Algebraic Integers

An algebraic integer $\alpha$ is a complex number which is a solution to an integer monic polynomial, i.e., $\exists c_0, \ldots, c_n \in \mathbb{Z}$ for some $n \in \mathbb{N}$ such that $\alpha^n + \sum_{i=0}^{n-1} c_i \alpha^i = 0$.

**Prop. 1** Algebraic integers form a subring of $\mathbb{C}$.

Closed under addition, subtraction, multiplication.

**Prop. 2** $\{\text{Rational numbers}\} \cap \{\text{algebraic integers}\} = \mathbb{Z}$

**Ex.** Roots of unity: solutions to $\alpha^n - 1 = 0$.

- $\chi_V(g)$ 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 $\omega$. For every $m$ coprime to $|G|$, there is an automorphism $\Gamma_m$ of $L$ given by $\omega \mapsto \omega^m$, and $x \in L$ belongs to $\mathbb{Q} \iff \Gamma_m(x) = x \forall$ coprime $m$.

$$\Gamma_m(\chi_V(g)) = \chi_V(g^m) \Rightarrow \chi_V(g) \in \mathbb{Q}. \quad \square$$

**Ex.** Every character of $G_n$ is integer-valued.

Pick $m$ coprime to $n! \Rightarrow m$ coprime to $1, \ldots, n$.

$g \in G_n$. need: $g^m$ has same cycle type as $g$.

$m$th power of an $i$-cycle is still an $i$-cycle, so $\sigma \sim \sigma^m$ for all $\sigma \in G_n$. 


let $d_1, \ldots, d_c$ be dims of irreducible reps of $G$.

We showed that $d_1^2 + \ldots + d_c^2 = |G|$. Goal: $d_i | |G| \forall i$.

If $k$ commutative ring, definition of $k[G]$ still makes sense:

$k[G]$ is free $k$-module w/ basis $\{e_g \mid g \in G\}$ and $e_g e_h = e_{gh}$.

Lemma. For $x = \sum_{g \in G} x_g e_g \in k[G]$ ($x_g \in k$) and rep. $V$ of $G$,

the eigenvalues of $\sum_{g \in G} x_g \rho_V(g)$ are algebraic integers.

Proof. 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 $\lambda$ eigenvalue of $\sum_{g \in G} x_g \rho_V(g)$, then $p(\lambda) = 0$.

$\Rightarrow \lambda$ is algebraic integer. \(\square\)

(Burnside). $d_i | |G|$ divides $|G|$ for each irreducible rep. $V$ of $G$.

Proof. Let $Y_1, \ldots, Y_c$ be conj. classes of $G$.

Let $Y_i$. Let $V_i$ be irreducible reps of $Y_i$.

For $i = 1, \ldots, c$, define $f_i \in CF(G)$ by $f_i(g) = 1$ if $g \in Y_i$.

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

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

If $V$ is irreducible, then $\rho f$ is scalar $= \lambda \cdot id_V$ where

$\lambda = \frac{|G|}{\dim V} \sum_{g \in V} \overline{(f, \overline{\rho(g)})}$.

Hence w/ $f = f_i$: $\rho f_i = \sum_{g \in Y_i} \rho(g)$ is scalar $\lambda_i \cdot id_V$, where
\[ \lambda_i = \frac{|G|}{\dim V} \langle f_i, X_V \rangle = \frac{|G|}{\dim V} - \frac{1}{|G|} \sum_{g \in G} X_V(g) = \frac{|G|}{\dim V} \chi_V(x_i) \]

Previous lemma \( \Rightarrow \lambda_i \) algebraic integers

\[ \Rightarrow \sum_{i=1}^{ \text{algebraic integer} } \lambda_i X_V(x_i) = \frac{1}{\dim V} \sum_{i=1}^{c \in \mathbb{Q}} \chi_V(x_i) \overline{\chi_V(x_i)} = \frac{|G|}{\dim V} \sum_{g \in G} X_V(g) X_V(\overline{g}) = \frac{|G|}{\dim V} \langle X_V, X_V \rangle \]

\[ \Rightarrow \frac{|G|}{\dim V} \in \mathbb{Q} \Rightarrow \frac{|G|}{\dim V} \in \mathbb{Z} \]

\[ \Rightarrow \dim V \text{ divides } |G| \]

\(\square\)