JOURNAL OF ALGEBRA 90, 446–460 (1984)

Some Applications of the First Cohomology Group

M. ASCHBACHER*

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

AND

R. GURALNICK

Department of Mathematics, University of Southern California, Los Angeles, California 90007

Communicated by David M. Goldschmidt

Received April 21, 1982

1. INTRODUCTION

Let G be a finite group and V a $GF(p)$ G-module (where $GF(p)$ is the field of p elements). We denote the first cohomology group of G on V by $H^1(G, V)$. The nontriviality of $H^1(G, V)$ is the obstruction to many results in finite groups. Often this is circumvented in the literature by imposing extra hypotheses on G such as $O_{p'}(G) \neq 1$ (cf. [2, Lemma 3.3] and [17, Theorem 1]). In this article, we show that $H^1(G, V)$ is not too big in many cases. We then apply this to certain problems in finite groups. The bound on $H^1(G, V)$ we obtain is the following:

THEOREM A. *If V is an irreducible faithful G-module over $GF(p)$, then* $|H^1(G, V)| < |V|$.

The finiteness condition on G is essential. For example, if G is free on d generators and V is a G-module over a field F, then it is easy to see that $\dim H^1(G, V) \geqslant (d-1) \dim V$ (with equality if $C_V(G) = 0$). The theorem is proved by reducing to the case where G is simple. The bound $|H^1(G, V)| \leqslant |V|$ is obtained from the following result.

THEOREM B. *Every finite simple group can be generated by two elements.*

* Supported in part by an NSF grant.

0021-8693/84 $3.00

Steinberg [16] proved this for G a Chevalley group. We verify it for the sporadic groups.

Although the bound in Theorem A is not sharp, it does have several applications. The first of these establishes a result proved by Thomas [17] in a special case. Suppose V is a minimal normal solvable subgroup of H. If H/V can be generated by d elements, when can H be generated by d elements? This problem is considered in Thomas [17] and also arose in [2, Sect. 4]. Clearly if V is contained in the Frattini subgroup of H, the answer is affirmative. So we may assume that V has a complement G in H. Then the answer depends on $|H^1(G, V)|$.

THEOREM C. *Let G be a finite group and V an irreducible G-module over $GF(p)$. Let H be the semidirect product VG. Let K be the normal subgroup of G minimal subject to $K \leqslant C = C_G(V)$, $C/K \simeq V^r$ (as a G-module) for some r, and to C/K possessing a complement in G/K. Set $q = |\mathrm{Hom}_G(V, V)|$ and suppose G can be generated by d elements.*

(1) *If V is the trivial module, then H can be generated by d elements if and only if $r < d$.*

(2) *If V is nontrivial, then H can be generated by d elements if and only if $hq^r < |V|^{d-1}$, where $h = |H^1(G/C, V)|$.*

Note Theorem C does not depend on the classification of simple groups. Thomas [17] proved that either $r > 0$ or H can be generated by $d > 1$ elements under the additional hypothesis that $O_{p'}(G/C) \neq 1$. As we shall see (2.7)(b), this implies $h = 1$. Hence his result is a special case of Theorem C. It follows from Theorem A that the assumption on $O_{p'}(G/C)$ is not necessary.

COROLLARY 1. *If V is faithful (or more generally $r = 0$) and $d > 1$, then H can be generated by d elements.*

COROLLARY 2. *Let $W = V^t$ and let $L = WG$. Then H can be generated by d elements if and only if $hq^{r+t-1} < |V|^{d-1}$ for V nontrivial. In particular, this holds if $t \leqslant s(d-2) + 1 - r$, where $|V| = q^s$.*

The first cohomology group is also useful in determining conjugacy classes of maximal subgroups. Indeed by [3], the problem of counting classes of maximal subgroups reduces to calculating $|H^1(G, V)|$ for V a faithful irreducible G-module and solving the problem for $L \leqslant G \leqslant \mathrm{Aut}\, L$ for L simple. Our goal is to relate the number of classes of maximal subgroups to the irreducible characters of G. We conjecture that the number of irreducible characters bounds the number of classes of maximal subgroups. This is true for G solvable (see [2, Corollary 3]).

By restricting attention to maximal subgroups M with $\ker_M G = \bigcap M^g = K$ and characters χ with $\ker \chi = K$, it suffices to consider M with $\ker_M G = 1$ and faithful characters. If G is solvable, there is at most one such class of maximal subgroups (cf. [2]). This is not true in general (e.g., G simple).

So set $\mathscr{C} = \{M^G \mid M$ maximal in G and $\ker_M G = 1\}$ and $\mathscr{F} = \{\chi \mid \chi$ is an irreducible faithful character$\}$. Thus to prove our conjecture, it suffices to show $|\mathscr{C}| \leqslant |\mathscr{F}|$. We obtain a weaker bound under the hypotheses $O_\infty G \neq 1$.

THEOREM D. *Let G be a finite group. Suppose $\mathscr{C}$ is nonempty and $O_\infty G \neq 1$. Then*

(a) *$F^*(G) = V$ is a minimal normal elementary abelian p-group for some prime p.*

(b) *$\mathscr{C}$ is the set of conjugacy classes of complements to V in G.*

(c) *If $M^G \in \mathscr{C}$, then 1_M^G is the sum of r distinct irreducible characters, χ_i, $1 \leqslant i \leqslant r$, where r is the number of orbits $(v_i G, 1 \leqslant i \leqslant r)$ of G on the dual space of V. Moreover $\deg \chi_i = |v_i G|$, and r is also the number of orbits of G on V.*

(d) $|\mathscr{C}| = |H^1(G/V, V)| < |V|$.

(e) $|\mathscr{C}| \leqslant \sum \deg \chi$, $\chi \in \mathscr{F}$.

