GROUPS WITH RELATIVELY FEW NON-LINEAR IRREDUCIBLE CHARACTERS

I. M. ISAACS AND D. S. PASSMAN

In (**4**), Seitz characterized those finite groups which have exactly one non-linear irreducible character (over the complex numbers). In this paper we are concerned with the general question of what can be deduced about a finite group G if the number of its non-linear irreducible characters $m(G)$ is given. In particular, does the assumption that $m(G)$ is in some sense small when compared with the order $|G|$ impose any restrictions on the structure of G? We show that if G is nilpotent and $m(G)$ is small, then G must have class $\leqq 2$ but that non-nilpotent groups need not even be metabelian (although Seitz showed that if $m(G) = 1$, then this must be the case). We do show however, that groups with small period and few non-linear characters when compared with the order must necessarily be nilpotent.

1. In a group G, any two conjugate elements must lie in the same coset of G', and hence each such coset is a normal subset of G, i.e., a union of conjugacy classes. We shall denote the number of classes of G contained in a normal subset S by $k(S)$.

LEMMA 1.1. *In a group G, $m(G) = \sum(k(G'x) - 1)$, where the sum runs over all cosets of G' in G. In particular, at most $m(G)$ cosets fail to be single classes. Also, $|\mathbf{Z}(G) \cap G'| \leqq m(G) + 1$ and if $1 < G' \subseteq \mathbf{Z}(G)$, then $|\mathbf{Z}(G)| \leqq 2m(G)$.*

Proof. We have that $\sum k(G'x) = k(G) = [G : G'] + m(G)$ since the number of irreducible characters of G is equal to $k(G)$. This yields

$$m(G) = \sum k(G'x) - [G : G'] = \sum(k(G'x) - 1).$$

Each $G'x$ which is not a single class contributes at least one to the sum, and thus the number of such cosets is $\leqq m(G)$.

Now, $k(G') \geqq |Z(G) \cap G'|$; thus $|Z(G) \cap G'| \leqq m(G) + 1$. Finally, if $G' \subseteq \mathbf{Z}(G)$ and $z \in \mathbf{Z}(G)$, then $G'z \subseteq \mathbf{Z}(G)$ and $k(G'z) = |G'|$. The number of cosets of G' containing elements of $\mathbf{Z}(G)$ is $[\mathbf{Z}(G):G']$, and thus $m(G) \geqq (|G'| - 1)[\mathbf{Z}(G):G']$. We then have that

$$|\mathbf{Z}(G)| \leqq \frac{m(G)|G'|}{|G'| - 1} \leqq 2m(G)$$

since $|G'| > 1$.

Received June 5, 1967.

https://doi.org/10.4153/CJM-1968-146-3 Published online by Cambridge University Press

We confine our attention to nilpotent groups for the remainder of this section.

PROPOSITION 1.2. *If G is nilpotent, then $|G'| \leqq 2^{m(G)}$.*

Proof. A series $1 = H_0 < H_1 < \ldots < H_r = G'$ can be found, where $H_i \triangle G$ and $[H_i:H_{i-1}] = p_i$, a prime for $1 \leqq i \leqq r$. Now, H_i/H_{i-1} is central in G/H_{i-1} and thus consists of p_i classes of G/H_{i-1}. It follows that

$$k(H_i - H_{i-1}) \geqq p_i - 1,$$

and thus

$$k(G') \geqq 1 + \sum_{i=1}^{r} (p_i - 1) \quad \text{and} \quad m(G) \geqq k(G') - 1 \geqq \sum (p_i - 1).$$

We claim that for any set of integers $p_i \geqq 2$,

$$\Pi p_i \leqq 2^{\Sigma(p_i - 1)}$$

and since $|G'| = \Pi p_i$, this will yield the desired result. The function $f(x) = x^{1/(x-1)}$ is monotone decreasing for $x \geqq 2$ and $f(2) = 2$; thus $x \leqq 2^{x-1}$ for $x \geqq 2$. Substituting p_i for x and multiplying yields the required inequality.

