6. ORTHONORMALITY

§6.1. Class Functions

A class function from a group $G$ to $\mathbb{C}$ is a map $f:G \to \mathbb{C}$ such that conjugate elements have the same value. The most important examples are characters. But while the set of characters is closed under addition and multiplication it is not closed under subtraction and so it does not form a ring. Class functions, on the other hand, do form a ring – in fact they form an algebra over $\mathbb{C}$. We denote the set of class functions on $G$ by $\text{CF}(G)$.

Clearly the dimension of $\text{CF}(G)$, as a vector space over $\mathbb{C}$, is the number of conjugacy classes. We now make $\text{CF}(G)$ into an inner product space by defining:

$$\langle \chi_1 \mid \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} (g \chi_1)(g^{-1} \chi_2) = \frac{1}{|G|} \sum_{g \in G} g \chi_1 \overline{g \chi_2}.$$  

Recall that in an inner product space the length of a vector $v$ is $\langle v \mid v \rangle$, that two vectors are orthogonal if their inner product is zero, and an orthonormal basis is one where the vectors are mutually orthogonal of unit length.

Example 1: The following table give three class functions on $S_3$:

<table>
<thead>
<tr>
<th>class</th>
<th>$\Omega_1$</th>
<th>$\Omega_2$</th>
<th>$\Omega_3$</th>
<th>$\Omega_4$</th>
<th>$\Omega_5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>1</td>
<td>6</td>
<td>8</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>-17</td>
<td>2.5</td>
<td>$\pi$</td>
<td>$\frac{1}{4}i$</td>
<td>$\omega$</td>
</tr>
<tr>
<td>e_1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>e_2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The rather stupid class function 0 is included just to show how general a class function can be. The class functions $e_1$, $e_2$ are part of what we might call the standard basis for $\text{CF}(S_3)$. But note that while they’re orthogonal, they don’t have unit length since, for example, $\langle e_1 \mid e_1 \rangle = \frac{1}{24}$ and $\langle e_2 \mid e_2 \rangle = \frac{1}{4}$. Of course we could multiply them by suitable scalars to get an orthonormal basis, but this so-called “standard basis” isn’t very useful.

§6.2. Orthogonality

Theorem 1: Let $\rho$, $\sigma$ be irreducible representations of the finite group $G$ over $\mathbb{C}$ on the vector spaces $U$, $V$ respectively and let $\phi:U \to V$ be a linear transformation. Then $\alpha = \sum_{x \in G} (x \rho)\phi(x^{-1} \sigma)$ is a $\mathbb{C}G$-module homomorphism: $U_\rho \to V_\sigma$.

Proof: Let $g \in G$. Then $(g \rho)\alpha = \sum_{x \in G} (g \rho)(x \rho)\phi(x^{-1} \sigma) = \sum_{h \in G} (h \rho)\phi(h^{-1} \sigma)(g \sigma) = \alpha(g \sigma)$. putting $h = gx$. So if $u \in U_\rho$, $(ug)\alpha = (u\alpha)g$. Extend by linearity.
Theorem 2: If $\rho$, $\sigma$ are inequivalent irreducible representations over $C$ and $\phi: U \rightarrow V$ is linear then: $\sum_{g \in G} (g\rho)(\phi(g^{-1}\sigma)) = 0$.

If $\rho = \sigma$ then it is $\begin{pmatrix} |G| \cdot \text{tr} \phi \\ \deg \rho \end{pmatrix} I$.

Proof: By Schur’s Lemma, $\sum_{g \in G} (g\rho)(\phi(g^{-1}\sigma)) = 0$ if $\rho$, $\sigma$ are inequivalent and $\lambda I$, for some $\lambda$, if $\rho = \sigma$. In the latter case $\lambda \cdot \deg \rho = \text{tr} \sum_{g \in G} (g\rho)(\phi(g^{-1}\rho)) = \sum_{g \in G} \text{tr}[(g\rho)(\phi(g\rho)^{-1})] = \sum_{g \in G} \text{tr} \phi = |G| \cdot \text{tr} \phi$.

Theorem 3: If $\rho$ and $\sigma$ are irreducible matrix representations of $G$, over $C$, of degrees $m$, $n$ respectively, then for all $i$, $j$, $s$, $t$:

$$\sum_{g \in G} (g\rho)_{ij}(g^{-1}\sigma)_{st} = \begin{cases} 0 & \text{if } \rho \text{ and } \sigma \text{ are inequivalent} \\ \frac{|G|}{\deg \rho} & \text{if } \rho = \sigma \text{ and } i = t \text{ and } j = s \end{cases}$$

Proof: $\sum_{g \in G} (g\rho)_{ij}(g^{-1}\sigma)_{st}$ is the $i$-th component of $\sum_{g \in G} (g\rho)E_{js}(g^{-1}\sigma)$ where $E_{js}$ is the $m \times n$ matrix with 1 in the $j$-$s$ position and 0’s elsewhere.

