

Zeros of irreducible characters of metabelian p - groups

TOM WILDE

ABSTRACT – We show that if χ is an irreducible complex character of a metabelian p - group P , where p is an odd prime, and if $x \in P$ satisfies $\chi(x) \neq 0$, then the order of x divides $|P|/\chi(1)^2$.

MATHEMATICS SUBJECT CLASSIFICATION (2010). 20C15; 20D15.

KEYWORDS. irreducible character, metabelian group, p - group

1. Introduction

All groups in this note are finite. As usual, $\text{Irr}(G)$ denotes the set of irreducible complex characters of the group G , and a p - group is a group whose order is a power of the prime p .

Let P be a p - group. If P has nilpotence class at most 2 and $\chi \in \text{Irr}(P)$, then χ is of central type. That is to say, $\chi(1)^2 = |P : Z(\chi)|$ where $Z(\chi)/\text{Ker}(\chi)$ is the center of $P/\text{Ker}(\chi)$ and consequently, χ vanishes on $P - Z(\chi)$. (See for example Theorem 2.31 and Corollary 2.30 in [1].)

In particular, if $x \in P$ and $\chi \in \text{Irr}(P)$ where P has class at most 2, and if $\chi(x) \neq 0$ then the order of x divides $|P|/\chi(1)^2$. In this note, we prove the following theorem, showing that provided p is odd, this property extends to all metabelian p - groups.

THEOREM 1.1. *Let P be a metabelian p - group, where p is odd. Let $\chi \in \text{Irr}(P)$ and $x \in P$ satisfy $\chi(x) \neq 0$. Then the order of x divides $|P|/\chi(1)^2$.*

Theorem 1.1 improves Theorem A(2) of [3]. The requirement that p be odd is necessary; for example, the dihedral group of order 16 has an irreducible character χ of degree 2, and an element x of order 8, with $\chi(x) \neq 0$. We do not know if it is

necessary to require that P be metabelian. Theorem C in [3] shows that Theorem 1.1 remains true without this requirement, provided the order of P divides p^9 .

2. Preliminary results

Our proof of Theorem 1.1 is via Proposition 2.1 below; this proposition is really our main result. After giving the straightforward proof of Theorem 1.1 from Proposition 2.1, the rest of this section will be taken up with preliminary lemmas. After these preparations, in Section 3, we give the proof of Proposition 2.1.

As usual, if a group H acts via automorphisms on a group A and if $g \in H$ and $\lambda \in \text{Irr}(A)$, then $\lambda^g \in \text{Irr}(A)$ is defined by $\lambda^g(x^g) = \lambda(x)$ for $x \in A$. Also, $C_H(\lambda) = \{g \in H \mid \lambda^g = \lambda\}$, the centralizer of λ in H .

PROPOSITION 2.1. *Let A and H be abelian p -groups, where p is odd, with H acting on A via automorphisms. Let $\lambda \in \text{Irr}(A)$ and set $\psi = \sum_{h \in H} \lambda^h$. If $x \in A$ has $\psi(x) \neq 0$, then the order of x divides $|A|/|H : C_H(\lambda)|$.*

Before working on the proof of Proposition 2.1, we will derive Theorem 1.1. Apart from Proposition 2.1, the main ingredient in the proof below is the standard fact that metabelian groups are normally monomial. (Recall that a group G is normally monomial if for each $\chi \in \text{Irr}(G)$ there is a linear character of a normal subgroup of G that induces χ .)

PROOF OF THEOREM 1.1. We have a metabelian p -group P , where p is odd, and $\chi \in \text{Irr}(P)$ and $x \in P$ satisfying $\chi(x) \neq 0$. Let $K = \text{Ker}(\chi)$ and let q be the order of the image of x in P/K . Then the order of x divides $q|K|$. If $|K| > 1$ then by induction, q divides $|P/K|/\chi(1)^2$, giving the result in this case.