If one could obtain the bound in (e) when $O_\infty G = 1$, it would follow that the number of classes of maximal subgroups of G is bounded by $\sum \deg \chi < |G|$, where the sum is over all nontrivial irreducible characters of G. The problem reduces to the case where $L \leqslant G \leqslant \operatorname{Aut} L$ with L simple.

Another application of Theorem A is to minimal relation modules. Let G be a finite group that can be generated by d elements (and no fewer). So $G \simeq F/R$, where F is free on d generators. Then $M = R/R'$ is a G-module and is called a minimal relation module for G. Of course, this module may depend on the particular presentation of G chosen. However, using Theorem A and [19, Proposition 2], one obtains:

THEOREM (Kimmerle and Williams [13, Theorem 3.1, Corollary 1]). *Let G be a finite nonabelian simple group.*

(i) *Minimal relation modules are unique.*

(ii) *If M is a minimal relation module, then M is a generator (i.e., $\mathbb{Z}G$ is a summand of some number of copies of M).*

See [13] for a more detailed account and extensions of the results.

The article is organized as follows. Section 2 contains some results on cohomology. We give an essentially self-contained group theoretic account of the necessary facts. In Section 3, generation of simple groups is discussed and Theorem B is proved. Theorems A and C are proved in Section 4. The final section is devoted to Theorem D.

2. Cohomology

Let G be a finite group. Throughout this section p will denote a fixed prime and V will be a finitely generated G-module over the field of p elements. Set $U(G, V) = \{\sigma \in \operatorname{Aut} VG \mid \sigma v = v \quad \forall\, v \in V \text{ and } \sigma(Vg) = Vg \quad \forall\, g \in G\}$. It is straightforward to verify the first result.

(2.1) *$U(G, V)$ is an elementary abelian p-group.*

Then $H^1(G, V)$ can be interpreted as $U(G, V)/\operatorname{Aut}_V(VG)$, where $\operatorname{Aut}_V VG$ are the automorphisms of VG induced by conjugation by some element of V. See [11, Chap. 3.5] for a discussion of this.

(2.2) *$U(G, V)$ acts regularly on the set of complements to V in VG.*

Proof. Let H be a complement to V in VG. Evidently, the map $\sigma: G \to H$ defined by $\sigma g = vg$ where $vg \in Vg \cap H$ is an isomorphism. Now σ extends to an element of $U = U(G, V)$ by defining $\sigma v = v$ for all $v \in V$. Thus U acts transitively on the set of complements of V. Since $N_U(G) = C_U(G) = 1$, the result follows.

An immediate consequence of (2.2) is:

(2.3) *$|H^1(G, V)|$ is the number of conjugacy classes of complements of V in VG.*

(2.4) (a) *If $G = \langle X_1, \ldots, X_t \rangle$, then $|U(G, V)| \leqslant \prod |U(X_i, V)|$.*

(b) *If $G = \langle g \rangle$, then $|U(G, V)| = |\{v \in V \mid (vg)^m = 1\}|$, where m is the order of g.*

(c) *If G can be generated by d elements, then $|U(G, V)| \leqslant |V|^d$.*

Proof. If $\sigma \in U(G, V)$ and $X = X_i < G$, then $\sigma_i = \sigma|_{VX} \in U(X, V)$. Since $\sigma = 1$ if and only if $\sigma_i = 1$ for each i, (a) holds. Since $\langle vg \rangle$ is a complement for V in $\langle V, g \rangle$ if and only if vg has order m, (b) follows. Now (c) follows from (a) and (b).

The next result indicates the connection between H^1 and generators for VG.

(2.5) *If V is irreducible and $G = \langle x_1, \ldots, x_d \rangle$, then VG can be generated by d elements if and only if $|U(G, V)| < |V|^d$. In particular, if V is also* *nontrivial, then* VG *can be generated by* d *elements if and only if* $|H^1(G, V)| < |V|^{d-1}$.

Proof. If $\alpha = (v_1, ..., v_d) \in V^d$, set $G_\alpha = \langle v_1 x_1, ..., v_d x_d \rangle$. Note that either G_α is a complement to V or $G_\alpha = VG$. Moreover, if $G_\alpha = G_\beta$ either $\alpha = \beta$ or $G_\alpha = VG$. Furthermore any complement is of the form G_α for some α. Thus $VG = G_\alpha$ for some α if and only if $|U(G, V)| < |V|^d$. Since $\{x_1, ..., x_d\}$ was an arbitrary generating set for G, the first result follows. The last statement follows, since if V is nontrivial and irreducible, $|\mathrm{Aut}_V G| = |V|$.

The next result gives a bound for $H^1(G, V)$ in terms of a composition series for V.

(2.6) *If* W *is a* G*-submodule of* V, *then* $|H^1(G, V)| \leqslant |H^1(G, W)|\, |H^1(G, V/W)|$ *with equality if* W *is a summand of* V.

Proof. Define $\phi: U(G, V) \to U(G, V/W)$ by $\phi(u)\, x = u(x)\, W$. Then ϕ is a homomorphism. Evidently $\ker \phi = \{u \in U(G, V) \mid [u, G] \leqslant W\}$ and can be identified with a subgroup of $U(G, W)$. Thus

$$|U(G, V)| \leqslant |U(G, W)|\, |U(G, V/W)|,$$

and clearly equality holds if W is a summand of V. The result follows since $|C_V(G)| \leqslant |C_W(G)|\, |C_{V/W}(G)|$ and so

$$|\mathrm{Aut}_V VG| \geqslant |\mathrm{Aut}_W WG|\, |\mathrm{Aut}_{V/W}(V/W)\, G|.$$

Clearly equality holds in case W is a summand.

We wish to reduce the general problem to the case where G is simple. Recall that a group L is quasisimple if $L = L'$ and $L/Z(L)$ is simple. A component of G is a subnormal quasisimple subgroup. Then $E(G)$ is the subgroup of G generated by its components. The generalized Fitting subgroup of G is $F^*(G) = E(G)\, F(G)$.

