Can. J. Math., Vol. XL1, No. 1, 1989, pp. 68-82

COPRIME GROUP ACTIONS FIXING ALL NONLINEAR IRREDUCIBLE CHARACTERS

I. M. ISAACS

1. Introduction. The main result of this paper is the following:

THEOREM A. *Let H and N be finite groups with coprime orders and suppose that H acts nontrivially on N via automorphisms. Assume that H fixes every nonlinear irreducible character of N. Then the derived subgroup of N is nilpotent and so N is solvable of nilpotent length* $\leqq 2$.

Why might one be interested in a situation like this? There has been considerable interest in the question of what one can deduce about a group G from a knowledge of the set

$$\mathrm{cd}(G) = \{\chi(1) | \chi \in \mathrm{Irr}(G)\}$$

of irreducible character degrees of G. Recently, attention has been focused on the prime divisors of the elements of $\mathrm{cd}(G)$. For instance, in [**9**], O. Manz and R. Staszewski consider π-separable groups (for some set π of primes) with the property that every element of $\mathrm{cd}(G)$ is either a π-number or a π'-number. They prove in that situation (although their result is stated slightly differently) that either G has a normal abelian Hall π or π'-subgroup or else G is solvable with nilpotent length $\leqq 5$.

Our Theorem A, which was communicated privately to Manz and Staszewski is a key ingredient in their proof. (I apologize to them for any difficulties caused by my two-year delay in getting this theorem into print.)

I would like to mention at this point, that it was B. Huppert, to whom this paper is dedicated, who is largely responsible for the renewed interest in character degree problems in recent years, especially problems of the type considered by Manz and Staszewski concerning prime divisors of character degrees. I would also like to thank Prof. Huppert for inviting me to Mainz in the summer of 1985 when most of this research was done and in the summer of 1987 when it was finally written up.

One may wonder what further conclusions one can draw about the group N of Theorem A. We know that N' must be nilpotent, but is there any bound on its nilpotence class? The answer is "no". In fact, even its derived length is unbounded.

Received September 11, 1987 and in revised form June 13, 1988. This research was partially supported by the National Science Foundation and the Deutsche Forschungsgemeinschaft. This paper is dedicated to B. Huppert on his sixtieth birthday.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

THEOREM B. *In the situation of Theorem A, the group N can have arbitrarily large derived length.*

The construction we use to prove Theorem B also allows us to build groups where the fraction of all irreducible characters which are nonlinear is arbitrarily small and yet the group has arbitrarily large derived length. This is relevant to the questions considered in [**6**] and indeed, the construction used here is a generalization of an example in that paper.

Finally, we mention that on the way toward proving Theorem A, we obtain a result relevant to a class of groups studied by A. R. Camina: groups having a normal subgroup K with $1 < K < G$ such that every conjugacy class of G outside of K is a union of cosets of K. It is well known that this holds if K is a Frobenius kernel in G. Camina proved [**1**] that if this is not the case, then either K or G/K must be a p-group for some prime p. Our result is the following.

THEOREM C. *If K and G satisfy Camina's condition above and G/K is a p-group, then G has a normal p-complement.*

This theorem generalizes some of the results in [**2**].

2. **Theorem** C.

We begin by proving a theorem that includes the result stated in the introduction as Theorem C.

(2.1) THEOREM. *Let $1 < K \lhd G$ and assume that G/K is a nontrivial nilpotent group. Suppose that each conjugacy class of G outside of K is a union of cosets of K. Then either*

(i) *G is a Frobenius group with kernel K or*

(ii) *G/K is a p-group for some prime p.*

If (ii) *holds, then G has a normal p-complement M and $\mathbf{C}_G(m) \subseteq K$ for all $m \in M - \{1\}$.*

Observe that the two cases are not mutually exclusive and that Theorem C is included within the last sentence. For our proof of Theorem A, we actually only need to use Theorem 2.1 when G/K is abelian. Adding that assumption to the hypotheses, however, would not, it seems, make the result substantially easier to prove.

Our proof includes some of Camina's arguments from [**1**].

Proof of Theorem 2.1. We begin with an observation (appearing in [**1**]) which we will use repeatedly. It is that if $g \in G - K$, then

$$|\mathbf{C}_G(g)| = |\mathbf{C}_{G/K}(Kg)|.$$

To see this, note that the conjugacy class $\mathrm{cl}_G(g)$ is the union of exactly those cosets of K which constitute the class $\mathrm{cl}_{G/K}(Kg)$. It follows that

$$|G:\mathbf{C}_G(g)| = |\mathrm{cl}_G(g)| = |K|\,|\mathrm{cl}_{G/K}(Kg)| = |K|\,|(G/K):\mathbf{C}_{G/K}(Kg)|$$

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

whence we obtain $|\mathbf{C}_G(g)| = |\mathbf{C}_{G/K}(Kg)|$ as claimed.

Now suppose that G splits over K so that $G = KU$ with $K \cap U = 1$ for some subgroup U. If $u \in U - \{1\}$, then the natural isomorphism between U and G/K yields

$$|\mathbf{C}_U(u)| = |\mathbf{C}_{G/K}(Ku)| = |\mathbf{C}_G(u)|$$

and so $\mathbf{C}_G(u) \subseteq U$. It follows that G is a Frobenius group and (i) holds.

We need another general observation. Let $g \in G - K$ and let $k \in \mathbf{C}_K(g)$. Then g is conjugate to gk and so

$$1 = (gk)^{o(g)} = k^{o(g)}$$

and hence $o(k)$ divides $o(g)$.