Hence, we can assume χ is faithful. Since P is metabelian, Corollary 2.6 in [2] shows that P has a subgroup A containing the commutator subgroup of P , and such that $\lambda^P = \chi$ for some linear character $\lambda \in \text{Irr}(A)$. Then $A \triangleleft P$ and since χ is faithful, A is abelian. Since $\chi(x) \neq 0$, $x \in A$. Let $H = P/A$, acting via conjugation on A . Since $\chi = \lambda^P$ and $x \in A$, $\chi(x) = \sum_{h \in H} \lambda^h(x)$. Since χ is irreducible, $C_H(\lambda) = 1$. By Proposition 2.1, the order of x divides $|A|/|H| = |P|/|H|^2 = |P|/\chi(1)^2$, as required. \square

In the remainder of this section, we present a sequence of preliminary lemmas. The last two results in this section, Corollary 2.6 and Lemma 2.7, are then used directly in our proof of Proposition 2.1 in Section 3.

We use standard notation except where indicated. If A and H are groups with A abelian and H acting on A via automorphisms, then we regard A as a $\mathbb{Z}H$ -module, and we write A and $\text{Irr}(A)$ multiplicatively with the action of $\mathbb{Z}H$ written exponentially. $\langle X \rangle$ is the group generated by a subset $X \subseteq A$. We say A is a cyclic $\mathbb{Z}H$ -module if it is generated as a $\mathbb{Z}H$ -module by some element $x \in A$, or equivalently, if $A = \langle \{x^h \mid h \in H\} \rangle$. We write $[x, h]$ for x^{h-1} where $x \in A$ and $h \in H$, and $[A, H]$ denotes the commutator submodule; $[A, H] = \langle [a, h] \mid a \in A, h \in H \rangle$. If

$\alpha \in \mathbb{Z}H$ then A^α denotes the group $\{x^\alpha | x \in A\}$. In particular, if $n \in \mathbb{N}$ then A^n is the subgroup consisting of the n^{th} - powers of elements of A . Also $\Omega_n(A)$ denotes the group of elements in A of order dividing n . The field generated by the values of a character ψ is denoted $\mathbb{Q}(\psi)$, and $\bar{\psi}$ denotes the complex conjugate character. Finally, we use ζ_n for $e^{2\pi i/n}$.

Our first lemma was inspired by Problem 3.12 in [1].

LEMMA 2.2. *Suppose A and H are groups with A abelian and H acting on A via automorphisms. Let $\lambda \in \text{Irr}(A)$ and set $\psi = \sum_{h \in H} \lambda^h$. Let $a_1, \dots, a_n \in A$, $n \geq 1$. Then*

$$\psi(a_1)\psi(a_2)\dots\psi(a_n)\bar{\psi}\left(\prod_{i=1}^n a_i\right) = \sum_{g_1, \dots, g_n \in H} \psi\left(\prod_{i=1}^n [a_i, g_i]\right).$$

PROOF. For $a \in A$, $\psi(a) = \sum_{h \in H} \lambda^{h^{-1}}(a) = \sum_{h \in H} \lambda(a^h)$. Hence

$$\psi(a_1)\psi(a_2)\dots\psi(a_n)\bar{\psi}\left(\prod_{i=1}^n a_i\right) = \sum_{h_0, h_1, \dots, h_n \in H} \lambda\left(\prod_{i=1}^n a_i^{h_i}\right) \bar{\lambda}\left(\prod_{i=1}^n a_i^{h_0}\right).$$

Since $H^{n+1} = \{(g_1 g_0, \dots, g_n g_0, g_0) | g_0, \dots, g_n \in H\}$, equivalently

$$\begin{aligned} \psi(a_1)\psi(a_2)\dots\psi(a_n)\bar{\psi}\left(\prod_{i=1}^n a_i\right) &= \sum_{g_0, g_1, \dots, g_n \in H} \lambda\left(\prod_{i=1}^n a_i^{g_i g_0}\right) \bar{\lambda}\left(\prod_{i=1}^n a_i^{g_0}\right) \\ &= \sum_{g_0, g_1, \dots, g_n \in H} \lambda^{g_0^{-1}}\left(\prod_{i=1}^n a_i^{g_i}\right) \\ &= \sum_{g_1, \dots, g_n \in H} \psi\left(\prod_{i=1}^n [a_i, g_i]\right) \end{aligned}$$

as required. \square

DEFINITION 2.3. Let B be a submodule of the $\mathbb{Z}H$ - module A , where H is any group. Then B^\natural is defined as follows:

$$B^\natural = \{b \in B : b^\alpha = 1 \text{ whenever } \alpha \in \mathbb{Z}H \text{ and } A^\alpha \subseteq B\}.$$

Clearly, B^\natural is a $\mathbb{Z}H$ - submodule of B .

