Andrew Doumont
Dan Lyness
Calum Shearer

3. Show that if $\chi \in \mathrm{Irr}(G)$ and $\chi(1) > 1$, then $\chi(g) = 0$ for some $g \in G$.

[Hints:

(a) Use Row orthogonality to deduce that $1 = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2$.

(b) Use the arithmetic-geometric mean inequality to show $\prod_{g \in G} |\chi(g)|^2 < 1$.

(c) Employ a norm argument to show that the norm, ν of $\prod_{g \in G} |\chi(g)|^2 < 1$ is an integer satisfying $0 \leq \nu < 1$.]

Proof. Row Orthogonality tells us that $1 = \langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2$. This sum is the average of $|G|$ terms, so the arithemetic-geometric mean inequality tells us that:

$$1 = \sum_{g \in G} |\chi(g)|^2 \geq \left(\prod_{g \in G} |\chi(g)|^2 \right)^{\frac{1}{|G|}}$$

However, we only have equality if all terms in the sum/ product are equal, i.e. $|\chi(g)| = |\chi(1)| = \chi(1)$ for all $g \in G$. But in this case row orthogonality gives $1 = \frac{|G|}{|G|}\chi(1)$, so $\chi(1) = 1$, which is contrary to the assumption $\chi(1) > 1$. Hence in this case, the arithemetic-geometric mean inequality is strict inequality.

As $\prod_{g \in G} |\chi(g)|^2 \geq 0$, this and the above immediately implies that

$$1 > \prod_{g \in G} |\chi(g)|^2 \geq 0$$

Now, $\chi(g)$ is an algebraic integer for all $g \in G$. As $\overline{\chi}$ is the character of the dual representation of the representation associated to χ, $\overline{\chi(g)}$ must also be an algebraic integer. Hence $\chi(g)\overline{\chi(g)} = |\chi(g)|^2$ is an algebraic integer, as algebraic integers form a ring. This also implies that $\prod_{g \in G} |\chi(g)|^2$ is an algebraic integer.

To show: this quantity is also rational.

If $|G| = n$, we have that $\chi(g)$ is the sum of $n-$th roots of unity, and hence are members of the field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. Then $\mathbb{Q}(\zeta_n)$ has Galois group given by automorphisms $\sigma_k(\zeta_n) = \zeta_n^k$, where k is coprime to n and σ_k is extended to make it a field automorphism that fixes $\mathbb{Q}$.

Now, $\chi(g^k) = tr(\rho(g^k)) = tr(\rho(g)^k) = tr(diag(\lambda_1, \dots, \lambda_m)^k) = tr(diag(\lambda_1^k, \dots, \lambda_m^k)) = \sum_{j=1}^m \lambda_j^k$, where the λ_j are the eigenvalues of $\rho(g)$ and $m = \chi(1)$. Then as $\chi(g)$ is precisely the sum of the eigenvalues λ_j, have that $\sigma_k(\chi(g)) = \sigma_k(\sum_{j=1}^m \lambda_j) = \sum_{j=1}^m \lambda_j^k = \chi(g^k)$. Now observe that $\sigma_k \left(\prod_{g \in G} \chi(g) \right) = \prod_{g \in G} \sigma_k(\chi(g)) = \prod_{g \in G} \chi(g^k)$ by the above and the fact that σ_k is a field automorphism.

Andrew Doumont
Dan Lyness
Calum Shearer

Claim 1. *When considered as a function between underlying sets, $\alpha_k \colon G \to G, g \to g^k$ is a bijection if* $\gcd(k, |G|) = 1$*, where G is any finite group.*

Proof. As G is finite, once we verify surjectivity then injectivity and hence bijectivity immediately follow. Since $\gcd(k, |G|) = 1$, we can write $1 = mk + n|G|$ for some $m, n \in \mathbb{N}$. Then given any $g \in G$, we have that: $\alpha_k(g^m) = g^{mk} = g^{1-n|G|} = g(g^{|G|})^{-n} = g$ (as raising an element to the order of the group always gives the identity). Hence $g \in \mathrm{Im}(\alpha_k)$. As $g \in G$ arbitrary, we have the claim. □

From this, we have that $G^k = G$, and so $\prod_{g \in G} \chi(g^k) = \prod_{h \in G^k} \chi(h) = \prod_{g \in G} \chi(g)$. So we have shown that $\sigma_k \left(\prod_{g \in G} \chi(g) \right) = \prod_{g \in G} \chi(g)$. As $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) =: H$ was arbitrary, we have that $\prod_{g \in G} \chi(g) \in \mathbb{Q}(\zeta_n)^H = \mathbb{Q}$, as by the Galois correspondence, the subfield fixed by all elements of the Galois group is precisely the base field. Hence from this we have that our original quantity, $\prod_{g \in G} |\chi(g)|^2 = \left| \prod_{g \in G} \chi(g) \right|^2 \in \mathbb{Q}$ as $\mathbb{Q}$ is closed under taking absolute value and squaring.

Hence $\prod_{g \in G} |\chi(g)|^2 \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$, so is an integer greater than 0 and strictly less than 1, and hence is 0. But the only way for $\prod_{g \in G} |\chi(g)|^2$ to equal 0 is if $|\chi(g)|^2 = 0$ for at least one $g \in G$, and $|\chi(g)|^2 = 0 \iff |\chi(g)| = 0 \iff \chi(g) = 0$, so we're done.

□