Suppose G does not split over K. We wish to establish (ii) and so we assume that the nilpotent group G/K is not a p-group for any prime p. We can choose, therefore, $z \in G - K$ such that $Kz \in \mathbf{Z}(G/K)$ and $o(Kz) = pq$ for primes $p \neq q$. Let r and s be the p'-part and q'-part of $o(z)$ respectively and let $x = z^r$ and $y = z^s$. Then $o(x)$ is a p-power, $o(y)$ is a q-power and $x, y \notin K$. Suppose $k \in \mathbf{C}_K(z)$. Then $k \in \mathbf{C}_K(x)$ and so $o(k)$ divides $o(x)$. Similarly, $o(k)$ divides $o(y)$ and hence $k = 1$. Therefore $\mathbf{C}_K(z) = 1$. Let $C = \mathbf{C}_G(z)$. Then $K \cap C = 1$ and

$$|C| = |\mathbf{C}_{G/K}(Kz)| = |G/K|$$

since $Kz \in \mathbf{Z}(G/K)$. It follows that $KC = G$ and this contradicts our nonsplitting assumption and shows that (i) or (ii) must occur.

Now assume that G/K is a p-group and let $P \in \mathrm{Syl}_p(G)$. By Tate's theorem (see Satz IV.4.7 of [5] or Theorem 6.31 of [7]), in order to prove that G has a normal p-complement, it suffices to show that $P \cap K \subseteq P'$. Let $z \in P - K$ with $Kz \in \mathbf{Z}(G/K)$ and let $Q = [P, z] \lhd P$. Since $[G, z] \subseteq K$, we have $Q \subseteq P \cap K$.

Now, by Corollary 2.24 of [7], for instance,

$$|\mathbf{C}_P(z)| \geqq |\mathbf{C}_{P/Q}(Qz)| = |P/Q|.$$

Therefore

$$|P/Q| \leqq |\mathbf{C}_P(z)| \leqq |\mathbf{C}_G(z)| = |\mathbf{C}_{G/K}(Kz)| = |G/K| = |P/P \cap K|$$

and hence $|Q| \geqq |P \cap K|$. Since $Q \subseteq P \cap K$, we have

$$P \cap K = Q = [P, z] \subseteq P'$$

and G has a normal p-complement M.

Finally, let $1 \neq m \in M$ and suppose $\mathbf{C}_G(m) \nsubseteq K$. Choose $g \in G - K$ centralizing m and note that $|\mathbf{C}_G(g)| = |\mathbf{C}_{G/K}(Kg)|$ is a p-power. Thus $\mathbf{C}_G(g)$ is a p-group and cannot contain m.

3. Theorem A. We need a preliminary lemma.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

(3.1) LEMMA. *Let P be a p-group with class $\leqq 2$ and suppose that P acts on some nontrivial p'-group Q such that $\mathbf{C}_P(x) \subseteq P'$ for all $x \in Q - \{1\}$. Then the action is Frobenius and P is either cyclic or isomorphic to Q_8.*

Proof. If the action is Frobenius, then, as is well known, P is cyclic or generalized quaternion. Since we are assuming that P has class $\leqq 2$, the only generalized quaternion group that can occur is Q_8.

It suffices, then, to show that the action is Frobenius and we do this by induction on $|P|$. If the action is not Frobenius, then there exists $x \in Q - \{1\}$ such that $\mathbf{C}_P(x) > 1$. Write $Z = \mathbf{C}_P(x)$ and note that $Z \subseteq P' \subseteq \mathbf{Z}(P)$ and so $Z \triangleleft P$. Let $C = \mathbf{C}_Q(Z)$ and note that $C > 1$ and P/Z acts on C.

If $y \in C - \{1\}$, then

$$\mathbf{C}_{P/Z}(y) = \mathbf{C}_P(y)/Z \subseteq P'/Z = (P/Z)'$$

and so the action of P/Z on C satisfies the hypotheses of the lemma. Since $|P/Z| < |P|$, the inductive hypothesis tells us that P/Z is either cyclic or isomorphic to Q_8.

If P/Z is cyclic, then P is abelian and this is a contradiction since $1 < Z \subseteq P'$. If $P/Z \cong Q_8$, then $P = AB$ for subgroups A, B containing Z with A/Z and B/Z cyclic of order 4. It follows that A and B are abelian and so $A \cap B \subseteq \mathbf{Z}(P)$ and $|P:\mathbf{Z}(P)| \leqq 4$. This forces $|P'| \leqq 2$ and since $Z \subseteq P'$, we conclude that $Z = P'$ and $Q_8 \cong P/Z$ is abelian, a contradiction.

We are almost ready now to prove Theorem A. Before we do, however, we wish to remind the reader of two relevant facts.

(3.2) LEMMA. *Let H act on N where $(|H|, |N|) = 1$. Then*

(a) *H fixes equal numbers of irreducible characters and conjugacy classes of N.*

(b) *If H fixes every irreducible character of N, then H acts trivially on N.*

Proof. Part (a) is a consequence of the fact that the number of H-fixed irreducible characters of N is equal to the total number of irreducible characters of $C = \mathbf{C}_N(H)$. If H is solvable, this equality follows by a result of G. Glauberman [3] (or see Chapter 13 of [7]). If N is solvable, the equality follows by results of E. C. Dade and the author. (Perhaps the most accessible proof of this can be found in [**8**].) By the Feit-Thompson theorem, at least one of N or H must be solvable and so the equality always holds.