§6.3. Orthogonality of Characters

Theorem 4: The irreducible characters of $G$ over $C$ form an orthonormal basis for $\text{CF}(G)$.

Proof: Let $\chi$ and $\theta$ be characters corresponding to the irreducible representations above. Then if $\rho$ and $\sigma$ are inequivalent:

$$\langle \chi | \theta \rangle = \frac{1}{|G|} \sum_{g \in G} g\chi^* g\theta = \frac{1}{|G|} \sum_{g \in G} (g\chi)(g^{-1}\theta) = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} (g\rho)_i (g^{-1}\sigma)_j = \frac{1}{|G|} \sum_{i,j} \sum_{g \in G} (g\rho)_i (g^{-1}\sigma)_j = 0.$$ 

Let $\chi$ be the character corresponding to the irreducible representation $\rho$ of degree $n$. Thus:

$$\langle \chi | \chi \rangle = \frac{1}{|G|} \sum_{i,j} \sum_{g \in G} (g\rho)_i (g^{-1}\rho)_j = \frac{1}{|G|} \sum_{i,j} \sum_{g \in G} (g\rho)_i (g^{-1}\rho)_j = \frac{1}{|G|} \sum_{i,j} \deg \rho = 1.$$ 

Theorem 5: If $\chi_{ij}$ is the $i$-$j$ entry in the character table for $G$ then:

$$\sum_{k} h_k X_{ik} X_{jk} = \delta_{ij} |G| \quad \text{and} \quad \sum_{i} \chi_{ik} \overline{\chi}_{ij} = \frac{\delta_{ij}}{h_i} |G|.$$ 

Proof: The first follows from above. Hence $\begin{pmatrix} \chi_{ik} \end{pmatrix}$ is a Hermitian matrix and hence so is its transpose.

Theorem 6: Every normal subgroup is the intersection of the kernels of irreducible representations that contain it.

Proof: By orthogonality the intersection of the kernels of irreducible representations is 1. If $H$ is a normal subgroup of $G$ the irreducible representations of $G/H$ induce irreducible representations of $G$. The kernels that contain $H$ are of the form $K/H$ where $K$ is a kernel for $G$. Thus the intersection of such kernels $= H$. 

34
It follows that the normal subgroups of \( G \) are recoverable from its character table, since \( g \in \ker \rho \iff g\chi = \deg \chi \).

**Theorem 7:** The intersection of the kernels of the linear representations is \( G' \).

**Proof:** If \( \rho \) is linear, \( G/\ker \rho \) is abelian so \( G' \leq \ker \rho \).

An irreducible representation \( \rho \) of \( G \) induces an irreducible representation of \( G/\ker \rho \).

If \( G' \leq \ker \rho \) then \( G/\ker \rho \) is abelian so \( \rho \) is linear.

**Corollary:** The number of linear characters of \( G \) is \( |G/G'| \).

**Theorem 8:** If \( \chi \) is the character of an irreducible representation of \( G \) then \( \deg \chi \) divides \( |G/Z(G)| \).

**Proof:** Case I: \( \rho \) faithful.

Right multiplication by an element of \( Z(G) \) permutes the conjugacy classes.

Define \( \Gamma_1, \Gamma_2 \) equivalent if \( \Gamma_1 z = \Gamma_2 \) for some \( z \in Z(G) \).

Suppose \( \Gamma z = \Gamma \) for some \( 1 \neq z \in Z(G) \). Then \( z\rho = \lambda I \) for some \( \lambda \neq 1 \) and \( \Gamma \chi = (\Gamma z) \chi = \lambda \cdot \Gamma \chi \) whence \( \Gamma \chi = 0 \).

\[
|G| = \sum \Gamma |\Gamma \chi| \Gamma \chi
\]

Terms where \( \Gamma \) is equivalent to fewer than \( |Z(G)| \) classes are 0.

So \( |G/Z(G)| = \sum \Gamma |\Gamma \chi| \Gamma \chi \)

where the sum is over a set of representative classes.