Although $|G'|$ is bounded by a function of $m(G)$ for nilpotent groups, there is no bound for solvable groups as is shown by the example of Theorem 3.1. Furthermore, $|G|$ is not bounded by a function of $m(G)$ even for p-groups as the abelian and extra-special p-groups clearly show. (If G is an extra-special p-group, then $m(G) = p - 1$.) The following theorem, however, yields a bound on $|G|$ when G is a p-group of class > 2.

THEOREM 1.3. *Let G be a p-group with $m(G) < p^e$. If $[G : G'] \geqq p^{3e-2}$, then G has class $\leqq 2$ and $|G'| \leqq m(G) + 1$.*

Proof. The proof is by induction on $|G'|$. If $|G'| = 1$, the result is trivial; thus, we assume that $G' > 1$, and hence we can find $U \triangle G$ with $U \subseteq G'$ and $|U| = p$. Then $m(G/U) \leqq m(G) < p^e$ and $G'/U = (G/U)'$; thus, $[G/U:(G/U)'] = [G : G'] \geqq p^{3e-2}$ and G/U satisfies the hypotheses. By the inductive hypothesis, G/U has class $\leqq 2$ and $|G'|/p = |(G/U)'| \leqq m(G/U) + 1$. Since $U \subseteq G'$, U is not in the kernel of every non-linear irreducible character of G, and thus $m(G/U) < m(G)$. Thus $|G'|/p \leqq m(G/U) + 1 \leqq m(G) < p^e$ and $|G'| < p^{e+1}$. Since $|G'|$ is a power of p, we have that $|G'| \leqq p^e$.

Since the product of an irreducible character with a linear character is irreducible, multiplication defines an action of the group C of linear characters of G on the set $\text{Irr}(G)$ of irreducible characters of G. If $\chi \in \text{Irr}(G)$ is non-linear, then, clearly, the size of the orbit of χ under the action of C is $\leqq m(G)$. Therefore, C has a subgroup K with $[C : K] \leqq m(G)$ and $\lambda\chi = \chi$ for all $\lambda \in K$. Let $H = \bigcap \{\ker\lambda | \lambda \in K\}$. Each $\lambda \in K$ may be viewed as a linear character of G/H and therefore

$$[G:H] \geqq |K| \geqq \frac{|C|}{m(G)} = \frac{[G:G']}{m(G)} > \frac{p^{3e-2}}{p^e} = p^{2(e-1)}.$$

If $x \in G - H$, then $\lambda(x)\chi(x) = \chi(x)$ for all $\lambda \in K$. Since $x \notin H$, $\lambda(x) \neq 1$ for some $\lambda \in K$, and thus $\chi(x) = 0$ and χ vanishes on $G - H$. Then

$$[G : H]\,[\chi, \chi]_G = [\chi|H, \chi|H]_H \leqq \chi(1)^2,$$

and thus $p^{2(e-1)} < [G : H] \leqq \chi(1)^2$. Therefore, $p^{e-1} < \chi(1)$ and since $\chi(1)$ must be a power of p, we have that $\chi(1) \geqq p^e$ for every non-linear irreducible character χ of G.

If $y \in G$ is arbitrary, then G acts on the class of y by conjugation and since $\mathrm{cl}(y) \subseteq G'y$, the degree of this permutation representation is $\leqq |G'| \leqq p^e$. If ϕ is the character of this representation, then ϕ is a sum of irreducible characters of G, one of which must be the principal character. Thus, the sum of the remaining irreducible constituents of ϕ has degree $< p^e$ and therefore ϕ can have no non-linear irreducible constituents. It follows that G' is in the kernel of ϕ, and thus acts trivially on $\mathrm{cl}(y)$ and $y \in \mathbf{C}(G')$. Since y was arbitrary, $G' \subseteq \mathbf{Z}(G)$ and the nilpotence class of G is $\leqq 2$. By Lemma 1.1 we have that $|G'| = |G' \cap \mathbf{Z}(G)| \leqq m(G) + 1$ and the proof is complete.

We give, as a corollary, an alternative statement of the theorem which does not involve the particular prime.