To complete the proof of (a), it suffices to note that $K \mapsto K \cap C$ defines a bijection from the set of all H-fixed classes of G onto the set of all classes of C. This fact, proved using the conjugacy part of the Schur-Zassenhaus theorem, also relies on the Feit-Thompson theorem to guarantee that one of H or N is solvable. (See Corollary 13.10 of [7].)

The proof of part (b) lies much less deep since it is no loss in that case to assume that H is cyclic. Then, a result of R. Brauer (Theorem 6.32 of [7]) can substitute for part (a) of this lemma to guarantee that H fixes each class of G. It follows that $K \cap C \neq \emptyset$ for each class K. (In fact, we could assume H is a p-group. In that case, this is a triviality.) Therefore,

$$G = \bigcup_{x \in G} C^x$$

and as is well known, this forces $C = G$.

The next result is a somewhat more precise formulation of Theorem A.

(3.3) THEOREM. *Let H act nontrivially on N (via automorphisms) and assume that $(|N|, |H|) = 1$. Suppose that H fixes every nonlinear irreducible character of N. Let $M = [N, H]$. Then,*

(a) $M' = N'$.

(b) *M is either abelian, a class 2 p-group for some prime p or a Frobenius group with kernel M'.*

(c) *N' is nilpotent.*

Proof. The subgroup $N'M$ is H-invariant and so H permutes its irreducible characters. We claim that H fixes every $\alpha \in \mathrm{Irr}(N'M)$ with the property that $N' \not\subseteq \ker \alpha$. To see this, let $\chi \in \mathrm{Irr}(N|\alpha)$ and note that $N' \not\subseteq \ker \chi$ so that χ is nonlinear and hence is H-invariant. It follows by Theorem 13.27 of [7] that some irreducible constituent β of $\chi_{N'M}$ is fixed by H. We can write $\alpha = \beta^n$ for some $n \in N$. If $h \in H$, then $n^h = nm$ for some $m \in M$ and we have

$$\alpha^h = (\beta^n)^h = (\beta^h)^{nm} = \beta^n = \alpha$$

since $\beta^h = \beta$ and $m \in N'M$. Thus α is H-invariant, as claimed.

Next, let $\upsilon \in \mathrm{Irr}(N')$ with $\upsilon \neq 1_{N'}$. We will show that υ cannot extend to a character $\hat{\upsilon} \in \mathrm{Irr}(N'M)$. If such an extension existed, then for any $\mu \in \mathrm{Irr}(N'M/N')$, we have that $\hat{\upsilon}\mu$ is irreducible and if $\hat{\upsilon}\mu_1 = \hat{\upsilon}\mu_2$ for $\mu_i \in \mathrm{Irr}(N'M/N')$, then $\mu_1 = \mu_2$ by Gallagher's theorem (6.17 of [7]). Now $N' \not\subseteq \ker \hat{\upsilon}$ and $N' \not\subseteq \ker(\hat{\upsilon}\mu)$ for $\mu \in \mathrm{Irr}(N'M/N')$ and so by the first paragraph, H fixes both $\hat{\upsilon}$ and $\hat{\upsilon}\mu$. If $h \in H$, we have

$$\hat{\upsilon}\mu = (\hat{\upsilon}\mu)^h = \hat{\upsilon}^h\mu^h = \hat{\upsilon}\mu^h$$

and thus $\mu = \mu^h$. We conclude that H fixes all of the irreducible characters of $N'M/N'$ and therefore (by 3.2 (b)) H acts trivially on this group. Thus, since $(|H|, |N|) = 1$, we have

$$[N, H] = [N, H, H] = [M, H] \subseteq [N'M, H] \subseteq N'$$

and H acts trivially on N/N' and so fixes all linear characters of N. It follows that H fixes all irreducible characters of N and so acts trivially on N, a contradiction. Therefore, υ is not extendible to $N'M$, as claimed.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

Now $N'/(N' \cap M)$ is a direct factor of $N'M/(N' \cap M)$ and it follows that every $\upsilon \in \mathrm{Irr}(N')$ with $N' \cap M \subseteq \ker \upsilon$ extends to $N'M$. By the previous paragraph, the only possibility is that $\upsilon = 1_{N'}$, and thus $N' \cap M = N'$ and $N' \subseteq M$. Finally, if $\upsilon \in \mathrm{Irr}(N')$ with $M' \subseteq \ker \upsilon$, then υ extends to $M = N'M$ since M/M' is an abelian group. Again, the only possibility is $\upsilon = 1_{N'}$, and this shows that $M' = N'$, proving (a).

If α is any nonlinear irreducible character of M, then $N' = M' \not\subseteq \ker \alpha$ and so α is H-invariant by the first paragraph. If, on the other hand, α is a linear character of M, we claim that α cannot be fixed by H unless $\alpha = 1_M$. If α is fixed, then $\alpha(m^h) = \alpha(m)$ for $m \in M$ and $h \in H$ and thus $m^{-1}m^h \in \ker \alpha$. Therefore, $[M, H] \subseteq \ker \alpha$. Recall, however, that

$$[M, H] = [N, H, H] = [N, H] = M$$

and so $\alpha = 1_M$, as claimed. It follows that the number of irreducible characters of M which are not fixed by H is precisely $|M:M'| - 1$ and by 3.2 (a), this must also be the number of conjugacy classes of M not fixed by H.