(2.7) *Let* V *be a* G*-module.*

(a) *If* $N \lhd G$ *and* $C_V(N) = 0$, *then* $|H^1(G, V)| \leqslant |H^1(N, V)|$.

(b) *If* $V = [O_{p'}(G), V]$, *then* $H^1(G, V) = 0$.

(c) *If* V *is a faithful irreducible* G*-module with* $H^1(G, V) \neq 0$, *then*

(i) $F^*(G) = E(G) = E$ *is a direct product of simple groups, and*

(ii) $V = \oplus V_i$, *where* V_i *is an irreducible nontrivial* E*-module, and* $|H^1(G, V)| \leqslant \prod |H^1(L_i, V_i)|$, *where* L_i *is a component of* G *with* $[L_i, V_i] \neq 0$.

Proof. Let Ω and Γ be the set of complements of V in VG and VN, respectively. If $H \in \Omega$, then $R = H \cap VN \in \Gamma$. Moreover, $R \lhd H$, and

$N_V(R) = C_V(N) = 0$. Thus $H = N_{VG}(R)$, and the map $H \to H \cap VN$ is an injection from Ω to Γ. Thus (a) holds.

If $V = [O_{p'}(G), V]$, then by (a) and th Schur–Zassenhaus Theorem, $|H^1(G, V)| \leqslant |H^1(O_{p'}(G), V)| = 1$.

Now assume V is a faithful irreducible module and $H^1(G, V) \neq 0$. By (b), $O_{p'}(G) = 1$. Since V is faithful, $O_p(G) = 1$. Thus (i) holds. By Clifford's Theorem, $V = \oplus V_i$ is a semisimple $E-$module. Furthermore as $C_V(E)$ is G-invariant, $C_V(E) = 0$. Thus for each V_i, there is a component L_i with $[L_i, V_i] \neq 0$. Another application of Clifford's Theorem implies L_i has no fixed points on V_i. Since $L_i \lhd E$, it follows by (a) that $|H^1(E, V_i)| \leqslant |H^1(L_i, V_i)|$. Then by (a) and (2.6), $|H^1(G, V)| \leqslant |H^1(E, V)| \leqslant \prod |H^1(L_i, V_i)|$.

We remark that if one is more careful, it is possible to show that in (c), in fact $|H^1(G, V)| \leqslant |H^1(L_i, V_i)|$.

(2.8) *If $P \leqslant X \leqslant G$ with $P \in \mathrm{Syl}_p(G)$, then $|H^1(G, V)| \leqslant |H^1(X, V)|$.*

Proof. Let $\phi\colon U(G, V) \to U(X, V)$ be the restriction mapping, and set $A = \mathrm{Aut}_V(VG)$ and $U = (G, V)$. Note ϕ is a homomorphism and $\ker \phi = \{u \in U \mid C_G(u) \geqslant X\}$. Let $u \in \ker \phi$. Then $W = \langle V, u \rangle$ is G-invariant, $[G, W] \leqslant V$, and $W = V \oplus \langle u \rangle$ as a P-module. Thus W splits as a G-module, and so $uv \in C_U(G)$ for some $v \in V$. Thus $u \in C_A(X)$. Hence $|U(G, V)| \leqslant |U(X, V)|\,|C_A(X)|$. The result now follows since

$$|H^1(G, V) = \frac{|U(G, V)|}{|A|} \leqslant \frac{|U(X, V)|\,|C_A(X)|}{|A|}$$

$$= \frac{|U(X, V)|}{|\mathrm{Aut}_V(VX)|} = |H^1(X, V)|.$$

(2.9) *Suppose $G = \langle X, T \rangle$ is a nonabelian simple group and either*

(a) *X is cyclic or a p'-group and $|T| = 2$, or*

(b) *X is a p'-group, $T = \langle t \rangle$, $t^2 \in N_G(X)$, and $G = \langle X, X^t \rangle$.*

Then $|H^1(G, V)| < |V|$.

Proof. By (2.6), we can assume V is irreducible (and nontrivial). Let $U = U(G, V)$. Then U is a G-module, and we can identify V with $\mathrm{Aut}_V(VG)$. So $[G, U] \leqslant V$. In either case, $|U| \leqslant |U(X, V)|\,|U(T, V)|$ by (2.4)(a). By (2.4)(b) or (2.7)(b), $|U(X, V)| \leqslant |V|$. If $|T| = 2$, then $|U(T, V)| = |\{v \in V \mid v^t = -v\}|$ by (2.4)(b). Since $t \notin Z(G)$, it follows that $|U(T, V)| < |V|$ and so $|H^1(G, V)| < |V|$. So assume (b) holds. Then $0 = C_U(G) = C_U(X) \cap C_U(X^t)$. Since X is a p'-group, $U = VC_U(X) = VC_U(X^t)$. So if $|U| = |V|^2$, then $V \cap C_U(X) = 0$ and $|V| = |C_U(X)|$. Hence as $t^2 \in N_G(X)$, $[t^2, C_U(X)] \leqslant$

$C_U(X) \cap V = 0$. Similarly, $[t^2, C_U(X^t)] = 0$ and so t^2 centralizes $C_U(X)\, C_U(X^t) = U$. Thus $t^2 = 1$ and (a) applies.

(2.10) *Let V be an irreducible G-module, $q = |\mathrm{Hom}_G(V, V)|$, and $\Delta = \Delta(G, V)$ the set of G-invariant subgroups I of $C = C_G(V)$ such that C/I is G-isomorphic to V and C/I has a complement in G/I. Then if $K = \bigcap I$, $I \in \Delta$,*

(a) *C/K is G-isomorphic to a direct sum of n copies of V and C/K has complement in G/K,*

(b) $|H^1(G, V)| = q^n \, |H^1(G/C, V)|$.