COROLLARY 1.4. *Let G be a p-group. If $[G : G'] > m(G)^3$, then G has class $\leqq 2$ and $|G'| \leqq m(G) + 1$.*

Proof. Let p^e be the smallest power of p larger than $m(G)$. Then $m(G) \geqq p^{e-1}$; thus, $[G : G'] < p^{3(e-1)}$ and since $[G : G']$ is a power of p, we have that $[G : G'] \geqq p^{3e-2}$ and the hypotheses of the theorem are satisfied and the result follows. Applying this to arbitrary nilpotent groups we obtain the following corollary.

COROLLARY 1.5. Let *G be non-abelian and nilpotent and suppose that $[G : G'] > m(G)^3$. Then $G = K \times P$, where P is a p-group of class 2, K is abelian, $|K| \leqq m(G)$, and $|G'| \leqq m(G)/|K| + 1$.*

Proof. Choose a non-abelian Sylow p-subgroup P of G and write $G = K \times P$. We then have that

$$(*) \qquad m(G) = m(P)[K : K'] + m(K)[P : P'] + m(K)m(P).$$

Since $m(G)^3 < [G : G'] = [K : K'][P : P']$, one of $[K : K']$ and $[P : P']$ must be $> m(G)$. Since $m(P) > 0$, this yields a contradiction from (*) if $m(K) > 0$, i.e., if K is non-abelian. Thus, K is abelian and $m(G) = |K|m(P)$; therefore, $|K| \leqq m(G)$ and

$$[P : P'] = [G : G']/|K| > m(G)^3/|K| \geqq (m(G)/|K|)^3 = m(P)^3.$$

The result now follows from Corollary 1.4.

It is of interest to note that these results may be stated independently of character theory. Since $m(G) = k(G) - [G : G']$, the condition $[G : G'] > m(G)^3$ is equivalent to $k(G) < [G : G']^{1/3} + [G : G']$. We conclude this section with one further result.

https://doi.org/10.4153/CJM-1968-146-3 Published online by Cambridge University Press

PROPOSITION 1.6. *There exists a function B defined on the natural numbers such that if G is a non-abelian nilpotent group, then the period of G is $\leqq B(m(G))$.*

Proof. If $[G:G'] \leqq m(G)^3$, then since by Proposition 1.2 $|G'| \leqq 2^{m(G)}$, we have that $|G| \leqq 2^{m(G)}m(G)^3$, and hence the period of G is bounded by $2^{m(G)}m(G)^3$. We may therefore assume that $[G:G'] > m(G)^3$, and thus by Corollary 1.5, G has class 2 and $1 < G' \subseteq \mathbf{Z}(G)$. By Lemma 1.1 we then have that $|\mathbf{Z}(G)| \leqq 2m(G)$, $|G'| \leqq m(G)+1$. If $x, y \in G$, then $[x,y]^n = [x^n, y]$ for any integer n, and thus $1 = [x,y]^{|G'|} = [x^{|G'|}, y]$ and since y is arbitrary, $x^{|G'|} \in \mathbf{Z}(G)$. Therefore, $x^{|G'|\,|\mathbf{Z}(G)|} = 1$ and the order of x is $\leqq |G'|\,|\mathbf{Z}(G)| \leqq 2m(G)(m(G)+1)$. It follows that the function $B(m) = \max\{2^m m^3, 2m(m+1)\}$ has the desired properties.

That Proposition 1.6 is not true if G is solvable but not nilpotent can be seen from the example of Theorem 3.1.