Now let K be a class of M. Since M/M' is abelian, K is contained in a single coset $M'x$ of M' in M. If K is H-invariant, then $M'x$ is invariant and so $M'x \in \mathbf{C}_{M/M'}(H)$. This centralizer is trivial, however, since M/M' is abelian and $[\,(M/M'), H] = M/M'$. It follows that every H-invariant class of M is contained in M' and so none of the classes of M not contained in M' is invariant and hence there are at most $|M:M'| - 1$ of these classes. Since each nontrivial coset of M' in M is a union of such classes, we conclude that each such coset is a single class.

At this point, we have nearly established the hypotheses of Theorem 2.1, with M and M' in place of G and K. What we are missing are the conditions $M' > 1$ and $M' < M$. If $M' = 1$, there is nothing we need to prove, and so we simply assume that $M' > 1$. If $M' = M$, then H fixes all irreducible characters of M and thus $M = [M, H] = 1$ by 3.2 (b) and this contradicts the nontriviality of the action of H on N. All of the hypotheses of 2.1 are thus satisfied.

If M is a Frobenius group with kernel M', then $N' = M'$ is nilpotent by Thompson's theorem and there is nothing more we need to prove. By Theorem 2.1, therefore, we may assume that M/M' is a p-group for some prime p, that M has a normal p-complement $Q \subseteq M'$ and that if $P \in \mathrm{Syl}_p(M)$ and $1 \neq x \in Q$, then $\mathbf{C}_P(x) \subseteq P \cap M'$.

We claim that $[M', H] \subseteq Q$. To see this, work in the semidirect product $G = MH$ and consider a chief factor U/V of G with $Q \subseteq V \subseteq U \subseteq M'$. Since M/Q is a p-group, $U/V \subseteq \mathbf{Z}(M/V)$. Now let λ be a nontrivial linear character of U with $V \subseteq \ker \lambda$ and let $\chi \in \mathrm{Irr}(M|\lambda)$. Then χ_U is a multiple of λ and we have $M' \not\subseteq \ker \chi$ and thus χ is nonlinear and so is fixed by H. It follows that λ is H-invariant and thus H fixes all elements of $\mathrm{Irr}(U/V)$ and hence H acts trivially on U/V and $[U, H] \subseteq V$. Since H centralizes all

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

chief factors of G between Q and M' and since $[M', H, H] = [M', H]$, it follows that $[M', H] \subseteq Q$ as claimed.

We now have $[M', H, M] \subseteq [Q, M] \subseteq Q$ and $[M, M', H] \subseteq [M', H] \subseteq Q$. It follows by the three-subgroups lemma (since $Q \lhd G$) that $[H, M, M'] \subseteq Q$. We have, however, $[H, M] = M$, and thus $[M, M'] \subseteq Q$. It follows that $[P, P'] = 1$ and P has class $\leqq 2$.

If $Q = 1$, then $M = P$ and we have nothing further to prove, and so we assume $Q > 1$. We know that for $1 \neq x \in Q$, we have $\mathbf{C}_P(x) \subseteq P \cap M'$. Since $M/P'Q$ is abelian, we have $M' \subseteq P'Q$ and thus $P \cap M' = P'$ and we are in the situation of Lemma 3.1. It follows that the action of P on Q is Frobenius and either P is cyclic or $P \cong Q_8$.

If P is cyclic, then $M' \subseteq Q$ and we have that $M' = Q$ and M is a Frobenius group with kernel M' and we are done. We assume, therefore, that $P \cong Q_8$.

We may assume that H acts faithfully on N. Then H acts faithfully on M/M' since if $C = \mathbf{C}_H(M/M')$, then C fixes all linear characters of M and hence fixes all irreducible characters of M and so acts trivially on M. Thus

$$1 = [M, C] = [N, H, C] \supseteq [N, C, C] = [N, C]$$

and so $C = 1$ by our assumption that H acts faithfully on N. Since M/M' is noncyclic of order 4 and is acted on faithfully by the nontrivial group H of odd order, we conclude that $|H| = 3$ and $G/Q \cong SL(2, 3)$ (where $G = MH$, the semidirect product).

Now let Q/L be a chief factor of G. Since the action of P on Q is Frobenius, we have that $\mathbf{C}_P(Q/L) = 1$ and also, by Thompson's theorem, Q is nilpotent and Q/L is thus elementary abelian. Thus Q/L is a faithful irreducible module for G/Q. We may view Q/L as being absolutely irreducible as a module for $SL(2, 3)$ over some (possibly not prime) field and so $|Q/L| = q^2$ where q is a power of some prime >3. (Since $|H| = 3$, the prime 3 cannot divide $|Q|$.)

Let $\lambda \in \mathrm{Irr}(Q)$ be nontrivial with $L \subseteq \ker \lambda$. If $\chi \in \mathrm{Irr}(M|\lambda)$, then $M' \nsubseteq \ker \chi$ and so χ is H-invariant and χ_Q has an H-invariant irreducible constituent which is conjugate to λ in M. It follows that λ is fixed by one of the four Sylow 3-subgroups of $G/Q \cong SL(2, 3)$. Each such Sylow subgroup, however, fixes exactly $q - 1$ nontrivial linear characters of Q/L and we conclude that $4(q - 1) \geqq q^2 - 1$ and thus $4 \geqq q + 1$. This is a contradiction since $q > 3$.

4. Construction. We begin work now toward the proof of Theorem B. We will show how to construct Frobenius groups N with kernels S which are p-groups of arbitrarily large derived length and such that N is acted on nontrivially by some group H of coprime order such that H fixes all of the nonlinear irreducible characters of N. These groups generalize an ex-

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

ample which appears in [**6**] (where the derived length of the Frobenius kernel is 2). Ultimately, they are motivated by G. Higman's "Suzuki 2-groups" in [**4**].

