November 26, 2024

Problem Set 10 Solutions

Exercise 1. Consider the group algebra $\mathbb{C}[G]$ of a finite group G. We know from the course that the the regular representation $\mathbb{C}[G]_{reg}$ decomposes as a direct sum

$$\mathbb{C}[G] = \bigoplus_{i=1}^{r} V_i^{\oplus \dim V_i}$$

where $\{V_i\}_{i=1}^r$ are the inequivalent irreducible representations of G. In particular, $\mathbb{C}[G]_{reg}$ always contains the trivial subrepresentation of the group with multiplicity 1. The following exercise gives a description of the complement to the trivial representation in $\mathbb{C}[G]_{reg}$ in the basis of group elements.

(a) Define a subspace N in $\mathbb{C}[G]$ by

$$N = \left\{ \sum_{g \in G} a_g g \ : \ a_g \in \mathbb{C}, \ \sum_{g \in G} a_g = 0 \right\}.$$

Show that $N \subset \mathbb{C}[G]$ is a $\mathbb{C}[G]$-submodule in the left regular module $\mathbb{C}[G]$ over itself and find its dimension.

(b) Consider the quotient module, $M = \mathbb{C}[G]/N$. Find its dimension, introduce a basis and describe its structure.

Solution 1. (a) First we check that $N \subset \mathbb{C}[G]$ is a vector subspace. Indeed, if we have $a = \sum_{g\in G} a_g g \in N$ and $b = \sum_{g \in G} b_g g \in N$, then

$$a + sb = a = \sum_{g\in G} a_g g + s \sum_{g \in G} b_g g = \sum_{g\in G} (a_g + s b_g) g$$

with $\sum_{g\in G}(a_g + sb_g) = \sum_{g\in G} a_g + s\sum_{g\in G} b_g = 0$, so that $a + sb \in N$. Now consider an action of $\mathbb{C}[G]$ on an element $a \in N$. Since $\mathbb{C}[G]$ is a vector space with basis $\{g\}_{g\in G}$, it suffices to consider the action of an arbitrary group element $x \in G$. We have

$$xa = x \sum_{g\in G} a_g g = \sum_{g \in G} a_g (xg) = \sum_{g\in G} a_{x^{-1}g} g \in N,$$

since left multiplication by x^{-1} permutes the elements of G and so $\sum_{g\in G} a_{x^{-1}g} = \sum_{g \in G} a_g = 0$. So N is a submodule of $\mathbb{C}[G]$ with respect to the left multiplication. Since all coefficients in the expression $\sum_{g\in G} a_g g$ but one can be chosen to be arbitrary complex numbers, and the last coefficient is uniquely determined by the condition $\sum_{g\in G} a_g = 0$, the dimension of N is $|G| - 1$.

(b) Consider the $\mathbb{C}[G]$-module $M = \mathbb{C}[G]/N$. Let 1 denote the neutral element of G. For any element in $\mathbb{C}[G]$ we can write uniquely $b = t \cdot 1 + \sum_{g \in G} a_g g$, where $\sum_{g\in G} a_g g \in N$. Then $M \simeq \mathbb{C} \cdot 1$ in this presentation. Let us compute the action of a group element $x \in G$ on M:

$$xb = x(t \cdot 1 + \sum_{g\in G} a_g g) = x \left((t + a_1) \cdot 1 + a_{x^{-1}} x^{-1} + \sum_{g \neq x^{-1}, g \neq 1} a_g g \right) =$$

$$= (t + a_1)x + a_{x^{-1}} \cdot 1 + \sum_{g\neq 1, g \neq x} a_{x^{-1}g} g = t \cdot 1 + \left[(a_{x^{-1}} - t) \cdot 1 + (t + a_1)x + \sum_{g \neq 1, g\neq x} a_{x^{-1}g} g \right] = t \cdot 1 + n,$$

where n is the sum of the terms in the square brackets. Since $\sum_{g\in G} a_g = 0$, we have that $n \in N$. Therefore, for any element t in one-dimensional $\mathbb{C}[G]$-module M, we have $x \cdot t = t$ for any $x \in G$, and therefore M is the trivial $\mathbb{C}[G]$-module.

Remark: Of course V_0 is also a subrepresentation in $\mathbb{C}[G]_{reg}$, that is spanned by $\sum_{g\in G} g$.

Exercise 2. A group is nilpotent if its ascending central series terminates in the whole group. The ascending central series is the sequence of normal subgroups

$$1 = Z_0 \subset Z_1 \subset \ldots \subset Z_i \subset \ldots,$$

where $Z_{i+1} = \{x \in G : xyx^{-1}y^{-1} \in Z_i \ \forall y \in G\}$. In particular, Z_1 is the center of G.

(a) Show that a nilpotent group is solvable.

(b) Give an example of a solvable group that is not nilpotent.

(c) Show that a group of order p^k, where p is a prime, is nilpotent.
(This is another way to show that a group of order p^k is solvable – an easy special case of Burnside's theorem).

Solution 2. (a) If the ascending central series terminates in a whole group, then we have a sequence of normal subgroups,

$$1 = Z_0 \subset Z_1 \subset \ldots \subset Z_{k-1} \subset Z_k = G,$$

such that for all $x, y \in Z_{i+1}/Z_i$, we have $\{xyx^{-1}y^{-1} = 1\}$, and so Z_{i+1}/Z_i is abelian. Therefore, by definition G is solvable.

