Algebraic Integers

An algebraic integer α is a complex number which is solution to integer monic polynomial, i.e., $\exists\, c_0, \dots, c_{n-1} \in \mathbb{Z}$ for some n s.t. $\alpha^n + \sum_{i=0}^{n-1} c_i \alpha^i = 0$

Prop. ① Algebraic integers form a subring of $\mathbb{C}$:
closed under addition, subtraction, multiplication.
② $\{\text{Rational numbers}\} \cap \{\text{algebraic integers}\} = \mathbb{Z}$

Ex. · Roots of unity: solutions to $t^n - 1 = 0$

· $\chi_V(g)$ is algebraic integer for all $g \in G$ and rep. V of G

Prop. Suppose for all integers m coprime to $|G|$, and all $g \in G$ that g is conjugate to g^m. Then $\chi_V(g) \in \mathbb{Z}$ for all $g \in G$, reps. V.

Pf. Suffices to show $\chi_V(g) \in \mathbb{Q}$.
Let L be field gen. by $\mathbb{Q}$ and a primitive $|G|^{th}$ root of unity ω. For every m coprime to $|G|$, there is an automorphism σ_m of L given by $\omega \to \omega^m$, and
$x \in L$ belongs to $\mathbb{Q} \iff \sigma_m(x) = x \;\; \forall$ coprime m.

$$\sigma_m(\chi_V(g)) = \chi_V(g^m) \xRightarrow{\text{assumption}} \chi_V(g) \in \mathbb{Q}. \qquad \square$$

Ex. Every character of S_n is integer-valued.
Pick m coprime to $n! \Rightarrow m$ coprime to $1, \dots, n$.
$\sigma \in S_n$. need: σ^m has same cycle type as σ.
mth power of an i-cycle is still an i-cycle, so
$\sigma \sim \sigma^m$ for all $\sigma \in S_n$.

Let $d_1, \ldots d_c$ be dim's of irred. reps of G.

We showed that $d_1^2 + \cdots + d_c^2 = |G|$. <u>Goal</u>: $d_i \mid |G| \ \forall i$.

If $\mathbb{k}$ commutative ring, definition of $\mathbb{k}[G]$ still makes sense:
$\mathbb{k}[G]$ is free $\mathbb{k}$ module w/ basis $\{e_g \mid g \in G\}$ and $e_g e_h = e_{gh}$.

<u>Lemma</u>. For $x = \sum_{g \in G} \alpha_g e_g \in \mathbb{Z}[G]$ $(\alpha_g \in \mathbb{Z})$ and rep. V of G,
the eigenvalues of $\sum_{g \in G} \alpha_g \rho_V(g)$ are algebraic integers.

<u>Pf</u> Consider the integer span of powers $\{x, x^2, x^3, \ldots\}$.
Subgroup of finitely generated abelian group is again finitely generated $\Rightarrow$ some power of x can be expressed as linear combination of lower powers.

$\Rightarrow$ integer monic polynomial $p(t)$ s.t. $p(x) = 0$.

$\Rightarrow$ If λ eigenvalue of $\sum_{g \in G} \alpha_g \rho_V(g)$, Then $p(\lambda) = 0$

$\Rightarrow$ λ is algebraic integer. $\square$

<u>Thm</u> (Burnside). $\dim V$ divides $|G|$ for each irred. rep. V of G.

<u>Pf</u>. Let $\gamma_1, \ldots, \gamma_c$ be conj. classes of G.
For $i = 1, \ldots, c$, define $f_i \in CF(G)$ by $f_i(g) = \begin{cases} 1 & \text{if } g \in \gamma_i \\ 0 & \text{else} \end{cases}$.

<u>Lemma</u>. Let $\rho: G \to GL(V)$ be rep, $f \in CF(G)$. Define

$$\rho_f = \sum_{g \in G} f(g)\rho(g) \quad \text{linear operator on } V.$$

If V is irreducible, then ρ_f is scalar $= \lambda \cdot \mathrm{id}_V$ where

$$\lambda = \frac{|G|}{\dim V} (f, \overline{\chi_V})_G.$$

Apply w/ $f = f_i$: $\rho_{f_i} = \sum_{g \in \gamma_i} \rho(g)$ is scalar $\lambda_i \cdot \mathrm{id}_V$,

$$\lambda_i = \frac{|G|}{\dim V}(f_i, \overline{\chi_V})_G = \frac{\cancel{|G|}}{\dim V}\frac{1}{\cancel{|G|}}\sum_{g\in\gamma_i}\chi_V(g) = \frac{|\gamma_i|}{\dim V}\chi_V(\gamma_i)$$

Previous lemma $\Rightarrow$ λ_i algebraic integers

$$\Rightarrow \sum_{i=1}^{c}\underbrace{\lambda_i}_{\text{algebraic integer}}\overline{\chi_V(\gamma_i)} = \frac{1}{\dim V}\sum_{i=1}^{c}|\gamma_i|\chi_V(\gamma_i)\overline{\chi_V(\gamma_i)}$$

$$= \frac{1}{\dim V}\sum_{g\in G}\chi_V(g)\overline{\chi_V(g)} = \frac{|G|}{\dim V}(\chi_V, \chi_V)_G$$

$$= \frac{|G|}{\dim V} \in \mathbb{Q} \Rightarrow \frac{|G|}{\dim V} \in \mathbb{Z}$$

$\Rightarrow$ dim V divides $|G|$ $\square$