We construct N as a subgroup of the group of units of a ring R and H as a subgroup of $\mathrm{Aut}(R)$. This "ring theoretic" construction was suggested by E. C. Dade after he read an earlier version of this paper in which S was constructed as a certain group of upper triangular matrices over a field F and N was a semidirect product of S with a subgroup of $F^{\times}$. Although Dade's construction is essentially equivalent to my earlier one, I agree with him that his version is an improvement and I thank him for suggesting it and allowing me to use it here.

We begin with a fairly standard result.

(4.1) LEMMA. *Let R be a ring* (*with* 1) *and suppose $J = J(R)$ is its Jacobson radical.*

(a) *The coset $S = 1 + J$ is a subgroup of the group of units of R.*

(b) *If $x \in J^u$ and $y \in J^v$ where u and v are positive integers, then the group commutator* $[(1 + x), (1 + y)] \equiv 1 + (xy - yx) \bmod J^{u+v+1}$.

Proof. Part (a) is completely standard. For (b), note that

$$\begin{aligned}&[(1 + x), (1 + y)] - 1\\ &= (1 + x)^{-1}(1 + y)^{-1}((1 + x)(1 + y) - (1 + y)(1 + x))\\ &= (1 + z)(xy - yx)\\ &\equiv xy - yx \bmod J^{u+v+1}\end{aligned}$$

where we have written $(1 + x)^{-1}(1 + y^{-1}) = 1 + z$ for some $z \in J$ by (a).

Now we construct a specific ring R. Fix a prime p and a positive integer m and let $F = GF(q)$ where $q = p^m$. Let $\theta \in \mathrm{Aug}(F)$ be the map $\alpha \mapsto \alpha^p$ and let $F\{X\}$ denote the corresponding "twisted polynomial ring" in the indeterminate X. In other words, the elements of $F\{X\}$ are "polynomials" of the form $\alpha_0 + \alpha_1 X + \dots + \alpha_k X^k$ with $\alpha_i \in F$. We do not assume that X commutes with the coefficents and instead we impose the relation

$$X\alpha = \alpha^{\theta}X \quad \text{for } \alpha \in F.$$

(It is well known that this does define a ring.)

Next, fix an integer n and note that

$$X^{n+1}F\{X\} = F\{X\}X^{n+1}$$

so that this object is a (two-sided) ideal which we denote (X^{n+1}). Let

$$R = F\{X\}/(X^{n+1})$$

and let x denote the image of X in R under the natural homomorphism.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

Then every element of R is uniquely of the form $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ and $|R| = q^{n+1}$. Also,

$$x^{n+1} = 0 \quad \text{and} \quad x\alpha = \alpha^{\theta}x \quad \text{for } \alpha \in F.$$

Note that $xR = Rx$ is a nilpotent ideal and $R/xR \cong F$. Thus $xR = J(R)$ and we write $xR = J$. We have $J^k = x^kR = Rx^k$ and so $J^n \neq 0$ and $J^{n+1} = 0$. In this situation, the group of Lemma 4.1 is

$$S = \{1 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n | \alpha_i \in F\}$$

and so $|S| = q^n$ and S is a p-group.

For integers $u \geqq 1$, write $S_u = 1 + J^u$ so that $S_u \subseteq S$ is a subgroup and

$$S = S_1 > S_2 > \ldots > S_n > S_{n+1} = 1.$$

Each element $s \in S_u$ is uniquely of the form $s = 1 + \alpha x^u + y$ with $\alpha \in F$ and $y \in J^{u+1}$. Let $\psi_u : S_u \rightarrow F$ be the map defined by $\psi_u(s) = \alpha$ where $s = 1 + \alpha x^u + y$ as above. In fact, ψ_u is a homomorphism from S_u onto the additive group of F. To see this, let $s, t \in S_u$ and write

$$s \equiv 1 + \alpha x^u \quad \text{and} \quad t \equiv 1 + \beta x^u \bmod J^{u+1}.$$

Then

$$st \equiv 1 + (\alpha + \beta)x^u \bmod J^{u+1}$$

and so

$$\psi_u(st) = \alpha + \beta = \psi_u(s) + \psi_u(t).$$

Note that $\ker(\psi_u) = S_{u+1}$ and so, in particular, $S_{u+1} \lhd S_u$.

We will compute the derived length of S by examining commutators of the form $[S_u, S_v]$ for $u, v \geqq 1$.

(4.2) COROLLARY. *Suppose $u, v \geqq 1$. Then $[S_u, S_v] \subseteq S_{u+v}$. Furthermore, if $u + v \leqq n$ and $s \in S_u$ and $t \in S_v$ with*

$$\psi_u(s) = \alpha \quad \textit{and} \quad \psi_v(t) = \beta,$$

then

$$\psi_{u+v}([s, t]) = \alpha\beta^{\theta^u} - \beta\alpha^{\theta^v}.$$

Proof. We have

$$s \equiv 1 + \alpha x^u \bmod J^{u+1} \quad \text{and} \quad t \equiv 1 + \beta x^v \bmod J^{v+1}$$

and so by 4.1 (b),

$$[s, t] \equiv 1 + (\alpha x^u \beta x^v - \beta x^v \alpha x^u) \bmod J^{u+v+1}.$$

In particular $[s, t] \in S_{u+v}$. Also,

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

$$x^u\beta = \beta^{\theta^u}x^u \quad \text{and} \quad x^v\alpha = \alpha^{\theta^v}x^v$$

and so

$$[s, t] \equiv 1 + (\alpha\beta^{\theta^u} - \beta\alpha^{\theta^v})x^{u+v} \bmod J^{u+v+1}.$$

If $u + v \leqq n$, this says that

$$\psi_{u+v}(\,[s, t]\,) = \alpha\beta^{\theta^u} - \beta\alpha^{\theta^v}$$

as claimed.

