(V \otimes_R \mathbb{C}) \leqslant p((p+\varepsilon)/4)$, and $O_p(G) = 1$, G has elementary Abelian Sylow p-subgroups.*

Proof. By Corollary 2, P is Abelian. Choose $y \in P$ of order p^2, if possible, and let $y^p = x$. Then $\bar{V}(1-y)^{p(p+\varepsilon)/4} = 0$, so $\bar{V}(1-x)^{(p+\varepsilon)/4} = 0$, which contradicts part (ii) of Theorem A, as $O_p(G) = 1_G$. Thus P is elementary Abelian.

COROLLARY 4. *Let r be the maximum dimension of any indecomposable summand of $\bar{V}_p$. Then if $O_p(G) = 1_G$, P has nilpotence class less than $4r/(p-\varepsilon)$, where $\varepsilon = \pm 1$ and $p \equiv \varepsilon \pmod 4$.*

Proof. We define the subspaces $[\bar{V}, P; i]$ of $\bar{V}$ by: $[\bar{V}, P; 1]$ is the subspace of $\bar{V}$ generated by $\{\bar{v}(1-x) : \bar{v} \in \bar{V}, x \in P\}$ and for $i > 1$, $[\bar{V}, P; i+1] = [[\bar{V}, P; i], P]$. We recall that $L_i(P)$ denotes the ith term of the lower central series of P.

The three subgroups lemma and an easy induction argument yields $[\bar{V}, L_i(P)] \leqslant [\bar{V}, P; i]$ for $i \geqslant 1$. Another induction argument yields $[\bar{V}, L_i(P); k] \leqslant [\bar{V}, P; ik]$ for $i, k \geqslant 1$. Since r is the maximum dimension of any indecomposable summand of $\bar{V}_p$, we have $[\bar{V}, P, r] = 0$.

Suppose that $O_p(G) = 1_G$, and let j be any integer greater than or equal to $4r/(p-\varepsilon)$. Then $[\bar{V}, L_j(P); (p-\varepsilon)/4] = 0$, so in particular, each element of $L_j(P)$ has minimum polynomial of degree $(p-\varepsilon)/4$ or less on $\bar{V}$. By Theorem A(ii), $L_j(P) = 1_G$. Thus class $(P) < 4r/(p-\varepsilon)$.

COROLLARY 5. *Suppose that $p \geqslant 7$ and that x is an element of order p in P such that $\bar{V}(1-x)^2 = 0$. Then $x \in O_p(G)$.*

Proof. Suppose that $x \notin O_p(G)$. By Theorem A(iii), $p = 7$. Also, we may choose a conjugate y of x such that $\langle x, y \rangle$ is not a p-group (in fact by Theorem 3.8.1 of [6], $\langle x, y \rangle$ involves $SL(2, p)$). Let $K = \langle x, y \rangle$. Then K' contains an element of order 6, say z in a component of $K/O_p(K)$.

Let $\bar{V}_1 = \bar{V} \otimes_F F_1$, where F_1 is an algebraically closed field containing F. The argument of Theorem 3.8.1 of [6] shows that the composition factors of $\bar{V}_{1K'}$ are all 1 or 2 dimensional. We show that they are all 2 dimensional. There is at least one 2-dimensional composition factor. If there are any trivial composition factors z has eigenvalues $1, \alpha, \beta$, where α and β are primitive 6th roots of unity. Since z is p-regular, the eigenvalues of z on $V \otimes_R \mathbb{C}$ are $1, -\omega, -\bar{\omega}$, where $\omega = \exp(2\pi i/3)$. This contradicts the well-known result of Blichfeldt (see [2] for a proof of this result, which is valid for quasi-primitive representations, though only stated for primitive ones). Thus all composition factors of $\bar{V}_{1K}$ are 2 dimensional.

Let $t = z^3$. Then t has only the eigenvalue -1 on $\bar{V}_1$. Since t is p-regular, $t \in Z(G)$. Let M be the normal subgroup of G generated by the conjugates of x. Then $t \in M'$, since $t \in \langle x, y \rangle'$. By Theorem A(ii), each irreducible component of V_M has dimension p^m for some integer m. This contradicts the fact that $t \in M'$, since t has only the eigenvalue -1 on V and p is odd.

Thus $x \in O_p(G)$, and the proof of Corollary 5 is complete.

An Application to a Theorem of Feit and Thompson

It is not difficult to prove, using Corollary 1 that if a finite group G has a faithful complex representation of degree $(p+1)/4$ or less, where p is a prime, then G has an Abelian normal Sylow p-subgroup. However, in [4] Feit and Thompson proved that if G has a faithful complex representation of degree less than $(p-1)/2$, then G has an Abelian normal Sylow p-subgroup. They used a complicated coherence argument to reduce to the case when p divided $|G|$ to the first power only. The next lemma gives an alternative reduction to this case and shows in fact that we only need to consider the case when the representation of G has degree $(p-1)/3$. Results of Brauer [1] can be used to eliminate this case.