2. Here we study not necessarily nilpotent groups for which $m(G)$ is given.

PROPOSITION 2.1. *If p is a prime and $p^a | [G:G']$, where $p^a > m(G)$, then G has a normal p-complement.*

Proof. As in the proof of Theorem 1.3, the group C of linear characters of G acts on the set $\mathrm{Irr}(G)$ by multiplication and if $\chi \in \mathrm{Irr}(G)$ is non-linear, then the orbit containing χ has size $\leqq m(G)$ and the subgroup $K = \{\lambda \in C \mid \lambda\chi = \chi\}$ satisfies $[C:K] \leqq m(G) < p^a$. But $p^a \mid [G:G']$ and $|C| = [G:G']$; therefore $p \mid |K|$. Thus, there exists $\lambda \in K$, $\lambda \neq 1$, $\lambda^p = 1$ with $\lambda\chi = \chi$. If $H = \ker\lambda$, then $H \triangle G$, $[G:H] = p$, and χ vanishes on $G - H$. Thus $[\chi|H, \chi|H]_H = [G:H][\chi, \chi]_G = p$. Since $\chi|H = a\sum_1^t \theta_i$ and $p = [\chi|H, \chi|H]_H = a^2 t$, it follows that $t = p$, and thus $p|\chi(1)$. Thus, every non-linear irreducible character of G has degree divisible by p and it follows from Theorem 2.5 (i) of (**2**) that G has a normal p-complement.

LEMMA 2.2. *Let π be a set of primes and let $G'x$ be a π-element of G/G'. Suppose that $G'x$ consists of a single class of G. Then x is a π-element of G and $\mathbf{C}_{G'}(x)$ is a π-group.*

Proof. We may write $x = yz$, where y and z are both powers of x, y is a π'-element, and z is a π-element. Now, $G' \triangle \langle G', x\rangle$ and $\langle G', x\rangle/G'$ is a π-group; thus all π'-elements of $\langle G', x\rangle$ are in G'. In particular, $y \in G'$; therefore $z \in G'x$, and thus z is conjugate to x in G and therefore x is a π-element.

If $u \in \mathbf{C}_{G'}(x)$ is a non-trivial π'-element, then ux is not a π-element. Since $ux \in G'x$, it is conjugate to x and this is a contradiction; thus, $\mathbf{C}_{G'}(x)$ must be a π-group and the proof is complete.

PROPOSITION 2.3. *Let $P \subseteq G$, where G is not nilpotent and P is an abelian p-subgroup of period $\leqq n$. Then $[PG':G'] \leqq nm(G)$.*

Proof. If $[PG':G'] \leqq m(G)$, nothing remains to be shown; thus, we may assume that $[PG':G'] > m(G)$, and thus Proposition 2.1 applies and G has a normal p-complement K. Let $H = G' \cap K$. If $H = 1$, then $K \subseteq \mathbf{Z}(G)$, G' is a p-group, and thus G is nilpotent, contrary to our assumption. Thus $H > 1$ and we can find an elementary abelian q-subgroup Q of H on which P acts. We may assume that Q is irreducible under this action, and thus, if $L \subseteq P$ is the kernel of the action, we see that P/L is cyclic, and thus $[P : L] \leqq n$. Now let $P_0 = P \cap G'$. We have that $[L : L \cap P_0] = [L : L \cap G'] = [LG' : G']$. Each coset of G' in LG' has a power of p as its order in G/G' and contains an element of L which centralizes the non-trivial p'-subgroup Q of G'. By Lemma 2.2, none of these cosets can consist of a single class of G, and thus by Lemma 1.1 there are at most $m(G)$ such cosets and $[LG' : G'] \leqq m(G)$. Thus

$$[PG' : G'] = [P : P \cap G'] = [P : P_0] \leqq [P : P_0 \cap L] = [P : L][L : P_0 \cap L] \leqq nm(G).$$

This establishes the proposition.

PROPOSITION 2.4. *Let P be a non-abelian Sylow p-subgroup of a non-nilpotent group G. Then $[PG' : G'] \leqq F(m(G))$ for a suitably chosen function F, independent of G.*