Clearly, we need to study the map $\langle \cdot\,, \cdot\rangle : F \times F \rightarrow F$ defined by

$$\langle \alpha, \beta\rangle = \alpha\beta^{\theta^u} - \beta\alpha^{\theta^v} \quad \text{for fixed } u, v \geqq 1.$$

Note that this map is F_0-bilinear where F_0 is the prime subfield of $F = GF(p^m)$.

(4.3) LEMMA. *Assume the previous notation and suppose that m is prime with $m > u + v$.*

(a) *If $\alpha \in F$ with $\alpha \neq 0$, then the F_0-subspace $\langle \alpha, F\rangle$ of F contains a hyperplane.*

(b) *There exist nonzero $\alpha, \beta \in F$ with $\langle \alpha, F\rangle \neq \langle \beta, F\rangle$.*

(c) *If $m \neq p$ and $\alpha \in F_0$, then $F_0 \not\subseteq \langle \alpha, F\rangle$.*

Proof. Since $\langle \alpha, \cdot\rangle$ is F_0-linear, (a) will follow if we prove that its nullspace is of dimension at most 1. If $\langle \alpha, \beta\rangle = 0 = \langle \alpha, \gamma\rangle$ with $\beta \neq 0$, therefore, we want to show that $\gamma \in F_0\beta$. We have

$$\alpha\beta^{\theta^u} - \beta\alpha^{\theta^v} = 0 = \alpha\gamma^{\theta^u} - \gamma\alpha^{\theta^v}$$

and so if $\gamma \neq 0$, we get

$$\beta^{-1}\beta^{\theta^u} = \alpha^{-1}\alpha^{\theta^v} = \gamma^{-1}\gamma^{\theta^u}$$

and hence

$$(\gamma\beta^{-1})^{\theta^u} = (\gamma\beta^{-1}).$$

Since m is prime and $m > u$, we see that θ^u generates the group $\langle\theta\rangle$ of order m. It follows that $\gamma\beta^{-1}$ is fixed by $\langle\theta\rangle = \mathrm{Gal}(F/F_0)$ and so $\gamma\beta^{-1} \in F_0$ as desired. This proves (a).

To prove (b) we use the trace map $T:F \rightarrow F_0$. Taking $\alpha = 1$, we have

$$\langle 1, \gamma\rangle = \gamma^{\theta^u} - \gamma$$

and so

$$T(\,\langle 1, \gamma\rangle\,) = T(\gamma^{\theta^u}) - T(\gamma) = 0.$$

The proof of (b) will be complete, therefore, if we can find $\beta, \gamma \in F$ with $T(\,\langle \beta, \gamma\rangle\,) \neq 0$. We have

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

$$\begin{aligned} T(\langle\beta, \gamma\rangle) &= T(\beta\gamma^{\theta^u}) - T(\gamma\beta^{\theta^v}) \\ &= T(\beta^{\theta^v}\gamma^{\theta^{u+v}}) - T(\gamma\beta^{\theta^v}) \\ &= T(\beta^{\theta^v}(\gamma^{\theta^{u+v}} - \gamma)). \end{aligned}$$

Since $m \nmid (u + v)$, we can choose γ so that

$$\gamma^{\theta^{u+v}} - \gamma \neq 0$$

and then we can choose β so as to make

$$\beta^{\theta^v}(\gamma^{\theta^{u+v}} - \gamma)$$

an arbitrary element of F. In particular, it can be made to have nonzero trace.

Finally for (c), we note that if $\alpha \in F_0$, then $\langle\alpha, F\rangle \subseteq \langle 1, F\rangle$ and so $T(\langle\alpha, F\rangle) = 0$. For $\gamma \in F_0$, however, we have $T(\gamma) = m\gamma$. Since $m \neq p$, it follows that $T(\gamma) \neq 0$ for $\gamma \neq 0$ and so $\gamma \notin \langle\alpha, F\rangle$.

The next result includes a simplification of the original version for which I would like to thank A. Mann.

(4.4) Corollary. *Assume the previous notation and let m be a prime number of m > n. Then* $[S_u, S_v] = S_{u+v}$.

Proof. By (4.2), $[S_u, S_v] \subseteq S_{u+v}$ and if $u + v > n$, then $S_{u+v} = 1$ and nothing remains to be proved. Suppose then that $u + v \leqq n$ and work by downward induction on $u + v$.

Now $\psi_{u+v}([S_u, S_v])$ is a subgroup (i.e., F_0-subspace) of F containing all elements of the form $\langle\alpha, \beta\rangle$ with $\alpha, \beta \in F$. Since $m > n$, we have $m > u + v$ and so by 4.3 (a), (b), $\psi_{u+v}([S_u, S_v])$ contains two different hyperplanes and so is all of F. Thus

$$\psi_{u+v}([S_u, S_v]) = \psi_{u+v}(S_{u+v})$$

and the result follows since $\ker(\psi_{u+v}) \subseteq [S_u, S_v]$. This is so since

$$\ker(\psi_{u+v}) = S_{u+v+1} = [S_{u+1}, S_v]$$

by the inductive hypothesis.