LEMMA 2.4. *Suppose A and H are abelian groups with H acting on A via automorphisms. Let $\lambda \in \text{Irr}(A)$ and set $\psi = \sum_{h \in H} \lambda^h$. Let B be a $\mathbb{Z}H$ - submodule of A such that $\psi(v) = 0$ if $v \in [A, H]$ and $v \notin B$. Fix $n \geq 1$, $y_1, \dots, y_n \in B$ and $r_1, \dots, r_n \in \mathbb{Z}$ and define a function Ψ on A as follows:*

$$\Psi(a) = \left(\prod_{i=1}^n \psi(a^{r_i} y_i)\right) \bar{\psi}\left(\prod_{i=1}^n a^{r_i} y_i\right)$$

for $a \in A$. Let $x \in A$ and assume that x generates A as $\mathbb{Z}H$ -module. Then $\Psi(x) = \Psi(xb)$ for $b \in B^\natural$.

PROOF. Let $b \in B^\natural$. Applying Lemma 2.2 with $a_i = (xb)^{r_i}y_i$ shows that

$$\Psi(xb) = \sum_{g_1, \dots, g_n \in H} \psi \left(\prod_{i=1}^n [x^{r_i} b^{r_i} y_i, g_i] \right).$$

Each term in brackets on the right side of this expression is a member of $[A, H]$. By hypothesis, if $v \in [A, H]$ but $v \notin B$ then $\psi(v) = 0$. Since $[b^{r_i}y_i, g_i] \in B$ for each i , a summand on the right can only be nonzero if $\prod_{i=1}^n [x^{r_i}, g_i] \in B$.

For $g_1, \dots, g_n \in H$, let $\alpha(g_1, \dots, g_n) = \sum_{i=1}^n r_i(g_i - 1) \in \mathbb{Z}H$. Since H is abelian, the map from A to A defined by $a \mapsto a^{\alpha(g_1, \dots, g_n)}$ for $a \in A$, commutes with the action of H . Since x generates A as a $\mathbb{Z}H$ -module, it follows that if $x^{\alpha(g_1, \dots, g_n)} \in B$ for particular $g_1, \dots, g_n \in H$, then $A^{\alpha(g_1, \dots, g_n)} \subseteq B$. Hence, we can write the expression above in the following form:

$$\Psi(xb) = \sum_{g_1, \dots, g_n \in H | A^{\alpha(g_1, \dots, g_n)} \subseteq B} \psi \left((xb)^{\alpha(g_1, \dots, g_n)} \prod_{i=1}^n [y_i, g_i] \right).$$

By definition of B^\natural , $b^{\alpha(g_1, \dots, g_n)} = 1$ in every term on the right. Hence $\Psi(xb) = \Psi(x)$ as claimed. \square

LEMMA 2.5. Let A, H, λ, ψ, B and x be as in Lemma 2.4 and additionally assume that $\psi(x) \neq 0$. Then $\psi(xb) \neq 0$ when $b \in B^\natural$ and furthermore the map $\mu : B^\natural \rightarrow \mathbb{C}^\times$ defined by

$$\mu(b) = \frac{\psi(xb)}{\psi(xb^{-1})}$$

is a linear character of B^\natural .

PROOF. First, we apply Lemma 2.4 with $n = r_1 = 1$ and $y_1 = 1$. Comparing the definition of Ψ , then $\Psi(a) = |\psi(a)|^2$ for $a \in A$, so Lemma 2.4 shows that $|\psi(x)|^2 = |\psi(xb)|^2$ for $b \in B^\natural$. In particular, $\psi(xb) \neq 0$ for $b \in B^\natural$, so μ is properly defined, and we also see that $|\mu(b)| = 1$ for $b \in B^\natural$.