Proof. Choose $F(m) \geqq m$ so that we may assume that $[PG' : G'] > m(G)$ and G has a normal p-complement by Proposition 2.1. If K is the complement, then $P \cong G/K$; therefore $m(P) \leqq m(G)$. Thus, P has period $\leqq B(m(P))$ $\leqq B^*(m(G))$, where B is the function whose existence is guaranteed by Proposition 1.6 and $B^*(m) = \max\{B(n) | n \leqq m\}$. Choose a self-centralizing normal subgroup A of P and apply Proposition 2.3 to conclude that $[AG' : G'] \leqq B^*(m(G))m(G)$. Now, $|P'| \leqq 2^{m(P)} \leqq 2^{m(G)}$ by Proposition 1.2, and since G has a normal p-complement, $P' = P \cap G'$; therefore $|P \cap G'| \leqq 2^{m(G)}$. Thus

$$|A| = [A : A \cap G']\,|A \cap G'| \leqq [AG' : G']\,|P \cap G'| \leqq B^*(m(G))m(G)2^{m(G)}.$$

Since P/A is isomorphic to a subgroup of $\mathrm{Aut}(A)$, its order is bounded by a function of $|A|$ and this yields a bound on $|P|$ and the result follows.

We shall need the following result of Landau (**3**) which is stated here as a lemma.

LEMMA 2.5. *There exists a function L defined on the natural numbers such that if G is a finite group and $k(G) \leqq n$, then $|G| \leqq L(n)$.*

THEOREM 2.6. *For each natural number n, there exists a function f_n such that if G is a finite group, then either*

(1) *G is abelian,*

(2) *$[G : G'] \leqq f_n(m(G))$ and $|G| \leqq L(m(G) + f_n(m(G)))$,*

(3) *$G = K \times P$, where K is abelian, $|K| \leqq m(G)$, P is a p-group of class 2, and $|G'| \leqq m(G)/|K| + 1$, or*

(4) *$G = G'A$, where $G' \cap A = 1$, A contains an (abelian) Sylow p-subgroup P of G with period $> n$, and at most $m(G)$ elements of A have non-trivial centralizers in G'.*

Proof. Since $k(G) = m(G) + [G : G']$, the second part of (2) follows from the first by Lemma 2.5. If we take $f_n(m) \geqq m^3$ for each n, then if G is nilpotent and does not satisfy (1) or (2), we have that $[G : G'] > f_n(m(G)) \geqq m(G)^3$ and by Corollary 1.5, G satisfies (3). We may therefore restrict our attention to non-nilpotent groups.

Let G be non-nilpotent and suppose that G does not satisfy (4). If p is a prime dividing $[G : G']$ and P is an abelian S_p-subgroup of G, then the p-part of $[G : G']$ is $[PG' : G']$. If $[PG' : G'] > m(G)$, then G has a normal p-complement K by Proposition 2.1 and $G = KP$. Since P was assumed to be abelian, $G' \subseteq K$ and each element of P is in a distinct coset of G'. By Lemma 1.1, at most $m(G)$ of them are in cosets which are not a single class of G. Since $|P| > m(G)$, we have that $G'x$ is a class for some $x \in P$, and hence $|\mathbf{C}(x)| = [G : G']$. By Lemma 2.2, $\mathbf{C}_{G'}(x)$ is a p-group but since $G' \subseteq K$, we have that $\mathbf{C}_{G'}(x) = 1$. Therefore, if $A = \mathbf{C}(x)$, we have that $A \cap G' = 1$; thus A is abelian and since $|A|\,|G'| = |G|$, we see that $G = G'A$. If $y \in A$ with $\mathbf{C}_{G'}(y) > 1$, then $\mathbf{C}_G(y) > A$ and $[G : \mathbf{C}(y)] < |G'|$; thus $G'y$ is not a single class of G. Since each $y \in A$ is in a distinct coset of G', there can be at most $m(G)$ such y with $\mathbf{C}_{G'}(y) > 1$. Since we have assumed that (4) does not hold, it follows that the period of P is $\leqq n$, and thus by Proposition 2.3, the p-part of $[G : G']$ is $\leqq nm(G)$. We see then that this is true for all primes dividing $[G : G']$ for which a Sylow subgroup of G is abelian.

