Group Theory- HW3, Problem 1
Ian Gossett

Problem. Give two proofs of the following claim, one using character theory and one not using character theory.

Claim. Let $p \in \mathbb{Z}$ be prime. If $\omega_1, \omega_2, ..., \omega_p$ are pth roots of unity and $\omega_1 + \omega_2 + ... + \omega_p = 0$, then these roots of unity are distinct.

Proof 1. (without character theory) Recall that the pth roots of unity can be written as $\omega^{m_1}, \omega^{m_2}, ..., \omega^{m_p}$ where $\omega \neq 1$ is a pth root of unity and $m_j \in \{0, 1, ..., p-1\}$ for each $j \in \{1, 2, ..., p\}$. Also recall that the minimal polynomial over $\mathbb{Q}$ for ω is $f(x) = \sum_{i=0}^{p-1} x^i$.

Let $\{a_1, a_2, ..., a_p\} \subseteq \mathbb{Z}_{\geq 0}$ with $\sum_{i=1}^{p} a_i = p$, and define $g(x) = \sum_{i=1}^{p} a_i x^{m_j}$. To prove the claim, it suffices to show that if $g(\omega) = 0$, then $a_j = a_k$ for all $j, k \in \{1, 2, ..., p\}$. To see this, note that if $a_i = a_j = a$ for some $a \in \mathbb{Z}_{\geq 0}$, then $\sum_{i=1}^{p} a_i = pa = p$, and hence $a = 1$. Thus $g(\omega)$ is the sum of p distinct roots of unity, each occurring exactly once.

To this end, suppose that $g(\omega) = 0$. Then ω is a root of $g \in \mathbb{Q}[x]$, and since f is the minimal polynomial for ω over $\mathbb{Q}$, we must have that f divides g. Hence, $\deg(f) \leq \deg(g)$, and since $m_j \leq p-1$ for each j, this implies that $\deg(f) = \deg(g)$. Thus, it must be the case that $f = ag$ for some constant a, so $a_i = a_j = a$ for each i, j, and the result is proved.

■

Proof 2. (with character theory) Suppose that $\omega_1, \omega_2, ..., \omega_p$ are pth roots of unity, $\omega_1 + \omega_2 + ... + \omega_p = 0$, and define the representation $\rho : \mathbb{Z}_p \to GL_p(\mathbb{C})$ by

$$1 \mapsto \begin{pmatrix} \omega_1 & & & & \\ & \omega_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \omega_p \end{pmatrix}.$$

Then

$$\rho(j) = \begin{pmatrix} \omega_1 & & & & \\ & \omega_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \omega_p \end{pmatrix}^j = \begin{pmatrix} (\omega_1)^j & & & & \\ & (\omega_2)^j & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & (\omega_p)^j \end{pmatrix},$$

and that ρ is a representation follows trivially.

By assumption, $\mathrm{tr}(\rho(1)) = \chi_\rho(1) = 0$. Note that for each $j \in \{1, 2, ..., p-1\}$, there exists an automorphism $\alpha_j : \mathbb{C} \to \mathbb{C}$ with the property that $\alpha_j(\omega_i) = (\omega_i)^j$ (such an α_j can be attained by extending $\sigma_j \in \mathrm{Gal}\,(\mathbb{Q}[\omega]/\mathbb{Q})$ with $\sigma_j(\omega_i) = (\omega_i)^j$) and we have $\chi_\rho(j) = \alpha_j(\chi_\rho(1)) = \alpha_j(0) = 0$.

Consequently,

$$\chi_\rho(j) = \begin{cases} p & \text{if } j = 0 \\ 0 & \text{if } j \neq 0 \end{cases},$$

which we recognize as the regular character, and hence ρ is the regular representation.

Recall that $\{\phi_k : \mathbb{Z}_p \to \mathbb{C} : \psi_k(1) = \omega^k, k \in \{0, 1, ..., p-1\}\}$ is a complete set of (pairwise inequivalent) irreducible representations of $\mathbb{Z}_p$, and that the regular representation decomposes uniquely into a direct sum of the irreducible representations of $\mathbb{Z}_p$, each occurring in the sum with multiplicity equal to its degree.

Since the ith diagonal entry of $\rho(j)$ is $\rho_i(j)$ where $\rho_i : \mathbb{Z}_p \to \mathbb{C}$ defined by $\rho_i(1) = \omega_i$ is a degree 1 irreducible representations of $\mathbb{Z}_p$, we see that the representation determined by ρ is the direct sum of the representations determined by ρ_i. Thus, the ρ_i must correspond to the p distinct irreducible representations, and $\omega_i = \rho_i(1) \neq \rho_j(1) = \omega_j$ if $i \neq j$. Hence, $\omega_1, \omega_2, .., \omega_p$ are distinct pth roots of unity.

■