(4.5) Corollary. *If m is prime and m > n, then the derived length* $\mathrm{dl}(S) > \log_2(n)$.

Proof. Write $S^{(k)}$ to denote the k-th term of the derived series of S with $S^{(0)} = S = S_1$. It follows by induction on k that $S^{(k)} = S_{2^k}$ since

$$S^{(k)} = [S^{(k-1)}, S^{(k-1)}] = [S_{2^{k-1}}, S_{2^{k-1}}] = S_{2^k}.$$

If $k = \mathrm{dl}(S)$, we have

$$1 = S^{(k)} = S_{2^k}$$

and thus $2^k > n$.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

The multiplicative group $F^\times$ is cyclic of order divisible by $p - 1$ and so there is a unique subgroup $C \subseteq F^\times$ of index $p - 1$.

(4.6) LEMMA. *Assume the above notation and suppose m is prime with $m > p$. Then $F^\times$ is the direct product $C \times F_0^\times$.*

Proof. Since $|C| \cdot |F_0^\times| = |F^\times|$, it suffices to show that $|C| = (q - 1)/(p - 1)$ is coprime to $|F_0^\times| = p - 1$. Suppose $d|(p - 1)$ and note that $|C| = 1 + p + \ldots + p^{m-1}$ since $q = p^m$. Because $p \equiv 1 \pmod{d}$, this yields

$$|C| \equiv m \pmod{d}.$$

If also $d||C|$, we have $|C| \equiv 0 \pmod{d}$ and thus $d|m$. Since m is prime, either $d = 1$ or $d = m$. It is not possible that $d = m$, however, since that would yield $m|(p - 1)$, contradicting $m > p$.

We identify C with the subgroup $C \cdot 1$ of the unit group $R^\times$ of R and we work inside $R^\times$.

(4.7) LEMMA. *Assume the previous notation. Then $C \subseteq \mathbf{N}(S)$. Furthermore, if m is a prime with $m > p$ and $m > n$, then $N = SC$ is a Frobenius group with kernel S and complement C.*

Proof. Let $s \in S$ and $\gamma \in C$ and assume $s \neq 1$. Then

$$s = 1 + \alpha x^u + y$$

for some unique nonzero $\alpha \in F$, integer u with $1 \leqq u \leqq n$ and element $y \in J^{u+1}$. Since

$$x^u\gamma = \gamma^{\theta^u}x^u,$$

we have

$$\gamma^{-1}s\gamma = 1 + \alpha\gamma^{-1}\gamma^{\theta^u}x^u + \gamma^{-1}y\gamma.$$

We see that $\gamma^{-1}s\gamma \in 1 + J = S$ and the first assertion follows. If $\gamma^{-1}s\gamma = s$, this forces

$$\gamma^{-1}\gamma^{\theta^u} = 1$$

(since $\gamma^{-1}y\gamma \in J^{u+1}$) and thus γ is fixed by θ^u. Since $\langle\theta^u\rangle = \langle\theta\rangle$ (because $u \leqq n < m$ and m is prime) it follows that $\gamma \in F_0$. By 4.6, $\gamma = 1$.

Next, we consider the subgroup $A \subseteq S$ defined by

$$A = 1 + xF_0[x].$$

In other words

$$A = \{1 + \alpha_1 x + \ldots + \alpha_n x^n | \alpha_i \in F_0\}.$$

Since $x\alpha = \alpha^\theta x = \alpha x$ for $\alpha \in F_0$, it is clear that A is abelian.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

(4.8) LEMMA. *Assume the previous notation and suppose that m is prime, $m > p$ and $m > n$. Then every conjugacy class of N in S meets A.*

Proof. Given an N-class $K \subseteq S$, suppose $K \cap A = \emptyset$. Let $s \in K$ and write

$$s = 1 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n.$$

Since $s \notin A$, there exists a subscript $w \geqq 1$ such that $\alpha_w \notin F_0$ and $\alpha_i \in F_0$ for all $i < w$. Choose $s \in K$ so that w is as large as possible.

Now let $u \geqq 1$ be the subscript such that $\alpha_u \neq 0$ but $\alpha_i = 0$ for all $i < u$. Then $u \leqq w$ and $s \in S_u$. Suppose $u = w$ and write $\alpha_u = \delta\epsilon$ where $\delta \in F_0^{\times}$ and $\epsilon \in \mathbf{C}$. (We are using 4.6 here.) Since $\alpha_u \notin F_0$, we have $\epsilon \neq 1$.

Because $u \leqq n < m$, we have $\langle \theta^u \rangle = \langle \theta \rangle$ and thus θ^u has no nontrivial fixed points on C (since $C \cap F_0 = \{1\}$ by 4.6). It follows that the map

$$\gamma \mapsto \gamma^{-1}\gamma^{\theta^u}$$

maps C onto itself and so we can choose $\gamma \in \mathbf{C}$ such that

$$\gamma^{-1}\gamma^{\theta^u} = \epsilon^{-1}.$$

We have

$$\gamma^{-1}s\gamma = 1 + \sum_{i=u}^{n} \alpha_i \gamma^{-1}\gamma^{\theta^i} x^i$$

and thus the coefficient of x^u in $\gamma^{-1}s\gamma$ is $\alpha_u\epsilon^{-1} = \delta \in F_0$. Now $\gamma^{-1}s\gamma \in K$ and the "w-value" of this element exceeds $u = w$. This contradicts the choice of s.