Suppose now that $p | [G : G']$ and that P is a non-abelian S_p-subgroup of G. Then the p-part of $[G : G']$ is $[PG' : G'] \leqq F(m(G))$ by Proposition 2.4. Thus, the contribution of each prime divisor to $[G : G']$ is $\leqq M = \max\{nm(G), F(m(G))\}$. In particular, if $p | [G : G']$, then $p \leqq M$, and hence there are at most $\pi(M)$ distinct prime divisors of $[G : G']$, where $\pi(M)$ is the number of primes $\leqq M$. Therefore, $[G : G'] \leqq M^{\pi(M)}$ and if we choose $f_n(m) = \max\{m^3, M^{\pi(M)}\}$, where $M = \max\{nm, F(m)\}$, G will satisfy (2) if it does not satisfy (1), (3), or (4) and the theorem is proved.

3. As has already been noted in §1, extra-special p-groups provide examples of arbitrarily large groups satisfying $m(G) = p - 1$ for a fixed prime p, and thus they yield examples of groups which satisfy only (3) of Theorem 2.6.

In this section we construct a series of groups for each prime which will yield examples where only (4) holds in Theorem 2.6. They also provide counter-examples to Corollary 1.5 for non-nilpotent groups. In fact, they show that there is no function h such that if $[G : G'] > h(m(G))$, then G' is abelian. What these groups definitely do not provide is a counter-example to the statement that there exists a function h such that if $[G : G'] > h(m(G))$, then G is solvable. In fact, by Theorem 2.6, this statement would follow if the conjecture that a group having a fixed point-free automorphism of prime power order is necessarily solvable were true.

The construction given below is modeled on G, Higman's construction of the Suzuki 2-group $A(n, \theta)$ in (**1**).

THEOREM 3.1. *Let p be a prime and $n \geqq 3$ an odd integer. Then there exists a p-group $H = H_{n,p}$ satisfying*

(1) $|H| = p^{2n}$, $|H'| = p^n$, $H' = \mathbf{Z}(H)$,

(2) *there exists cyclic $A \subseteq \mathrm{Aut}(H)$ with $\mathbf{C}_H(a) = 1$ for all $a \neq 1$ in A. Also, $|A| = 2^{-t}(p^n - 1)$, where t is defined by $p - 1 = 2^t r$, r being odd,*

(3) $k(H) = 1 + (p^n - 1)(p + 1)$, *and*

(4) *if G is the split extension of H by A, then $k(G) = 2^t(p + 1) + 2^{-t}(p^n - 1)$ and $m(G) = 2^t(p + 1) < p^2$ and $m(G)$ is independent of n.*

Proof. Let $F = \mathrm{GF}(p^n)$ and let H be the subset of $\mathrm{GL}(3, F)$ consisting of matrices of the form

$$\begin{bmatrix} 1 & \alpha & \xi \\ 0 & 1 & \alpha^p \\ 0 & 0 & 1 \end{bmatrix} = (\alpha, \xi),$$

where the ordered pair notation is used as a shorthand for the matrix. Note that $(\alpha, \xi)(\beta, \eta) = (\alpha + \beta, \xi + \eta + \alpha\beta^p)$, and thus H is a group, $1 = (0, 0)$, $|H| = p^{2n}$, and $Z = \{(0, \xi)\}$ is a subgroup with $|Z| = p^n$. Clearly, (α, ξ) and (β, η) commute with each other if and only if $\alpha\beta^p = \beta\alpha^p$, i.e., if and only if $\beta = 0$ or $\alpha/\beta = (\alpha/\beta)^p$. Since $n > 1$, it follows that $Z = \mathbf{Z}(H)$, and since $x \rightarrow x^p$ is an automorphism of F which generates the Galois group of F over its prime field, $\alpha/\beta = (\alpha/\beta)^p$ if and only if $\alpha/\beta \in \mathrm{GF}(p)$, i.e., $\alpha = s\beta$, $0 \leqq s < p$. If $\alpha = s\beta$, then $(\beta, \eta)^s = (\alpha, \zeta) = (\alpha, \xi)(0, \zeta - \xi)$, and thus $\mathbf{C}((\alpha, \xi)) = \langle Z, (\alpha, \xi)\rangle$ if $\alpha \neq 0$. Now $(\alpha, \xi)^p \in Z$; thus, if $\alpha \neq 0$, $|\mathbf{C}((\alpha, \xi))| = p^{n+1}$ and the class containing each non-central element of H has size p^{n-1}. Thus

$$k(H) = |Z| + \frac{|H| - |Z|}{p^{n-1}} = p^n + (p^{2n} - p^n)/p^{n-1} = 1 + (p^n - 1)(p + 1).$$