To show that μ is a linear character of B^\natural , let $y_1, y_2 \in B^\natural$ and in Lemma 2.4, take $n = 4$ and set

$$r_1 = r_2 = 1; r_3 = r_4 = -1; y_3 = 1; y_4 = (y_1 y_2)^{-1}.$$

Now

$$\Psi(a) = \psi(ay_1)\psi(ay_2)\psi(a^{-1})\psi(a^{-1}y_1^{-1}y_2^{-1})\psi(1)$$

for $a \in A$. By Lemma 2.4, $\Psi(x) = \Psi(xy_1^{-1}y_2^{-1})$. Substituting yields

$$\begin{aligned} & \psi(xy_1)\psi(xy_2)\psi(x^{-1})\psi(x^{-1}y_1^{-1}y_2^{-1})\psi(1) \\ &= \psi(xy_2^{-1})\psi(xy_1^{-1})\psi(x^{-1}y_1y_2)\psi(x^{-1})\psi(1). \end{aligned}$$

Since $y_1, y_2 \in B^{\natural}$, all of the factors are nonzero. On rearrangement, we find

$$\mu(y_1)\mu(y_2) = \frac{\psi(xy_1)}{\psi(xy_1^{-1})} \frac{\psi(xy_2)}{\psi(xy_2^{-1})} = \frac{\psi(x^{-1}y_1y_2)}{\psi(x^{-1}y_1^{-1}y_2^{-1})} = \frac{\bar{\psi}(xy_1^{-1}y_2^{-1})}{\bar{\psi}(xy_1y_2)} = \frac{1}{\bar{\mu}(y_1y_2)}.$$

Since $|\mu(y_1y_2)| = 1$, it follows that $\mu(y_1)\mu(y_2) = \mu(y_1y_2)$, so μ is a linear character of B^{\natural} , as required. \square

COROLLARY 2.6. *Let A, H, λ, ψ, B and x be as in Lemma 2.4 and assume, as in Lemma 2.5, that $\psi(x) \neq 0$. In addition, assume that A and H are p - groups where p is odd, that $\cap_{h \in H} \text{Ker}(\lambda^h) = 1$ and that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\zeta_p)$. Then the exponent of B^{\natural} divides p .*

PROOF. Let $B_0 = (B^{\natural})^p$ and assume for a contradiction that $|B_0| > 1$. Let μ be the linear character of B^{\natural} that was introduced in Lemma 2.5. Clearly $\mu(B^{\natural}) \subseteq \mathbb{Q}(\psi)$, so $\mu(B^{\natural}) \subseteq \mathbb{Q}(\zeta_p)$ and so $B_0 \subseteq \text{Ker}(\mu)$. Since B_0 is a nontrivial $\mathbb{Z}H$ - module and B_0 and H are p - groups, $|C_{B_0}(H)| > 1$. However, for any $b \in C_{B_0}(H)$,

$$\psi(xb) = \sum_{g \in H} \lambda^g(xb) = \sum_{g \in H} \lambda^g(x)\lambda(b) = \psi(x)\lambda(b)$$

so $\mu(b) = \psi(xb)/\psi(xb^{-1}) = \lambda(b)^2$. As p is odd and $B_0 \subseteq \text{Ker}(\mu)$, $C_{B_0}(H) \subseteq \text{Ker}(\lambda)$. Hence $C_{B_0}(H) \subseteq \cap_{h \in H} \text{Ker}(\lambda^h) = 1$, a contradiction. \square

The following lemma supplies a submodule B to use with Corollary 2.6.

LEMMA 2.7. *Let A and H be abelian p - groups with H acting on A via automorphisms. Let the exponent of $[A, H]$ be p^e . If $0 \leq r \leq e$, then A contains a $\mathbb{Z}H$ - submodule B with $\Omega_{p^r}(A) \subseteq B$, such that B^{\natural} has exponent at least $p^{\min(r+1, e-r)}$.*

