Jennifer Gensler
Nick Jamesson
Justin Willson

2. Give two proofs of the following claim, one using character theory and one not using character theory. Claim. If $\omega_1, \ldots, \omega_p$ are p-th roots of unity, and $\omega_1 + \cdots + \omega_p = 0$, then these roots of unity are distinct.

Proof. (Proof using character theory.)
Suppose $\omega_1, \ldots, \omega_p$ are p-th roots of unity and $\omega_1 + \cdots + \omega_p = 0$. Let $\rho : \mathbb{Z}_p \to GL_p(\mathbb{C})$ be defined by $1 \mapsto \begin{pmatrix} \omega_1 & & \\ & \ddots & \\ & & \omega_p \end{pmatrix}$. Let $n \in \mathbb{Z}_p$. Then since ρ is a homomorphism we have

$$\begin{aligned} \rho(n) &= \rho(1)^n \\ &= \begin{pmatrix} \omega_1 & & \\ & \ddots & \\ & & \omega_p \end{pmatrix}^n \\ &= \begin{pmatrix} \omega_1^n & & \\ & \ddots & \\ & & \omega_p^n \end{pmatrix} \end{aligned}$$

Let ζ_p denote a primitive p-th root of unity. Note that $\varphi_n : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p)$ defined by $x \mapsto x^n$ is an automorphism for all n with $(n, p) = 1$. Also note that for each i we have $\omega_i = \zeta_p^{k_i}$ for some $0 \leq k_i < p$. So we have $\omega_i \in \mathbb{Q}(\zeta_p)$ for all i. Applying the automorphism φ_n to the given equation $\omega_1 + \cdots \omega_p = 0$ yields $\omega_1^n + \cdots \omega_p^n = 0^n = 0$ for all n such that $(n, p) = 1$. If $n = 0$, then $\omega_1^0 + \cdots + \omega_p^0 = 1 + \cdots + 1 = p$. Therefore, $\chi_\rho = \chi_{\text{Reg}}$.

Let $\rho_i : \mathbb{Z}_p \to \mathbb{C}$ be the irreducible representation defined by $1 \mapsto \omega_i$, for $1 \leq i \leq p$. Note each ρ_i is irreducible since they are linear (have dimension 1). Let χ_i denote the character for each ρ_i. Since ρ is diagonal we have $\rho = \oplus_{i=1}^p \rho_i$. Therefore, $\chi_\rho = \chi_1 + \cdots + \chi_p$. Since $\chi_\rho = \chi_{\text{Reg}}$ and $\chi_{\text{Reg}} = \sum n_i \chi_i'$ where $n_i = \dim \chi_i'$ and χ_i' denotes irreducible characters, we must have by the uniqueness of decompositions that each character χ_i is distinct and so each ω_i is distinct. □

Proof. (Proof not using character theory.) Let ω be a primitive p-th root of unity. Then for $1 \leq i \leq p$, we know $\omega_i = \omega^{n_i}$ for some $0 \leq n_i < p$. This gives

$$\omega^{n_1} + \cdots + \omega^{n_p} = 0.$$

By combining terms whose exponents are equal (i.e. if $n_i = n_j$ we get $\omega^{n_i} + \omega^{n_j} = 2\omega^{n_i}$), we obtain the following:

$$a_1\omega^{n_{i_1}} + \cdots + a_k\omega^{n_{i_k}} = 0$$

where $1 \leq a_j \leq p$ for each $1 \leq j \leq k$ and each of the exponents is distinct. Then ω is a root of the polynomial $a_1x^{n_{i_1}} + \cdots + a_kx^{n_{i_k}}$, which is a polynomial of degree $< p$ that lies in $\mathbf{Q}[x]$. Note we may assume without loss of generality that $n_{i_1} < \cdots < n_{i_k}$ and if $n_{i_1} = 0$ our polynomial becomes $a_1 + a_2x^{n_{i_2}} + \cdots + a_kx^{n_{i_k}}$ instead. But the minimal polynomial of ω over $\mathbf{Q}$ is $1 + x + \cdots + x^{p-1}$. Since minimal polynomials are unique up to constants, we

Jennifer Gensler
Nick Jamesson
Justin Willson

must have $a_1 x^{n_{i_1}} + \cdots + a_k x^{n_{i_k}} = 1 + x + \cdots + x^{p-1}$. This shows that the exponents are distinct and hence the ω_i's are distinct.

□