Proof. To prove (a) we take $K = 1$. Let X be a minimal normal subgroup of G contained in C. As $K = 1$, there exists $I \in \Delta$ with $X \nleqslant I$. Hence $C = XI$ and $X \cap I = 1$. So $C = X \times I$. Also there is $G_I \leqslant G$ with $G = CG_I$ and $G_I \cap C = I$. Furthermore $X \simeq XI/I = C/I$ is G-isomorphic to V.

We are done if $I = 1$, so choose $J \in \Delta - \{I\}$. Then $C = IJ$ and $I/J \cap I \simeq C/J$ is G isomorphic to V. Let $Y = G_I \cap G_J$. Then $Y \cap I = G_J \cap I = J \cap I$. So $[I: Y \cap I] = |V|$ and $|YI| = |Y|\,|V|$. However, $G = G_I C = G_J C = G_I G_J$, so $[G_I : Y] \leqslant [G: G_J] = |V|$. So $G_I = VI$ and $Y \cap I = I \cap J$, and $J \cap I \in \Delta(G_I, V)$. Hence

$$1 = \bigcap_{J \in \Delta} J = \bigcap_{I \neq J \in \Delta} J \cap I \geqslant \bigcap_{L \in \Delta(G_I,\, V)} L.$$

So by induction on the order of G, I is the direct sum of G modules isomorphic to V and I has a complement in G_I. Thus $C = X \times I$ has a complement in G and is isomorphic to n copies of V.

It remains to prove (b). Suppose H is a complement to V in VG. Then as above $I = C \cap C_H(V) \in \Delta$ (or $C = C_H(V)$). In any case, $K \leqslant H$, and so we can assume $K = 1$. So by (a), $G = CL$ with $C \simeq V^n$. Let ϕ: $U(G, V) \to U(L, V) \simeq U(G/C, V)$ be the restriction map. Since any $u \in (L, V)$ can be extended to an element $u \in U(G, V)$ (e.g., take u to centralize C), ϕ is onto. Now $\ker \phi = C_U(L)$, $U = U(G, V)$. If $u \in \ker \phi$, u is determined by its action on C, and so $\ker \phi \simeq \mathrm{Hom}_L(C, V)$. Thus $|U(G, V)| = q^n \, |U(L, V)|$, and so $|H^1(G, V)| = q^n \, |H^1(G/C, V)|$.

3. Generation of Simple Groups

If $X < G$, let $\eta(X)$ be the set of maximal subgroups of G which contain X. Let $\mathscr{I}(G)$ be the set of involutions in G. The first result is presumably well known.

(3.1) *If $G = A_n$, $n > 4$, then $G = \langle t, x \rangle$ for some $t \in \mathscr{I}(G)$ and $x \in G$.*

Proof. If $n=5$, take $X \in \mathrm{Syl}_5(G)$ and $t \in \mathscr{I}(G) - N_G(X)$. Then $G = \langle X, t\rangle$. So assume $n > 5$. Set $t = (12)(n-1, n)$ and $x = (1, 2 \cdots n-1)$ if n is even and $t = (1, n)(2, n-1)$ and $x = (1, 2 \cdots n-2)$ if n is odd. Then $H = \langle x, t\rangle$ is obviously transitive. We claim H is doubly transitive. This is clear for n even. If n is odd, either this holds or $\{n-1, n\}$ is a set of imprimitivity for H. The latter is impossible since n is odd. Also $[t, x]$ is a five cycle. The result now follows for $n > 7$ by [18, Theorem 13.9] and by inspection for $n = 6$ or 7.

Let $\mathrm{Chev}(p)$ denote the simple Chevalley groups defined over a field of characteristic p.

(3.2) *Let $G \in \mathrm{Chev}(p)$, $U \in \mathrm{Syl}_p(G)$, and $z \in Z(U)$. If $\langle z, z^g\rangle$ is not a p-group, then $G = \langle U, z^g\rangle$. In particular, $G = \langle U, U^g\rangle$ for some $g \in G$ with $g^2 \in N_G(U)$.*

Proof. Assume $L = \langle z, z^g\rangle$ is not a p-group. If $G \neq H = \langle U, z^g\rangle$, then by a result of Tits [15, 1.6], $H \leqslant X$ a parabolic subgroup. Hence $Z(U) \leqslant C_X(O_p(X)) \leqslant O_p(X)$. Thus $L \leqslant \langle O_p(X), z^g\rangle$ a p-group. Hence $G = H$. Now choose $1 \neq z \in Z(U) \cap Z(U_r)$ for some root subgroup U_r. If G is a group over the field of two elements, then the Weyl group W is actually embedded in G and we may identify g with w_r. Otherwise let H be a torus in $N_G(U)$. Since $W \simeq N(H)/H$, we may take $g \in N(H)$ so g maps onto w_r. Then $g^2 \in N_G(U)$, $U_r^g = U_{-r}$, and $\langle z, z^g\rangle$ is not a p-group. Thus $G = \langle U, z^g\rangle = \langle U, U^g\rangle$.