PROOF. Let $B \supseteq \Omega_{p^r}(A)$ be defined by $B/\Omega_{p^r}(A) = C_{A/\Omega_{p^r}(A)}(H)$. We can assume $r < e$ or the result is trivial. Then $\Omega_{p^r}(A) < A$ and so $B > \Omega_{p^r}(A)$ since A and H are p - groups, but $[B, H] \subseteq \Omega_{p^r}(A)$. Let $C = [A, H]^{p^r}$. We claim that $B \cap C \subseteq B^{\natural}$. If $\alpha \in \mathbb{Z}H$ then since H is abelian, $[a, g]^{\alpha} = [a^{\alpha}, g]$ for all $a \in A$ and $g \in H$, so $[A, H]^{\alpha} = [A^{\alpha}, H]$. Hence if $A^{\alpha} \subseteq B$, then

$$C^{\alpha} = [A, H]^{p^r \alpha} = [A^{\alpha}, H]^{p^r} \subseteq [B, H]^{p^r} = 1.$$

It follows that $B \cap C \subseteq B^{\natural}$ as claimed.

Clearly $\Omega_{p^r}(C) = \Omega_{p^r}(A) \cap C \subseteq B \cap C$. As C has exponent p^{e-r} , $\Omega_{p^r}(C)$ has exponent $p^{\min(r, e-r)}$. If $e-r \leq r$, we can conclude that B^{\natural} has at exponent at least $e-r$ as required. Otherwise, $e-r > r$. Then $C \not\subseteq \Omega_{p^r}(A)$, so $C\Omega_{p^r}(A)/\Omega_{p^r}(A)$ is a nontrivial $\mathbb{Z}H$ - submodule of $A/\Omega_{p^r}(A)$. Since A and H are p - groups, it follows from the definition of B that $B \cap C\Omega_{p^r}(A) > \Omega_{p^r}(A)$. Since $\Omega_{p^r}(A) \subseteq B$, the modular law shows $B \cap C\Omega_{p^r}(A) = (B \cap C)\Omega_{p^r}(A)$. Hence $B \cap C \not\subseteq \Omega_{p^r}(A)$. Since $B^{\natural} \supseteq B \cap C$, we have $B^{\natural} \not\subseteq \Omega_{p^r}(A)$ or in other words, the exponent of B^{\natural} is at least p^{r+1} as required. \square

3. Proof of Proposition 2.1

In this section we give the proof of Proposition 2.1. We need a final standard lemma about roots of unity.

LEMMA 3.1. *Let p be a prime. If $e > 1$ and ζ is a primitive $(p^e)^{\text{th}}$ root of unity, then $\text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\zeta) = 0$.*

PROOF. The Galois group $\text{Gal}(\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p))$ is identified with the integer residues mod p^e that are congruent to 1 mod p . Therefore since $\zeta^p \neq 1$,

$$\text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\zeta) = \sum_{j=0}^{p^{e-1}-1} \zeta^{1+pj} = \zeta \frac{\zeta^{p^e} - 1}{\zeta^p - 1} = 0$$

as required. \square

PROOF OF PROPOSITION 2.1. Let the information (A, H, λ, x) be a counterexample to Proposition 2.1, where A and H are abelian p -groups with H acting on A by automorphisms, $\lambda \in \text{Irr}(A)$ and $x \in A$. Let $\psi = \sum_{h \in H} \lambda^h$, so by hypothesis $\psi(x) \neq 0$. Assume that (A, H, λ, x) has been chosen among counterexamples to Proposition 2.1 to minimize, firstly the field degree $|\mathbb{Q}(\psi) : \mathbb{Q}|$, and secondly $|A|$.

Let p^e be the order of x , and set $p^t = |A|/|H : C_H(\lambda)|$. Proposition 2.1 asserts that $e \leq t$, so we are assuming for a contradiction that $t \leq e - 1$. Note that $\lambda \neq 1$ since Proposition 2.1 holds trivially in that case, and hence also $t \geq 1$, since the $|H : C_H(\lambda)|$ characters that are H -conjugate to λ are all nontrivial irreducible characters of A .

Let B be the $\mathbb{Z}H$ -submodule of A generated by x , and let λ_B and ψ_B be the restrictions of λ and ψ to B . Since there are $|A : B|$ characters of A that extend λ_B , $|C_H(\lambda_B) : C_H(\lambda)| \leq |A : B|$, so $|B|/|H : C_H(\lambda_B)| \leq |A|/|H : C_H(\lambda)| = p^t$. Hence (B, H, λ_B, x) is a counterexample to Proposition 2.1. Since $\mathbb{Q}(\psi_B) \subseteq \mathbb{Q}(\psi)$, our choice of counterexample implies that $A = B$, so A is the cyclic $\mathbb{Z}H$ -module generated by x . In particular, the exponent of A is p^e .