(b) The center of $G = S_3$ is trivial, and therefore its ascending central series terminates at the first step. However, S_3 contains a normal subgroup $C_3 \simeq \{1, (123), (132)\}$. We have a sequence of normal subgroups with abelian factors,

$$1 \subset C_3 \subset S_3,$$

so that S_3 is solvable. Alternatively, S_3 is solvable as a group of order $6 = 2 \cdot 3$ by Burnside's theorem.

(c) A group G of order p^k, $k > 1$, has a nontrivial center of order a power of p, because otherwise the class equation

$$p^k = |Z| + \sum_{i>1} |C_i|$$

where each $|C_i|, i > 1$ is divisible by p, cannot be satisfied. Then consider the group G/Z. It has order p^m with $m < k$ and the same argument applies. By induction, we can construct an ascending central series that terminates with the whole group.

Exercise 3. Show that if V is an irreducible complex representation of a finite group G, and $\mathrm{dimV} > 1$, then there is an element $g \in G$ such that $\chi_V(g) = 0$. *Hint:*

(a) Use orthonormality of characters to show that the arithmetic mean of the numbers $|\chi_V(g)|^2$ for $g \neq e$ is strictly less than 1. Deduce that

$$\beta = \prod_{g \neq e} |\chi_V(g)|^2 < 1.$$

(b) Consider the map $G \to G$ defined by $g \to g^j$, where j is any positive integer such that $\mathrm{gcd(j, |G|)} = 1$. Show that it is a bijection, and deduce that it leaves the number β fixed.

(c) Show that $\beta \in \mathbb{Z}[\xi]$, where $\xi = e^{2\pi i/|G|}$ is the $|G|$-th root of unity. Use (b) to show that $\beta = 0$.

Solution 3. (a) We have,

$$(\chi_V, \chi_V) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)\overline{\chi_V(g)} = \frac{1}{|G|} \sum_{g \in G} |\chi_V(g)|^2 = 1.$$

Then

$$\sum_{g \neq e} |\chi_V(g)|^2 = |G| - \mathrm{dim}^2(\mathrm{V}) \quad \Longrightarrow \quad \frac{1}{|\mathrm{G}| - 1} \sum_{\mathrm{g} \neq \mathrm{e}} |\chi_\mathrm{V}(\mathrm{g})|^2 = \frac{|\mathrm{G}| - \mathrm{dim}^2(\mathrm{V})}{|\mathrm{G}| - 1} < 1.$$

Set $m = |G| - 1$. Then by the arithmetic-geometric mean inequality we have for these numbers that their geometric mean is also strictly less than 1,

$$\sqrt[m]{\prod_{g \neq e} |\chi_V(g)|^2} \leq \frac{1}{m} \sum_{g \neq e} |\chi_V(g)|^2 < 1 \quad \Longrightarrow \quad \beta = \prod_{g \neq e} |\chi_V(g)|^2 < 1.$$

(b) The map $g \to g^j$ maps $e \to e \in G$. If $g \neq e$, then $g^j \neq e$ because g generates a cyclic subgroup in G whose order must divide $|G|$, and gcd(j, |G|) = 1. Suppose now that $h \neq e, g \neq e$ and $k = h^j = g^j \in G$. Then k generates a cyclic subgroup $K = \{e, k, k^2, \ldots k^{s-1}\}$ in G, such that $K \subset H = \{e, h, h^2, \ldots h^{n-1}\} \subset G$, where the positive integers s and n divide $|G|$. Then $h^{js} = k^s = e$, and therefore $js = nt$ for some positive integer t. Then $s = nt/j$, and since gcd(n, j) = 1, s is a multiple of n. Since $K \subset H$, we have $m = s$ and $K = H$. By the same argument, $K = H'$, the cyclic subgroup generated by g. Therefore, the cyclic subgroups generated by g and h are the same, and in particular $h = g^k$, for some k, such that $g^{kj} = g^j$. Then $g^{(k-1)j} = e$, and $k - 1$ is divisible by the order of the group generated by g. Therefore, $h = g^{k-1}g = eg = g$.

(c) All characters of G are sums of roots of unity of orders that divide $|G|$, and so are their conjugates. Therefore, $\beta = \prod_{g \neq e} |\chi_V(g)|^2$ is a polynomial in $\xi = e^{2\pi i/|G|}$ with integer coefficients. Let $\beta = a_0 + \sum_{i=1}^{|G|-1} a_i \xi^i$. By (b), the map $g \to g^j$ leaves β unchanged and in each character it acts by sending ξ to ξ^j. We have $\beta \in \mathbb{Q}(\xi)$ the extension of the filed $\mathbb{Q}$ by the roots of unity of order $|G|$. The Galois group of this extension is isomorphic to $(\mathbb{Z}/|G|\mathbb{Z})^*$, which is exactly generated by the automorphisms $\xi \to \xi^j$ with j coprime to $|G|$. The elements stabilized by the Galois group of $\mathbb{Q}(\xi)$ are exactly $\mathbb{Q}$. Since $\beta \in \mathbb{Q}$ is an algebraic integer, we conclude that $\beta \in \mathbb{Z}$. Therefore, $0 \leq \beta < 1$ and finally $\beta = 0$.