Now for each \( \Gamma \),

\[
|\Gamma\chi/\deg \chi \in Z^*. \quad \text{So } |G/Z(G)|/\deg \chi \in Z^* \cap Q = Z.
\]

**Case II:** \( K = \ker \rho > 1 \).

\( \deg \chi \) divides \( |G/K)/Z(G/K)| \)

\( = |G/K)/(Y/K)| = |G/Y \) which divides \( |G/Z(G)| \) where \( Y/K = Z(G/K) \) and \( Z(G)K \leq Y \).

§6.4. Groups of Order \( p^aq^b \)

**Theorem 9:** Let \( \rho \) be a representation of \( G \) of degree \( n \) with character \( \chi \). Suppose \( g \in G \) has \( h \) conjugates where \( \gcd(h, n) = 1 \). Then either \( g\chi = 0 \) or \( g\rho \in Z(G\rho) \).

**Proof:** For some \( r, s \in Z, 1 = rh + sn \) so \( \frac{g\chi}{n} = r\left(\frac{h(g\chi)}{n}\right) + s(g\chi) \in Z^* \). Let \( g \) have order \( N \) and let \( \omega = e^{2\pi i/N} \). Then \( g\chi \) is a sum \( n \) powers of \( \omega \) and so \( \left| \frac{g\chi}{n} \right| \leq 1 \).

The image of \( \frac{g\chi}{n} \) under any automorphism of \( Q[\omega] \) will have the same minimum polynomial over \( Q \) as \( \frac{g\chi}{n} \) itself and so will be an algebraic integer. Thus taking the product over all automorphisms, \( \theta \), of \( Q[\omega] \), \( \prod \left(\frac{(g\chi)^\theta}{n}\right) \in Z^* \).

By Galois Theory \( \prod (g\chi)^\theta \in Q \) and so \( \prod \left(\frac{(g\chi)^\theta}{n}\right) \in Q \cap Z^* = Z \).
Suppose \( g \rho \not\in Z(G\rho) \). Then \( \left| \frac{g\chi}{n} \right| < 1 \), because if \( \left| \frac{g\chi}{n} \right| = 1 \), all the eigenvalues of \( g \rho \) are equal and so \( g \rho \) is a scalar linear transformation in which case it lies in \( Z(G\rho) \).

Hence \( \prod \left( \frac{(g\chi)0}{n} \right) < 1 \) and so is zero.

**Theorem 10:** Groups of order \( p^aq^b \) are soluble (where \( p, q \) are primes).

**Proof:** Let \( G \) be a minimal counter-example. That is, \(|G| = p^aq^b\) but \( G \) is not soluble. Clearly \( G \) is a non-abelian simple group and so \( Z(G\rho) = 1 \) for any non-trivial irreducible representation \( \rho \).

Let \( P \) be a Sylow \( p \)-subgroup and let \( 1 \neq g \in Z(P) \). Then \( P \leq C_G(g) \) and so the number of conjugates of \( g \) in \( G \) is a multiple of \( q \).

Let \( A \) be the set of irreducible characters of \( G \) whose degree is a multiple of \( q \) and let \( B \) be the set of non-trivial characters of \( G \) whose degree is coprime to \( q \).

If \( \Phi \) is the regular character of \( G \) then:

\[
0 = g\Phi = \sum_{\chi} (\deg \chi)(g\chi) = 1 + \sum_{\chi \in A} (\deg \chi)(g\chi) + \sum_{\chi \in B} (\deg \chi)(g\chi)
\]

\[
= 1 + \sum_{\chi \in A} (\deg \chi)(g\chi) = 1 + qz \text{ for some } z \in \mathbb{Z}'.
\]

Hence \( \frac{-1}{q} \in \mathbb{Q} \cap \mathbb{Z}^* = \mathbb{Z} \), a contradiction.

A **Hall subgroup** of \( G \) is a subgroup \( H \) such that the order of \( H \) is coprime to its index. If \( \Pi \) is any set of primes a Hall \( \Pi \)-subgroup is one where the prime divisors of \(|H|\) all lie in \( \Pi \). Hall subgroups are a generalisation of Sylow subgroups. However, while Sylow \( p \)-subgroups exist for all primes \( p \), a Hall \( \Pi \)-subgroup may not exist for some set of primes \( \Pi \).

For example \( A_5 \) has no Hall \( \Pi \)-subgroup if \( \Pi = \{3, 5\} \), that is, no subgroup of order 15.

**Theorem 11:** A finite group is soluble if and only if it has a Hall \( \Pi \)-subgroup for every set of primes \( \Pi \).

Theorem 10 follows easily from Theorem 11, but in fact requires Theorem 10 in its proof. So this is yet another theorem of finite group theory that needs representation theory in its proof.