Next, let $K = \bigcap_{h \in H} \text{Ker}(\lambda^h)$ and regard λ and ψ as characters of A/K . The order of $xK \in A/K$ is at least $p^e/|K|$, so $(A/K, H, \lambda, xK)$ is a counterexample to Proposition 2.1 and again by choice of counterexample, it follows that $K = 1$.

Our next objective is to show that $\mathbb{Q}(\psi) = \mathbb{Q}(\zeta_p)$. Firstly, $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\zeta_{p^e})$ since the exponent of A is p^e . Also, if $\lambda_{C_A(H)}$ and $\psi_{C_A(H)}$ are the restrictions of λ and ψ respectively to $C_A(H)$, then $\psi_{C_A(H)} = \psi(1)\lambda_{C_A(H)}$, and $\lambda_{C_A(H)}$ is faithful since $\bigcap_{h \in H} \text{Ker}(\lambda^h) = 1$. Since A and H are p -groups with $|A| > 1$, $|C_A(H)| > 1$, and it follows that $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\psi)$.

As p is odd, $\text{Gal}(\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p))$ is a cyclic p -group. By Galois theory, therefore $\mathbb{Q}(\psi) = \mathbb{Q}(\zeta_{p^l})$ for some l with $1 \leq l \leq e$. We first establish that $l \leq t$, as follows. The distinct Galois conjugate characters ψ^σ , $\sigma \in \text{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})$ each have $|H : C_H(\lambda)|$ linear constituents, and have no pairwise common constituents, so

$$|H : C_H(\lambda)| |\mathbb{Q}(\psi) : \mathbb{Q}| \leq |A|$$

and so $|\mathbb{Q}(\psi) : \mathbb{Q}| \leq p^t$. But $|\mathbb{Q}(\psi) : \mathbb{Q}| = p^{l-1}(p-1)$, so as $p > 2$ it follows that $l \leq t$ as claimed.

To show that in fact $l = 1$, we start from (A, H, λ, x) and construct another counterexample, which we label $(A_1, H_1, \lambda_1, x_1)$, such that $\mathbb{Q}(\psi_1) \subseteq \mathbb{Q}(\zeta_p)$, where $\psi_1 = \sum_{h_1 \in H_1} \lambda_1^{h_1}$. To begin this construction, let $C = \langle \zeta_{p^t} \rangle \subseteq \mathbb{C}^\times$ and extend the action of H to $A \times C$ by letting H act trivially on C . Let S be the Sylow p - subgroup of $(\mathbb{Z}/p^e\mathbb{Z})^\times$ and let $H_1 = H \times S$. Since $t < e$, the exponent of $A \times C$ is p^e , so S has a well - defined action on $A \times C$ via $(a, c)^{k+p^e\mathbb{Z}} = (a^k, c^k)$ for $k \in \mathbb{Z}$, $k \equiv 1(p)$. These actions define an action of H_1 on $A \times C$. Let $\iota : C \rightarrow \mathbb{C}^\times$ be the identity map, regarded as a linear character of C . Since $l \leq t$, it follows that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\iota)$. Define $\lambda_1 = \lambda \times \iota \in \text{Irr}(A \times C)$.

If $a \in \Omega_p(C_A(H))$ then $\lambda(a)$ is a p^{th} - root of unity. Since $t \geq 1$, $\lambda(a) \in C$. Hence, we can define a subgroup $W \subseteq A \times C$ by

$$W = \{(a, \bar{\lambda}(a)) | a \in \Omega_p(C_A(H))\}.$$

Then $W \subseteq C_{A \times C}(H_1) \cap \text{Ker}(\lambda_1)$. Since $C_A(H)$ is cyclic (because $\lambda_{C_A(H)}$ is faithful as noted earlier), $|W| = |\Omega_p(C_A(H))| = p$. Let $A_1 = (A \times C)/W$ be the quotient $\mathbb{Z}H_1$ - module and regard $\lambda_1 \in \text{Irr}(A_1)$.