(3.3) *If $G \in \mathrm{Chev}(p)$ of Lie rank 1, then $G = \langle X, t\rangle$ for some cyclic subgroup X and some $t \in \mathscr{I}(G)$.*

Proof. First suppose $G = L_2(q)$ with q odd. If $q \leqslant 9$, this follows by inspection. For $q > 9$, choose X cyclic of order $(q+1)/2$. Then $\eta(X) = \{N_G(X)\}$. So $G = \langle X, t\rangle$ for $t \in \mathscr{I}(G) - N_G(X)$. If $G = L_2(q)$ or $Sz(q)$ with $q > 2$ even, let X be cyclic of order $q-1$. Then $\eta(X) = \{N_G(X), B, B^s\}$ where B is a Borel subgroup of G and s inverts X. Then $G = \langle X, t\rangle$ for any $t \in \mathscr{I}(G)$ with $t \notin B \cup B^s \cup N_G(X)$ (e.g., take $t \in C_G(s) - X$). Note ${}^2G_2(3)' \simeq L_2(8)$. So finally assume $G = U_3(q)$ $(q \neq 2)$ or ${}^2G_2(q)$ $(q \neq 3)$. Then there exists X cyclic of order $(q^3+1)/(q+1)$ or $(q+1) + (3q)^{1/2}$ with $\eta(X) = \{N_G(X)\}$. So $G = \langle X, t\rangle$ for any $t \notin N_G(X)$.

We now consider the sporadic groups. Let $\mathrm{Spor}_1 = \{M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, Mc, J_2, Co_3, He, HS, Co_2, Co_1, J_1, J_3, J_4, Ly, Ru, F_2, F_1\}$. The properties of the sporadic groups we need are given in [10, Sect. 5].

(3.4) *Let $G \in \mathrm{Spor}_1$ and p be as given in Table I. If $T \in \mathrm{Syl}_p(G)$, then $\eta(T)$ is as listed in the table.*

TABLE I

G	p	$\eta(T)$
M_{11}	11	$L_2(11)$
M_{12}	11	$L_2(11), M_{11}, M_{11}$
M_{22}	11	$L_2(11)$
M_{23}	23	$N_G(T)$
M_{24}	23	$M_{23}, L_2(23)$
Mc	11	M_{11}, M_{22}, M_{22}
J_2	7	$PGL_2(7)$
Co_3	23	M_{23}
He	17	$Sp_4(4)\, Z_2$
HS	11	M_{11}, M_{11}, M_{22}
J_1	19	$N_G(T)$
J_3	19	$L_2(19), L_2(19)$
J_4	37	$N_G(T)$
Co_2	23	M_{23} and possibly $L_2(23)$
Ly	67	$N_G(T)$
Ru	29	$N_G(T)$ or at most 3 $L_2(29)$
F_2	47	$N_G(T)$
F_1	59	$N_G(T)$ or $L_2(59)$
Co_1	23	$Co_2, Co_3, 2^{11}M_{24}$

Proof. This follows for the first 10 groups in the table by [5–8, 14]. Suppose G is one of the remaining groups and $p \neq r$ is a prime divisor of G. If R is an elementary abelian r-subgroup of G, then by considering $|GL(R)|$, T cannot act faithfully on R unless $G = Co_1$ and $|R| = 2^{11}$. Since $r \nmid |C_G(T)|$, T is not contained in $N_G(R)$ except in the one case mentioned above. In that case, there is a unique conjugacy class of elementary abelian subgroups of order 2^{11}. Thus $T \leqslant N_G(R)$ for a unique R of order 2^{11} (for $N_G(R) \simeq RM_{24}$ and $N_G(R) \geqslant N_G(T)$). So it suffices to consider $H \in \eta(T)$ with $H = N_G(K)$ and $K \simeq L \times \cdots \times L$, L nonabelian simple. Also, since $H = KN_H(Q)$ where $Q \in \mathrm{Syl}_2(K)$ and $p \nmid |N_H(Q)|$, $p \mid |K|$. Since $p^2 \nmid |G|$, this implies $K \simeq L$ is simple. Since $|K| \mid |G|$, the possibilities for K are limited.

In particular, if $G \simeq J_1$, J_4, F_2, or Ly, then the only possibility for K is $L_2(p)$. However, by considering $N_G(T)$, this is not possible. Thus for these groups $\eta(T) = \{N_G(T)\}$. If $G = Co_2$, then $K \simeq L_2(23)$ or M_{23}. In either case $N_K(T) = N_G(T)$. Choose $X \leqslant N_G(T)$ with $|X| = 11$. Since $N_G(T)$ is maximal in K, $K = \langle N_G(T), N_K(X)\rangle$. If $K \simeq L_2(23)$, then $|N_K(X)| = 22$ while if $K \simeq M_{23}$, $|N_K(X)| = 55$. Since $N_G(X)/X \simeq Z_{10}$, the isomorphism type of K determines $N_K(X)$ and hence K. Hence $|\eta(T)| \leqslant 2$ (note M_{23} actually occurs [6]).

If $G = J_3$, the result follows from [9].

If $G = Ru$ and K exists, then $K \simeq L_2(29)$. Then $N_G(T) = N_K(T)$. Let $S \in \mathrm{Syl}_7(N_G(T))$. Hence $N_K(T)$ is dihedral of order 28. Since $N_G(T)$ contains three such subgroups and $K = \langle N_G(T), N_K(S)\rangle$, it follows that $|\eta(T)| \leqslant 3$. Furthermore, since $N_G(T) = N_K(T)$, $K = H$ if it exists.

Similarly, if $G = F_1$ then $H = K \simeq L_2(59)$ and $N_G(T) = N_K(T)$. Let $S \in \mathrm{Syl}_{29}(N_G(T))$. Then $N_K(S)$ is dihedral of order of 58. There is a unique subgroup of that type in $N_G(S)$. Since $K = \langle N_G(T), N_K(S)\rangle$, it follows that $|\eta(T)| = 1$.

