Advanced Algebra I

GROUP ALGEBRA

Recall that by a regular representation of $G$, we consider a vector space with basis $\{e_s\}_{s \in G}$. Let $\mathbb{C}[G]$ be the vector space with basis $\{e_s\}_{s \in G}$. One can have a natural ring structure on $\mathbb{C}[G]$ as following:

$$\sum_{s \in G} a_s e_s + \sum_{s \in G} b_s e_s = \sum_{s \in G} (a_s + b_s) e_s,$$

$$(\sum_{s \in G} a_s e_s)(\sum_{t \in G} b_t e_t) = \sum_{s, t} a_s b_t e_{st} = \sum_{u \in G} (\sum_{s, t} a_s b_t) e_u.$$

We call $\mathbb{C}[G]$ the group algebra of $G$.

We claim that $\mathbb{C}[G] \cong \prod_{i=1}^{r} M_{n_i}(\mathbb{C})$.

Where $r$ is the number of conjugacy classes of $G$ and $n_i$ is the degree of each irreducible representation.

First of all, the irreducible representation $\rho_i : G \to GL(W_i)$ induces an algebra homomorphism $\tilde{\rho}_i : \mathbb{C}[G] \to End(W_i) \cong M_{n_i}(\mathbb{C})$ by $\tilde{\rho}_i(\sum_{s \in G} a_s e_s) = \sum_s a_s \rho_i(g)$. Hence one has

$$\tilde{\rho} : \mathbb{C}[G] \to \prod_{i=1}^{r} End(E_i) \cong \prod_{i=1}^{r} M_{n_i}(\mathbb{C}).$$

We first claim the $\tilde{\rho}$ is surjective. Suppose not, then there is a linear relation on the images. It follows that there is a relation on the coefficients of $\rho_i$. In particular, there is a linear relation on $\chi_i$. By the orthogonal property, this is impossible. Hence $\tilde{\rho}$ is surjective. However, they have the same dimension. Hence $\tilde{\rho}$ is an isomorphism.

**Remark 0.1.** $\mathbb{C}[G]$ is abelian if and only if $G$ is abelian.

Our next goal it to determine the center $Z(\mathbb{C}[G])$. In order to check $x = \sum a_s e_s$ is in center or not, we need to check for all $t \in G$,

$$x = \sum_{s \in G} a_s e_s = e_t^{-1} x e_t = \sum_{s \in G} a_s e_{t^{-1}st} = \sum_{s \in G} a_{ts^{-1}} e_s.$$

Note that $t^{-1}st$ is conjugate to $s$. Thus, it’s equivalent to have $a_s = a_{s'}$ for all $s'$ conjugate to $s$.

A special case is that the above equation holds for $e_c := \sum_{\sigma \in c} e_\sigma$, where $c$ is a conjugacy class. Moreover, by our computation above, it’s indeed that

$$Z(\mathbb{C}[G]) = \{ \sum_{i=1}^{r} a_i e_{c_i} | a_i \in \mathbb{C}, c_i \text{ runs through all conjugacy classes} \}.$$
Example 0.2. Let $G = S_3$. Then the center has a basis $e_{(1)}, e_{(12)} + e_{(13)}, e_{(123)} + e_{(132)}$

By viewing the isomorphism $\tilde{\rho}$, one sees that if $u = \sum a_se_s \in Z(\mathbb{C}[G])$, then $\tilde{\rho}(u)$ is of the form $\lambda_iI$ on the irreducible representation $V_i$. The value $\lambda$ can be computed. Note that the coefficient $a_s$ actually gives a class function on $G$ because $a_s = a_{s'}$ for $s, s'$ in the same conjugate class. We write it as $a^G$. By averaging process, one has $\tilde{\rho}_i = \sum_{s \in G} a_s \rho_i(s)$ linear transformation on $V_i$. Thus one has

$$\lambda_i = \frac{1}{d_i} \text{tr}(\sum_{s \in G} a_s \rho_i(s)) = \frac{1}{d_i} \sum a_s \chi_i(s).$$

Theorem 0.3. Keep notation as before, then one has $d_i | g$.

To prove this result, we need some facts on integral extension and algebraic integers.

Remark 0.4. (1) Let $R$ be a commutative ring, one can view it as a $\mathbb{Z}$-module. An element $x \in R$ is said to be integral over $\mathbb{Z}$ if $x$ satisfies a monic integral polynomial in $\mathbb{Z}[x]$.

(2) In a commutative ring $R$, the elements which are integral over $\mathbb{Z}$ forms a subring of $R$.

(3) If $R = \mathbb{C}$, then subring of elements which are integral over $\mathbb{Z}$ is called ring of algebraic integers, denoted $\mathbb{A}$.

(4) $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Remark 0.5. The character $\chi(s)$ is an algebraic integer for all $\chi$ and all $s \in G$. This is because $\chi$ is sum of eigenvalues of a representation $\rho$. However, the eigenvalues are root of unity which are algebraic integers.

Proposition 0.6. Let $u = \sum a_se_s \in Z(\mathbb{C}[G])$ such that $a_s \in \mathbb{A}$. Then $u$ is integral over $\mathbb{Z}$.

Proof. Since $Z(\mathbb{C}[G])$ is generated by $e_c$. Let $c_1, ..., c_r$ be all the conjugacy classes and let $a_i := a_{s_i}$ for some $s_i \in c_i$. We first consider $R := \oplus_{i=1}^r \mathbb{Z}e_{c_i}$. It’s clear that $R$ is a subring of $Z(\mathbb{C}[G])$ which is finitely generated over $\mathbb{Z}$. Now let $M = \mathbb{Z}[a_1, ..., a_r]$. Since $a_i$ is integral over $\mathbb{Z}$, it follows that $M$ is a finite $\mathbb{Z}$-module. One checks that $\mathbb{Z}[u] \subset \oplus_{i=1}^r Me_{c_i}$. Hence $u$ is integral over $\mathbb{Z}$. □

Proof of the theorem. For each $i$, take $u = \sum_{s \in G} \chi(s^{-1})e_s$. It’s clear that $u \in Z(\mathbb{C}[G])$. By the previous Proposition, one has that $u$ is integral over $\mathbb{Z}$.

Note that one has natural ring homomorphism $\omega_i : Z(\mathbb{C}[G]) \to \mathbb{C}$,
by sending $u$ to $\lambda_i$ the multiple of its $i$-component. It follows that the homomorphic image $\lambda_i$ is an algebraic integer. One has now

$$\lambda_i := \frac{1}{d_i} \sum \chi_i(s^{-1})\chi_i(s) = \frac{g}{d_i} < \chi_i, \chi_i > = \frac{g}{d_i}.$$

Hence $\lambda_i \in \mathcal{A} \cap \mathbb{Q} = \mathbb{Z}$. It follows that $d_i | g$. \qed