It follows that $w > u$. Set $v = w - u \geqq 1$ use the notation

$$\langle \alpha, \beta \rangle = \alpha\beta^{\theta^u} - \beta\alpha^{\theta^v}$$

as in 4.2 and 4.3. By 4.3 (a), $\langle \alpha_u, F \rangle$ contains an F_0-hyperplane of F but by 4.3 (c), it does not contain F_0. It follows that $\langle \alpha_u, F \rangle + F_0 = F$ and so the coset $\langle \alpha_u, F \rangle + \alpha_w$ contains some element of F_0 and we can choose $\beta \in F$ such that

$$\langle \alpha_u, \beta \rangle + \alpha_w \in F_0.$$

Now write $t = 1 + \beta x^v \in S$ and compute

$$s^t = s[s, t] \equiv \left(1 + \sum_{i=u}^{w} \alpha_i x^i\right)(1 + \langle \alpha_u, \beta \rangle x^w) \bmod J^{w+1}.$$

It follows that

$$s^t = 1 + \sum_{i=u}^{w-1} \alpha_i x^i + (\alpha_w + \langle \alpha_u, \beta \rangle)x^w \bmod J^{w+1}.$$

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

Since $\alpha_w + \langle \alpha_u, \beta \rangle \in F_0$, the "$w$-value" of s^t exceeds w. This is a contradiction and 4.8 is proved.

The automorphism θ of F can be extended to an automorphism of the ring R (which we continue to call θ) by setting $x^\theta = x$. Let $H \subseteq \mathrm{Aut}(R)$ be the subgroup generated by θ so that $|H| = m$. Note that H acts on the unit group $R^\times$ and fixes (setwise) the subgroups S and C. In particular, H acts on N.

(4.9) THEOREM. *Given a prime number p and an integer n* $\geqq 1$, *choose a prime number m* $> \max(p, n)$. *Let N and H be as above so that H acts on N. Then*

(a) $|H| = m$ *and* $|N| = p^{mn}(p^m - 1)/(p - 1)$ *are coprime.*

(b) N' *is a p-group with derived length exceeding* $\log_2(n)$.

(c) *H fixes all of the* $p^n - 1$ *nonlinear irreducible characters of N.*

(d) *H fixes none of the* $(p^m - 1)/(p - 1) - 1$ *nontrivial linear characters of N.*

Proof. That $(|H|, |N|) = 1$ follows since

$$p^m - 1 \equiv p - 1 \not\equiv 0 \pmod{m}$$

since m is prime and $m > p$. This establishes (a).

Since N is a Frobenius group with kernel S and cyclic complement C, we see that $N' = S$ and (b) holds 4.5. Also, the linear characters of N are essentially the linear characters of C. Since $\mathbf{C}_C(H) = C \cap F_0^\times = 1$ by 4.6, statement (d) follows.

The conjugacy classes of N are of two types: those contained in S and the $|C| - 1$ nontrivial cosets of S in N. Each class of the first type contains an element of $A = \mathbf{C}_S(H)$ by 4.8 and so is fixed by H. None of the classes of the second type is fixed by H since $\mathbf{C}_C(H) = 1$. Therefore, all but $|C| - 1$ of the classes of N are H-invariant and since H is cyclic, it follows that all but $|C| - 1$ of the irreducible characters of N are fixed by H. It follows (in view of (d)) that H fixes all of the nonlinear irreducible characters of N.

At this point, we have proved enough of the result to yield Theorem B of the introduction. To complete the proof of (c), we need to show that there are exactly p^n classes of N contained in S. Since each such class meets A and $|A| = p^n$, it suffices to show that each class of N in S meets A in a single element.

Since $\mathbf{C}_{N/S}(H)$ is trivial, we see that $\mathbf{C}_N(H) = \mathbf{C}_S(H) = A$. By general facts about coprime actions, each H-invariant class of N meets A in a class of A and since A is abelian, this is a single element, as required.

(4.10) COROLLARY. *Let* $r(G)$ *be the fraction of the irreducible characters of the solvable group G which are nonlinear. Given* $\epsilon > 0$, *there exist groups G with arbitrarily large derived length such that* $r(G) < \epsilon$.

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press

Proof. Take n large and m very much larger than n in 4.9.

References

1. A. R. Camina, *Some conditions which almost characterize Frobenius Groups*, Israel J. of Math. *31* (1978), 153-160.
2. David Chillag and I. D. Macdonald, *Generalized Frobenius groups*, Israel J. of Math. *47* (1984), 111-122.
3. G. Glauberman, *Correspondence of characters for relatively prime operator groups*, Can. J. Math. *20* (1968), 1465-1488.
4. G. Higman, *Suzuki 2-groups*, Illinois J. of Math. *7* (1963), 79-96.
5. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin-Heidelberg-New York, 1967).
6. I. M. Isaacs and D. S. Passman, *Groups with relatively few nonlinear irreducible characters*, Can. J. Math. *20* (1968), 1451-1458.
7. I. M. Isaacs, *Character theory of finite groups* (Academic Press, New York, 1976).
8. ——— *Character correspondences in solvable groups*, Advances in Math. *43* (1982), 284-306.
9. O. Manz and R. Staszewski, *Some applications of a fundamental theorem by Gluck and Wolf in the character theory of finite groups*, Math. Zeit. *192* (1986), 383-389.

University of Wisconsin,
Madison, Wisconsin

https://doi.org/10.4153/CJM-1989-003-2 Published online by Cambridge University Press