Finally, consider $G = Co_1$. If K exists, then $K \simeq L_2(23)$, Co_2, Co_3, M_{23}, or M_{24}. Furthermore, since $N_K(T) = N_G(T)$ has order $23 \cdot 11$, $H = K = N_G(K)$. First note that if $T < K \simeq M_{23}$, then $K = \langle N_G(T), N_K(E)\rangle$ for $E \in \mathrm{Syl}_{11}(N_G(T))$. Since $|N_K(E)| = 55$ and $N_G(E)$ contains a unique subgroup of order 55, there is a unique $T < K \simeq M_{23}$. Now G acts on a 24-dimensional lattice (see [6]). This gives rise to a 24-dimensional complex representation ϕ of G. We claim each K fixes a nonzero point. If $K \simeq M_{23}$, this follows by the uniqueness of K (since there is a subgroup of Co_1 of type M_{23} centralizing a two-dimensional space). Let L denote the subgroup of G with $T \leqslant L \simeq M_{23}$. If $K \simeq M_{24}$, then $L < K$, and so $(\phi_K, 1_L^K) = (\phi_L, 1_L) = 2$. Thus ϕ_K is the permutation character of M_{24}. Similarly, if $K \simeq L_2(23)$, $(\phi_K, 1_N^K) = 2$ where $N = N_G(T)$, and so $\phi_K = 1_N^K$. Finally, if $K \simeq Co_2$ or Co_3, then either ϕ_K is irreducible or it has a trivial constituent (since $\phi_L = 1_L + 1_L + \chi$ where χ is irreducible and $L < K$). However, from their character tables, Co_2 and Co_3 have no irreducible representations of degree 24. Now by reducing mod 2, we obtain a representation of G over $GF(2)$. There are three orbits of nonzero points in this representation with stabilizers RM_{24}, Co_2, and Co_3, where R is an elementary abelian group of order 2^{11}. Thus there are three conjugacy classes of maximal subgroups M containing T. Since $N_M(T) = N_G(T)$, there is a unique $M > T$ in each class. Hence $|\eta(T)| = 3$.

(3.5) *If* $G \in \mathrm{Spor}_1$, $T \in \mathrm{Syl}_p(G)$, *and* $x \in G^{\#} = G - \{1\}$, *then* $G = \langle T^g, x\rangle$ *for some* $g \in G$.

Proof. Note $x^G = \{x^g \mid g \in G\} \not\subseteq \bigcup X$, $X \in \eta(T)$. This is clear for those G with $|\eta(T)| = 1$. Easy counting arguments yield that conclusion in the other cases. So there exists $h \in G$ with $G = \langle T, x^h\rangle = \langle T^g, x\rangle$ with $g = h^{-1}$.

See [4] for another proof of (3.5) for the Mathieu groups.

(3.6) *If* G *is a sporadic simple group, then* $G = \langle t, x\rangle$ *for some* $x \in \mathscr{I}(G)$ *and some* $t \in G$.

Proof. By (3.5), it suffices to consider $G \simeq M(22)$, $M(23)$, $M(24)'$, ON, Sz, F_3, *or* F_5.

First assume $G = F_5$ and let $T \in \mathrm{Syl}_{19}(G)$. Arguing as in (3.4), we see that if $K \in \eta(T)$, then either $K = N_G(T)$ or $K \simeq L_2(19)$. Thus if $z \in \mathscr{I}(K)$ z inverts an element of order 9. There is only one such class of involutions.

Hence $G = \langle T, t\rangle$ for $t \in \mathscr{I}(G) - z^G$. Similarly, if $G = M(24)'$ and $T \in \mathrm{Syl}_{29}(G)$, there is a unique class of involutions represented in any $K \in \eta(T)$. Here $K \simeq L_2(29)$ or $N_G(T)$.

If $G = F_3$, let $T \in \mathrm{Syl}_{19}(G)$. Then $N_G(T) = \langle T, g\rangle$ where g has order 18. Set $y = g^9$. Now $C_G(y) = QA_9$, where Q is an extraspecial group of order 2^9. So we can choose $x \in \mathscr{I}(C_G(y))$ so that xg^2 has order divisible by 7. Arguing as (3.4), we see that if $K \in \eta(T)$, then $7 \nmid |K|$ and $g^2 \in K$. Thus $G = \langle T, x\rangle$.

In the remaining cases choose primes p and q as follows: $(p, q) = (11, 13)$, $(11, 13)$, $(17, 23)$, and $(19, 31)$ for $G = Sz$, $M(22)$, $M(23)$, and ON, respectively. Arguing as in (3.4), we see that $\eta(S) \cap \eta(T)$ is empty for $S \in \mathrm{Syl}_p(G)$ and $T \in \mathrm{Syl}_q(G)$. Thus $G = \langle s, t\rangle = \langle st, t\rangle$, where $S = \langle s\rangle$ and $T = \langle t\rangle$. However, one can check the character tables of G to determine that

$$f(s, t, x) = \sum_{\chi \in \mathrm{Irr}\, G} \frac{\chi(s)\,\chi(t)\,\chi(x)}{\chi(1)} \neq 0$$

for $x \in \mathscr{I}(G)$. Since $f(s, t, x) \neq 0$ implies that the product of the conjugacy classes s^G and t^G contains x, we can choose s and t so that $x = st$. The result now follows.

The results of this section together with those of Steinberg [16] now yield Theorem B. (Actually, the one case $G = {}^2F_4(2)'$ is still open. However, arguing as above, it follows that for $T \in \mathrm{Syl}_{13}(G)$, $G = \langle T, x\rangle$ for x a 2-central involution.)

4. Theorems A and C

Suppose V is an irreducible faithful G-module over $GF(p)$. Our goal is to show $|H^1(G, V)| < |V|$. By (2.4), (2.7), and Theorem B, we have:

(4.1) $|H^1(G, V)| \leqslant |V|$.

By (2.6) and (2.7), it suffices to show $|H^1(G, V)| < |V|$ for G simple. So assume (G, V) is a minimal counterexample.

(4.2) $G \in \mathrm{Chev}(p)$ *with* $l = \mathrm{rank}\, G > 1$.

Proof. G is not an alternating group, sporadic group, or rank 1 group by (2.9), (3.1), (3.3), and (3.6). If $G \in \mathrm{Chev}(r)$, then $r = p$ by (2.9) and (3.2).

