6. ORTHONORMALITY

§6.1. Orthogonality

Theorem 1: Let ρ, σ be irreducible representations of the finite group G over ℂ on the vector spaces U, V respectively and let ϕ:U→V be a linear transformation. Then $\alpha = \sum_{x \in G} (x\rho)\phi(x^{-1}\sigma)$ is a ℂG-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 ρ, σ are inequivalent irreducible representations over ℂ and ϕ:U→V is linear then: $\sum_{g \in G} (g\rho)\phi(g^{-1}\sigma) = 0$.

If ρ = σ then it is $\left(\frac{|G|.\text{tr }\phi}{\deg \rho}\right) I$.

Proof: By Schur's Lemma, $\sum_{g \in G} (g\rho)\phi(g^{-1}\sigma) = 0$ if ρ, σ are inequivalent, and

λI, for some λ, if ρ = σ.

In the latter case $\lambda.\deg\rho = tr\sum_{g\in G}(g\rho)\phi(g^{-1}\rho) = \sum_{g\in G} tr[(g\rho)\phi(g\rho)^{-1}] = \sum_{g\in G} tr\phi = |G|.tr\phi$.
✋☺

Theorem 3: If ρ and σ are irreducible matrix representations of *G*, over ℂ, of degrees *m*, *n* respectively, then for all *i*, *j*, *s*, *t*:

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

Proof: $\sum_{g\in G}(g\rho)_{ij}(g^{-1}\sigma)_{st}$ is the i-t 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. ✋☺

§6.2. Orthogonality of Characters

Theorem 4: The irreducible characters of G over ℂ form an orthonormal basis for CF(G).

Proof: Let χ and θ be characters corresponding to the irreducible representations above.

Then if ρ and σ are inequivalent:

$$\langle\chi|\theta\rangle = \frac{1}{|G|}\sum_{g\in G} g\chi\ \overline{g\theta} = \frac{1}{|G|}\sum_{g\in G}(g\chi)(g^{-1}\theta) = \frac{1}{|G|}\sum_{g\in G}\sum_{i}(g\rho)_{ii}\sum_{j}(g^{-1}\sigma)_{jj}$$

$$= \frac{1}{|G|}\sum_{i,j}\sum_{g\in G}(g\rho)_{ii}(g^{-1}\sigma)_{jj} = 0 \cdot$$

Let χ be the character corresponding to the irreducible representation ρ of degree *n*. Thus:

$$\langle \chi | \chi \rangle = = \frac{1}{|G|} \sum_{i,j} \sum_{g \in G} (g\rho)_{ii} (g^{-1}\rho)_{jj} = = \frac{1}{|G|} \sum_{i} \sum_{g \in G} (g\rho)_{ii} (g^{-1}\rho)_{ii} =$$

$$\frac{1}{|G|} \sum_{i} \frac{|G|}{\deg \rho} = 1.$$

Theorem 5: If χ_{ij} is the *i-j* entry in the character table for G then:

$$\sum_k h_k \chi_{ik} \overline{\chi_{jk}} = \delta_{ij} |G| \text{ and } \sum_k \chi_{ki} \overline{\chi_{kj}} = \frac{\delta_{ij}}{h_i} |G|.$$

Proof: The first follows from above. Hence $\left(\frac{\chi_{ij}}{\sqrt{h_j}} \right)$ 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 is H.

It follows that the normal subgroups of G are recoverable from its character table, since g ∈ kerρ if and only if gχ = degχ. ✋☺

Theorem 7: The intersection of the kernels of the linear representations is G′.

Proof: If ρ is linear, G/kerρ is abelian so G′ ≤ kerρ.

An irreducible representation ρ of G induces an irreducible representation of G/kerρ.

If G′ ≤ kerρ then G/kerρ is abelian so ρ is linear. ✋☺

Corollary: The number of linear characters of *G* is |G/G′|.

Theorem 8: If χ is the character of an irreducible representation of G then degχ divides |G/Z(G)|.

Proof: Case I: ρ faithful.

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

Define Γ_1, Γ_2 to be equivalent if $\Gamma_1 z = \Gamma_2$ for some z ∈ Z(G).

Suppose Γz = Γ for some 1 ≠ z ∈ Z(*G*).

Then zρ = λI for some λ ≠ 1 and Γχ = (Γz)χ = λ.Γχ whence Γχ = 0.

Hence $|G| = \sum_{\Gamma} |\Gamma| . \Gamma\chi . \overline{\Gamma\chi}$

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

So $|G/Z(G)| = \sum_{\Gamma} |\Gamma| . \Gamma\chi . \overline{\Gamma\chi}$ where the sum is over a set of representative classes.

Now for each Γ, |Γ|.Γχ/degχ ∈ ℤ*.

So |G/Z(G)|/degχ ∈ ℤ* ∩ 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 $Z(G)K \leq Y$. ✋☺

§6.3. Groups of Order $p^a q^b$

Theorem 9: Let ρ be a representation of G of degree n with character χ. Suppose $g \in G$ has h conjugates where $\mathrm{GCD}(h, n) = 1$. Then either $g\chi = 0$ or $g\rho \in Z(G\rho)$.

Proof: For some $r, s \in \mathbb{Z}$, $1 = rh + sn$ so $\frac{g\chi}{n} = r\left(\frac{h(g\chi)}{n}\right) + s(g\chi) \in \mathbb{Z}^*$.

Let g have order N and let $\omega = e^{2\pi i/N}$.

Then $g\chi$ is a sum n powers of ω and so $\left|\frac{g\chi}{n}\right| \leq 1$.

The image of $\frac{g\chi}{n}$ under any automorphism of $\mathbb{Q}[\omega]$ will have the same minimum polynomial over $\mathbb{Q}$ as $\frac{g\chi}{n}$ itself and so will be an algebraic integer.

Thus taking the product over all automorphisms, θ, of $\mathbb{Q}[\omega]$, $\Pi\left(\frac{(g\chi)\theta}{n}\right) \in \mathbb{Z}^*$.

By Galois Theory $\Pi(g\chi)\theta \in \mathbb{Q}$ and so $\Pi\left(\frac{(g\chi)\theta}{n}\right) \in \mathbb{Q} \cap \mathbb{Z}^* = \mathbb{Z}$.

Suppose $g\rho \notin Z(G\rho)$. 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 $\Pi\left(\frac{(g\chi)\theta}{n}\right) < 1$ and, being a non-negative integer, it is zero, ✋☺

Theorem 10: Groups of order $p^a q^b$ are soluble (where p, q are primes).

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

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 Φ is the regular character of G then:

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

$$= 1 + \sum_{\chi \in A} (\deg\chi)(g\chi) = 1 + qz$$

for some $z \in \mathbf{Z}^*$.

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 Π is any set of primes a Hall Π-subgroup is one where the prime divisors of |H| all lie in Π. Hall subgroups are a generalisation of Sylow subgroups. However, while Sylow *p*-subgroups exist for all primes p, a Hall Π-subgroup may not exist for some set of primes Π. For example A_5 has no Hall Π-subgroup if Π = {3, 5}, that is, no subgroup of order 15.

Theorem 11: A finite group is soluble if and only if it has a Hall Π-subgroup for every set of primes Π. ✋

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.