It is easy to see that it is sufficient to consider the case when G has a faithful irreducible complex representation of degree $<(p-1)/2$, and the Sylow p-subgroups of G are trivial intersection sets.

PROPOSITION 6. *Let G be a finite group, p be a prime, V be a faithful irreducible $\mathbb{C}G$-module with $\dim_{\mathbb{C}}(V) \leqslant (p-1)/2$. Let P be a Sylow p-subgroup of G such that $P \cap P^g = 1_G$ for all $g \in G \backslash N_G(P)$. Then $V_{N_G(P)}$ is irreducible and one of the following occurs*:

(i) $P \lhd G$.

(ii) $|P| = p$ *and* $\dim_{\mathbb{C}}(V) = (p-1)/3$.

(iii) $|P| = p$ *and* $\dim_{\mathbb{C}}(V) = (p-1)/2$.

Proof. Suppose that (i) does not occur. Then $O_p(G) = 1_G$. We claim that V is primitive. Otherwise $V = W^G$, where W is a $\mathbb{C}H$-module of dimension at most $(p-1)/4$ and H is a subgroup of G. Let $K = \bigcap_{g \in G} H^g$. Then $p \nmid [G:K]$, since $[G:H] < p$. Furthermore, V_K is a direct sum of $\mathbb{C}K$-modules of dimension at most $(p-1)/4$, so that K has an Abelian normal Sylow p-subgroup by Theorem A(ii), contrary to the fact that $O_p(G) = 1_G$ and $P \ntriangleleft G$.

By Corollary 3, P is elementary Abelian. By Corollary 1, $\dim_{\mathbb{C}}(V) \geqslant (p+3)/4$. Suppose that $|P| > p$. We may suppose that V is a faithful RG-module, where R is the localization at some prime ideal containing p of some ring of algebraic integers in a cyclotomic number field. Let π be the unique prime ideal of R and let F be the residue field R/π.

Let $H = N_G(P)$, and let $W = V \otimes V^* \otimes V \otimes V^*$. If $C_W(H) = C_W(G)$, the arguments of Theorem A(ii) yield a contradiction. Let $\bar{V} = V/\pi V$. Then $[\bar{V}, P; (p-1)/2] = 0$. By Lemma A 2.3 of [5], $[\bar{W}, P; 2p-5] = 0$.

We define the mapping ϕ: $C_W(H) \to C_W(G)$ as we did in Theorem A. There must be some $w \in C_w(H)$ with $w\phi = 0$, $\bar{w} \neq 0$, as in Theorem A.

Let $\{g_i\colon 1 \leqslant i \leqslant r\}$ be a complete set of (H, P) double-coset representatives in G. Then

$$\bar{w}\phi = \bar{w} + \sum_{i=2}^{r} \bar{w}g_i \sum_{x \in P} x.$$

Since $\bar{w}\phi \neq \bar{w}$, there is some i such that $\bar{w}g_i \sum_{x \in P} x \neq 0$. Let P be generated by $\{x_j\colon 1 \leqslant j \leqslant n\}$, and by no proper subset. Then

$$\bar{w}g_i \sum_{x \in P} x = \bar{w}g_i \prod_{j=1}^{n} (1-x_j)^{p-1}.$$

Thus $[\bar{W}, P; n(p-1)] \neq 0$, a contradiction, as $[\bar{W}, P; 2p-5] = 0$ and $n > 1$. Thus $|P| = p$.

By Theorem A(i), $V_{N_G(P)}$ is irreducible. By Corollary 1, V_p is multiplicity free, and $\dim_{\mathbb{C}}(V) \geqslant (p+3)/4$. Since V_p is multiplicity free and $V_{N_G(P)}$ is irreducible, we see that $\dim_{\mathbb{C}}(V)$ is a divisor of $p-1$. Hence we see that $\dim_{\mathbb{C}}(V) = (p-1)/3$ or $(p-1)/2$, as claimed.

References

1. R. Brauer, On groups whose order contains a prime number to the first power. I, II, *Amer. J. Math.* **64** (1942), 401–420; 421–440.
2. L. Dornhoff, "Group Representation Theory, Part A," Dekker, New York, 1972.
3. W. Feit, Some properties of the Green correspondence, *in* "Theory of Finite Groups" (R. Brauer and C. H. Sah, Eds.), pp. 139–148, Benjamin, New York, 1969.
4. W. Feit and J. G. Thompson, On groups which have a faithful representation of degree less than $(p-1)/2$, *Pacific J. Math.* **4** (1961), 1257–1262.
5. G. Glauberman, Global and local properties in finite groups, *in* "Finite Simple Groups" (M. B. Powell and G. Higman, Eds.), pp. 1–63, Academic Press, London, 1971.
6. D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.
7. J. F. Rigby, Primitive linear groups containing a normal nilpotent subgroup larger than the centre, *J. London Math. Soc.* **35** (1960), 389–400.

481/83/2-13