So assume $G \in \mathrm{Chev}(p)$ with Lie rank l. Set $F = \mathrm{Hom}_G(V, V)$ and $q_V = |F|$. Theorem A will follow from the next result.

(4.3) $|V| > |H^1(G, V)|$.

We sketch the proof. This is certainly true if $l = 1$. So assume $l > 1$. Choose a parabolic subgroup M of G as follows:

(i) If $G = L_n(q)$, M is the stabilizer of a projective point.

(ii) If $G = P\Omega_n^{\varepsilon}(q)$, $n \geqslant 6$, $G \not\simeq L_4(q)$, M is the stabilizer of a singular point in the corresponding orthogonal space.

(iii) If $G = Sp_6(2)$, $U_5(2)$, or $PSp_4(3)$, M is the stabilizer of a maximal totally isotropic subspace.

(iv) If $G = G_2(2)'$, then M is the normalizer of a 4-group.

(v) Otherwise $M = N_G(Z)$ for a long root subgroup Z of G.

Set $H = O^{p'}(M)$ and $Q = O_p(M)$. Then H/Q has Lie rank $l - 1$. Let Q_0 be the minimal M invariant subgroup of Q such that $\tilde{Q} = Q/Q_0$ is a semisimple M module. Then H/Q is faithful and irreducible on $\tilde{Q}$ unless $G = G_2(q)$, $q > 2$, in which case M/Q is faithful and irreducible on $\tilde{Q}$, or $G = F_4(q)$, q even, in which case $\tilde{Q} = \tilde{Q}_1 \oplus \tilde{Q}_2$, where M is faithful on $\tilde{Q}$ and $\tilde{Q}_1$ and $\tilde{Q}_2$ are distinct irreducibles. Moreover, either $H = O^p(H)$ and H/Q is quasisimple or $G = {}^2F_4(2)'$, $G_2(q)'$, $L_3(q)$, or $PSp_4(q)'$, $q \leqslant 3$. In any case, $H/O^p(H)$ is cyclic.

Let V_i, $1 \leqslant i \leqslant r$, be the composition factors of a chief series for V as an M-module. Since $[Q, V_i] = 0$, $r \geqslant 2$. Also $[H, V_i] \neq 0$ for some i since $[H, V] \neq 0$. If $[H, V_i] = 0$, then $h_i = |H^1(M, V_i)| \leqslant |V_i|$ by (2.10) and the fact that $H/O^p(H)$ is cyclic. If $[H, V_i] \neq 0$ and $V_i \simeq \tilde{Q}$ (or $\tilde{Q}_j$ if $G = F_4(q)$, q even), then it follows by (2.7), (2.10), and induction that $h_i = |H^1(M, V_i)| = |H^1(M/Q, V_i)| < |V_i|$. If $V_i \simeq \tilde{Q}$ (or $\tilde{Q}_j$), the same reasoning shows that $h_i = q\,|H^1(M/Q, V_i)|$ where $q = |\mathrm{End}_M(\tilde{Q})|$. Now $|H^1(M/Q, \tilde{Q})|$ for these cases are essentially all known (see [10]), and it follows that $h_i < |V_i|$ unless $G = L_3(q)$, q even. So excluding this last case, it follows from (2.6) and (2.8) that $|H^1(G, V)| \leqslant \prod h_i < |V|$.

So it remains to consider $G = L_3(q)$, q even. Then $G = \langle t, z \rangle$, for some $z \in \mathscr{I}(G)$ and $t \in G$ [1]. Thus (4.3) follows.

We remark that by being more careful, it is possible to show

(4.4) $|H^1(G, V)| < q_V^{-l}\,|V|$.

Indeed, by induction, it suffices to show this for $l \leqslant 3$ since either $r \geqslant 3$ or $r = 2$ and each V_i is nontrivial.

(4.5) *Theorem* C *holds.*

Proof. By (2.5), H can be generated by d elements if and only if $|H^1(G, V)| < |V|^e$ where $e = d$ or $d - 1$ depending on whether V is trivial or not. It follows from (2.10) that $|H^1(G, V) = hq^r$. Thus (2) is true. Now (1) follows by noticing if V is trivial, then $h=1$ and $q=p=|V|$. (Note that this only uses results in Section 2.)

(4.6) *Corollaries* 1 *and* 2 *are true.*

Proof. If V is faithful, then $r=0$ and by Theorem A, $h<|V|\leqslant|V|^{d-1}$. So Corollary 1 follows from Theorem C(2).

Let s be the smallest positive integer so that $R=UG$ cannot be generated by d elements with $U=V^s$. Set $S=V^{s-1}G$. Applying Theorem C(2) to S and $R=VS$, we see that $hq^{r+s-2}<|V|^{d-1}\leqslant hq^{r+s-1}$. Since L can be generated by d elements precisely when $t<s$, Corollary 2 follows.

5. Theorem D

Let G be a finite group. We wish to relate the number of conjugacy classes of maximal subgroups of G to the characters of G. Let $K \lhd G$. We restrict our attention to maximal subgroups N of G with $\ker_N G=K$ and to characters χ with $\ker\chi=K$. So by passing to G/K, we can assume $K=1$.

Now let M be a maximal subgroup of G with $\ker_M G=1$. If $O_\infty(G)\neq 1$, it follows from [2, Lemma 3.3] that:

(5.1) $V=F^*(G)$ *is a minimal normal elementary abelian p-group for some prime p.*

Set $\mathscr{C}=\{N^G \mid N \text{ is maximal and } \ker_N G=1\}$. So if $N^G\in\mathscr{C}$, $N\cap V=1$, and $G=VN$. Thus

(5.2) $\mathscr{C}=\{N^G \mid N$ *is a complement to* $V\}$.