Recall that $\psi_1 = \sum_{h_1 \in H_1} \lambda_1^{h_1}$. If $a_1 \in A_1$ is the image of $(a, c) \in A \times C$, then

$$\psi_1(a_1) = \sum_{\sigma \in S} \left(c \sum_{h \in H} \lambda(a^h) \right)^\sigma = \text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\psi(a)c) \in \mathbb{Q}(\zeta_p).$$

Hence $\mathbb{Q}(\psi_1) \subseteq \mathbb{Q}(\zeta_p)$. If $\psi(a) \neq 0$, we claim that $\psi_1(a_1) \neq 0$ for some choice of $c \in C$. In other words, we claim there exists $c \in C$ such that $\text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\psi(a)c) \neq 0$. Indeed, since C spans $\mathbb{Q}(\zeta_{p^t})$ over \mathbb{Q} , we may choose (not necessarily uniquely) $b_c \in \mathbb{Q}$ for $c \in C$ such that $1/\psi(a) = \sum_{c \in C} b_c c$. Then

$$|\mathbb{Q}(\zeta_{p^e}) : \mathbb{Q}(\zeta_p)| = \sum_{c \in C} b_c \text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\psi(a)c)$$

so there exists $c \in C$ with $\text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\psi(a)c) \neq 0$, as claimed. As $\psi(x) \neq 0$, we can fix $c \in C$ such that $\psi_1(x_1) \neq 0$, where x_1 is the image of (x, c) in A_1 .

We now have $(A_1, H_1, \lambda_1, x_1)$ with $\mathbb{Q}(\psi_1) \subseteq \mathbb{Q}(\zeta_p)$ and we need to verify that this information constitutes a counterexample to Proposition 2.1.

By construction, $\psi_1(x_1) \neq 0$. We claim that the order of x_1 is p^e . Indeed, x_1 is the image of (x, c) in A_1 and the orders of x and c are respectively p^e and a divisor of p^t , so as $t \leq e - 1$, $(x, c)^{p^{e-1}} = (x^{p^{e-1}}, 1)$. Thus if $(x, c)^{p^{e-1}} \in W$ then $x^{p^{e-1}} \in C_A(H)$ and $\lambda(x^{p^{e-1}}) = 1$. But then $x^{p^{e-1}} \in \cap_{h \in H} \text{Ker}(\lambda^h) = 1$, which is not the case. Hence the order of x_1 is p^e as claimed.

Define t_1 by $p^{t_1} = |A_1|/|H_1 : C_{H_1}(\lambda_1)|$. We will show that $t_1 = t$. If $h \in H$ and $\sigma \in S$ are such that $(h, \sigma) \in C_{H_1}(\lambda_1)$, then since H acts trivially on C , it follows that σ fixes ι , while if $\sigma \in S$ fixes ι , then since $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\iota)$, σ fixes ψ and hence

there exists $h \in H$ with $(h, \sigma) \in C_{H_1}(\lambda_1)$, where h is unique up to multiplication by an element of $C_H(\lambda)$. Therefore, projection $(h, \sigma) \mapsto \sigma$ gives an isomorphism

$$C_{H_1}(\lambda_1)/C_H(\lambda) \cong \text{Gal}(\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\iota)).$$

Hence, we can compute:

$$p^{t_1} = \frac{(|A||C|/|W|)|C_H(\lambda)|p^{e-t}}{|H||S|} = \frac{|A|p^{t-1}|C_H(\lambda)|p^{e-t}}{|H|p^{e-1}} = p^t$$

and so $t_1 = t$, as required. Since $\psi_1(x_1) \neq 0$ and x_1 has order p^e , $(A_1, H_1, \lambda_1, x_1)$ is a counterexample to Proposition 2.1 with $\mathbb{Q}(\psi_1) \subseteq \mathbb{Q}(\zeta_p)$, as promised. Since our original counterexample (A, H, λ, x) was chosen to minimize $|\mathbb{Q}(\psi) : \mathbb{Q}|$ and satisfies $\mathbb{Q}(\psi) \supseteq \mathbb{Q}(\zeta_p)$, it now follows that $\mathbb{Q}(\psi) = \mathbb{Q}(\zeta_p)$.

