Frobenius Divisibility, part 2

Theorem: $|G| = n$, φ irreducible, $\dim \varphi = d$

$\Longrightarrow d \mid n$

Recap: $T_g := \sum_{x \in Cl(g)} \varphi_g \in Hom(V,V)$ $\quad g \in G$

s.t $T_g = \lambda_g I$, $\quad \lambda_g \in \mathbb{C}$

Set R = subgroup of $(\mathbb{C}, +)$

generated by $\{ \underline{\zeta^i} \lambda_g \mid 0 \le i < n, g \in G \}$

$\zeta = e^{2\pi i/n}$

Showed: $\frac{n}{d} \in R$.

WTS: $R \cap \mathbb{Q} = \mathbb{Z}$. $\Rightarrow \frac{n}{d} \in \mathbb{Z}$

Claim 1: R is a subring of $\mathbb{C}$, $1 \in R$

Idea: show $\zeta^i \lambda_g \cdot \zeta^j \lambda_h \in R$

$$\zeta^{i+j} \underbrace{\lambda_g \lambda_h}$$

$$\zeta^{i+j} = \zeta^k, \quad 0 \le k < n$$

I'll show: $\boxed{\lambda_g \lambda_h = \sum_{x_i}' m_{x_i} \lambda_{x_i}, \quad m_{x_i} \in \mathbb{Z}}$

will show: R is closed under mult.

$$\lambda_e = 1 \in R.$$

since $T_g = \lambda_g I$, it suffices to show

Lemma: $T_g T_h = \sum_{x_i}' m_{x_i} T_{x_i}$, $m_{x_i} \in \mathbb{Z}$

$\{x_i\}$ - set of representatives of conjugacy classes in G

Proof:

$$T_g T_h = \sum_{u \in Cl(g)}' \varphi_u \sum_{v \in Cl(h)}' \varphi_v$$

$$= \sum_{u \in Cl(g)} \sum_{v \in Cl(h)} \varphi_{uv}$$

$$T_g T_h = \sum_{u \in Cl(g)}' \sum_{v \in Cl(h)}' \varphi_{uv}$$

$x = uv$

$$T_g T_h = \sum_{x \in G}' m_x \varphi_x \quad , m_x \geq 0$$

$m_x = |M_x|, \quad M_x = \{ (u,v) \in Cl(g) \times Cl(h) \mid uv = x \}$

<u>Claim</u>: x, y conjugate $\Rightarrow$ $m_x = m_y$

$$M_x \longrightarrow M_y \qquad y = axa^{-1}$$

$$(u,v) \longmapsto (aua^{-1}, ava^{-1})$$

is a bijection of sets

$$\Rightarrow \quad T_g T_h = \sum_{x_i}' m_{x_i} \cdot T_{x_i}$$

$\Rightarrow$ R subring of $\mathbb{C}$, $\quad 1 = \lambda_e \in R.$

$(R, +)$ is finitely generated $(\{ S^{-1} \lambda_g \})$

and torsion free $(R \leq (\mathbb{C}, +))$

$\Rightarrow$ $(R, +) \cong \mathbb{Z}^N$, $\quad N \geq 1$

$1 \in R \implies \mathbb{Z} \subseteq R \cap \mathbb{Q}$

Suppose $\alpha = \frac{a}{b} \in R \cap \mathbb{Q}$, $a, b \in \mathbb{Z}$, $b \neq 0$

Let $F : R \to R$, $F(r) := \alpha r$ (R is a ring)

homomorphism of abelian groups

$R \simeq \mathbb{Z}^N$, can choose a $\mathbb{Z}$ basis $B = \{e_1, \dots, e_N\}$ of R

$$F(e_j) = \sum_{i=1}^{N} c_{ij} e_i, \quad c_{ij} \in \mathbb{Z}$$

$$([F]_B = C = (c_{ij}))$$

$F(r) = \alpha r$, $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$

$$a e_j = b \alpha e_j = b F(e_j) = b \sum_i c_{ij} e_i = \sum_i (b c_{ij}) e_i$$

linear indep of $B \implies a = b c_{jj} \implies \frac{a}{b} = c_{jj} \in \mathbb{Z}$.

coeff of e_j