We wish to describe the constituents of 1_M^G. Set $V^*=\mathrm{Hom}(V,\mathbb{C}-\{0\})$. Then V^* is a G-module via $\alpha^g(v)=\alpha(vg^{-1})$. Set $C=C_G(\alpha)=\{g\in G \mid \alpha^g=\alpha\}$. We can extend α to C by $\alpha(vg)=\alpha(v)$ for $g\in C\cap M$. Denote this by α_1.

(5.3) (a) $(\alpha_1,\alpha^C)=1$.
(b) $(\alpha^C,\alpha^C)=(\alpha^G,\alpha^G)=[C\colon V]$.
(c) $(\alpha^G,\beta^G)=0$ *if* $\alpha\neq\beta^g$.

Proof. By Frobenius reciprocity, $(\alpha_1,\alpha^C)=(\alpha_1|_V,\alpha)=1$ and (a) follows. Similarly, $(\alpha^C,\alpha^C)=(\alpha,\alpha^C|_V)=[C\colon V]$. Also $(\alpha^G,\beta^G)=(\alpha,\beta|_V)=\sum_{g\in G}(\alpha,\beta^g)/|V|=|\{g\in C \mid \alpha=\beta^g\}|/|V|$. Now (b) and (c) follow.

By (b), we see that if γ is an irreducible constituent of α^C, then γ^G is also irreducible. In particular, by (a), α_1^G is irreducible. Furthermore, by (c), if $\alpha\neq\beta^g$ for some g, then $\alpha_1^G\neq\beta_1^G$.

(5.4) $1_M^G = \sum \alpha_1^G$, *where the sum is over the orbits* αG *of* G *on* V^*, *and* $\deg(\alpha_1^G) = |\alpha G|$.

Proof. Note that since $V \leqslant C$, $G = MC$, and so C acts transitively on the cosets of M. Hence $1_M^G|_C = 1_{C\cap M}^G$. Another application of Frobenius reciprocity yields $(1_M^G, \alpha_1^G) = (1_{C\cap M}^C, \alpha_1) = (\alpha_1|_{C\cap M}, 1_{C\cap M}) = 1$. Since $\alpha_1^G \neq \beta_1^G$ if $\alpha G \neq \beta G$, the sum $\sum \alpha_1^G$ is certainly a part of 1_M^G. The result follows since $\sum \alpha_1^G(1) = [G: C] = |\alpha G|$, and so $\sum \alpha_1^G(1) = |V^*| = |V| = |G: M|$.

Note that since the representation of G on V^* is the inverse transpose representation of G on V, each element has the same number of fixed points on V and V^*. Thus G has the same number of orbits on V and V^*. To complete the proof of Theorem D, note that by Theorem A and (5.1) and (5.2), $|\mathscr{C}| = |H^1(G/V, V)| < |V|$. Hence $|\mathscr{C}| \leqslant \sum \deg \chi$, where the sum is over the nontrivial constituents of 1_M^G. Since $\ker \chi = \ker_M G = 1$ (cf. [2]), Theorem D follows.

Note added in proof. We have been informed that Mark Cartwright has independently completed the proof of Theorem B for the sporadic groups.

References

1. A. A. Albert and J. G. Thompson, Two element generation of the projective unimodular group, *Illinois Math. J.* **3** (1959), 421–439.
2. M. Aschbacher and R. Guralnick, Solvable generation of groups and Sylow subgroups of the lower central series, *J. Algebra* **77** (1982), 189–201.
3. M. Aschbacher and L. Scott, Maximal subgroups of finite groups, preprint.
4. J. Brenner, R. Guralnick, and J. Wiegold, Two generator groups, III, in press.
5. G. Butler, The maximal subgroups of the sporadic simple group of Held, *J. Algebra* **69** (1981), 67–81.
6. J. Conway, Three lectures on exceptional groups, *in* "Finite Simple Groups" (G. Higman and M. Powell, Eds.), Academic Press, London/New York, 1971.
7. L. Finkelstein, The maximal subgroups of Conway's group C_3 and McLaughlin's group, *J. Algebra* **25** (1973), 58–89.
8. L. Finkelstein and A. Rudvalis, Maximal subgroups of the Hall Janko Wales group, *J. Algebra* **24** (1973), 486–493.
9. L. Finkelstein and A. Rudvalis, The maximal subgroups of Janko's simple group of order 50,232,960, *J. Algebra* **30** (1974), 122–143.
10. D. Gorenstein and R. Lyons, The local structure of finite groups of characteristic 2 type, *Mem. Amer. Math. Soc.* **276** (1983).
11. K. Gruenberg, "Cohomologic Topics in Group Theory," Lecture Notes in Mathematics No. 143, Springer-Verlag, Berlin/New York 1970.
12. W. Jones and B. Parshall, On the 1-cohomology of finite groups of Lie type, *in* "Proceedings, Conference on Finite Groups" (W. R. Scott and F. Gross, Eds.), Academic Press, New York, 1976.

13. W. KIMMERLE AND J. S. WILLIAMS, On minimal relation modules and 1-cohomology of finite groups, *Archiv der Math.* **42** (1984), 214–223.
14. S. S. MAGLIVERAS, The subgroup structure of the Higman–Sims simple group, *Bull. Amer. Math. Soc.* **77** (1971), 535–539.
15. G. SEITZ, Flag transitive subgroups of Chevalley groups, *Ann. of Math.* **97** (1973), 27–56.
16. R. STEINBERG, Generators for simple groups, *Canad. J. Math.* **14** (1962), 277–283.
17. R. THOMAS, On the number of generators for certain finite groups, *J. Algebra* **71** (1981), 576–582.
18. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.
19. J. S. WILLIAMS, Trace ideals of relation modules of finite groups, *Math. Z.* **163** (1978), 261–274.