We can now conclude the proof, working with our original counterexample (A, H, λ, x) and $\psi = \sum_{h \in H} \lambda^h$. Let $X = [A, H]$. Since $|A| > 1$ and A and H are p -groups, $X < A$. Let λ_X and ψ_X be the restrictions of λ and ψ respectively to X . We claim that $C_H(\lambda_X) = C_H(\lambda)$. For suppose $g \in C_H(\lambda_X)$. Then for any $y \in A$,

$$\psi(y)\bar{\lambda}(y) = \sum_{h \in H} \lambda([y, h]) = \sum_{h \in H} \lambda^g([y, h]) = \psi(y)\bar{\lambda}^g(y)$$

so if $\psi(y) \neq 0$ then $\lambda^g(y) = \lambda(y)$. In particular, this holds if $y = x^h$ for $h \in H$. Since A is generated by x as $\mathbb{Z}H$ -module, it follows that $\lambda^g(a) = \lambda(a)$ for all $a \in A$, and so $g \in C_H(\lambda)$, as claimed.

Let $p^r = |X|/|H : C_H(\lambda_X)|$. Since $|X| < |A|$ and $C_H(\lambda_X) = C_H(\lambda)$, $r < t$. Since also $\mathbb{Q}(\psi_X) \subseteq \mathbb{Q}(\psi)$, by our choice of counterexample, Proposition 2.1 holds for (X, H, λ_X, y) for any $y \in X$. Hence ψ vanishes on $X - \Omega_{p^r}(X)$.

Let the exponent of X be p^f . Then $f \leq e$ and we will first consider the possibility that $f = e$. By Lemma 2.7, there exists a $\mathbb{Z}H$ -module B with $\Omega_{p^r}(A) \subseteq B \subseteq A$ such that B^\natural has exponent divisible by $p^{\min(r+1, e-r)}$. But since $\mathbb{Q}(\psi) = \mathbb{Q}(\zeta_p)$, all the conditions of Corollary 2.6 are satisfied by A, H, λ, ψ, B and x . So B^\natural has exponent dividing p . Comparing these conclusions, we have

$$\min(r+1, e-r) \leq 1.$$

However, $r \geq 1$ since λ_X is nontrivial and has $|X|/p^r$ conjugates under the action of H . Thus $e-r \leq 1$. But then $e \leq r+1 \leq t \leq e-1$, a contradiction.

We are left with $f < e$, so $X^{p^{e-1}} = [A^{p^{e-1}}, H] = 1$. Then $D = \langle x^{p^{e-1}} \rangle$ satisfies $D \subseteq C_A(H)$, so $\psi_D = \psi(1)\lambda_D$. Since $\bigcap_{h \in H} \text{Ker}(\lambda^h) = 1$, λ_D is a faithful character of D . Since D is the unique minimal subgroup of $\langle x \rangle$, we see that the restriction of ψ to $\langle x \rangle$ is a sum of faithful linear characters of $\langle x \rangle$. Since $\psi(x) \in \mathbb{Q}(\zeta_p)$,

$$|\mathbb{Q}(\zeta_{p^e}) : \mathbb{Q}(\zeta_p)|\psi(x) = \text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\psi(x)) = \sum_{h \in H} \text{tr}_{\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}(\zeta_p)}(\lambda^h(x))$$

where by the previous sentence, for each $h \in H$, $\lambda^h(x)$ is a primitive $(p^e)^{\text{th}}$ root of unity. Since $e \geq t+1 \geq 2$, Lemma 3.1 shows that $\psi(x) = 0$ contrary to hypothesis. This completes the proof. \square

REFERENCES

- [1] I.M. Isaacs, *Character theory of finite groups*, Academic Press, 1976.
- [2] I.M. Isaacs – D.S. Passman, *Groups whose irreducible representations have degrees dividing p^e* , Illinois J. Math. **8** Issue 3 (1964), pp. 446–457.
- [3] T. Wilde, *Supports of irreducible characters of p - groups*, ArXiv:1307.5780v1.

Received submission date; revised revision date