If we set $p - 1 = 2^t r$ for odd r, then $2^t|(p^n - 1)$ since

$$p^n - 1 = (p - 1)(1 + p + p^2 + \ldots + p^{n-1}).$$

Since n is odd, there is an odd number of terms in the second factor which must therefore be odd and $2^{t+1}(p^n - 1)$. Let λ be a generator of the multiplicative group of F and set $\mu = \lambda^{2^t}$. Since λ has order $p^n - 1$, the order of μ is $2^{-t}(p^n - 1)$. Define the mapping σ: $H \rightarrow H$ by $(\alpha, \xi)^\sigma = (\alpha\mu, \xi\mu^{p+1})$. Then σ is a group automorphism and $(\alpha, \xi)^{\sigma m} = (\alpha\mu^m, \xi\mu^{m(p+1)})$. If σ^m fixes (α, ξ) for $0 < m < 2^{-t}(p^n - 1)$, then since $\mu^m \neq 1$, we have that $\alpha = 0$. If $\mu^{m(p+1)} = 1$, then $2^{-t}(p^n - 1)|m(p + 1)$. We claim, however, that $2^{-t}(p^n - 1)$ and $p + 1$ are relatively prime, for if q is a prime, $q|(p + 1)$, then $p \equiv -1 \bmod q$; thus $p^n \equiv -1 \bmod q$. If $q|2^{-t}(p^n - 1)$, then $0 \equiv p^n - 1 \equiv -2 \bmod q$; thus $q = 2$. However, $2 \nmid 2^{-t}(p^n - 1)$, and this establishes the claim. Thus, $2^{-t}(p^n - 1)|m(p + 1)$ contradicts $0 < m < 2^{-t}(p^n - 1)$ and $\mu^{m(p+1)} \neq 1$ and $\xi = 0$. This establishes (2) of the theorem if $A = \langle\sigma\rangle$.

Clearly, H/Z is abelian; thus $H' \subseteq Z$ and $|H'| = p^s \leqq p^n$. Since H' admits A, we have that $2^{-t}(p^n - 1)|(p^s - 1)$. Since 2^t divides $p^s - 1$ and $2^{-t}(p^n - 1)$

is odd, we have that $(p^n - 1)|(p^s - 1)$; thus $p^n \leqq p^s$, and therefore $H' = Z$ and (1) follows.

Finally, since no $a \in A$, $a \neq 1$ can fix any class of H except $\{1\}$, it follows that the number of classes of G that are contained in H is

$$1 + (p^n - 1)(p + 1)/|A| = 1 + 2^t(p + 1).$$

It is clear that every coset of H $(=G')$ in G except for H itself is a single class and there are $2^{-t}(p^n - 1) - 1$ such cosets. This yields

$$k(G) = 2^t(p + 1) + 2^{-t}(p^n - 1)$$

and

$$m(G) = k(G) - [G : G'] = 2^t(p + 1) \leqq (p - 1)(p + 1) < p^2$$

and the proof is complete.

References

1. G. Higman, *Suzuki 2-groups*, Illinois J. Math. *7* (1963), 79–96.
2. I. M. Isaacs and D. S. Passman, *A characterization of groups in terms of the degrees of their characters*. II, Pacific J. Math., *24* (1968), 467–510.
3. E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante*, Math. Ann. *56* (1903), 671–676.
4. G. Seitz, *Finite groups having only one irreducible representation of degree greater than one*, Proc. Amer. Math. Soc. *19* (1968), 459–461.

University of Chicago,
Chicago, Illinois;
Yale University,
New Haven, Connecticut

https://doi.org/10.4153/CJM-1968-146-3 Published online by Cambridge University Press