Algebraic Integers

Defn: We say $\lambda \in \mathbb{C}$ is an algebraic integer if λ is an eigenvalue of a matrix with integer entries (alternatively, if λ is the root of a monic polynomial with integer coefficients).

Examples: 1) $n \in \mathbb{Z}$: eigenvalue of $[n]$
· root of $x-n$

2) $\sqrt{2}$: eigenvalue of $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$
· root of x^2-2

3) $\zeta = e^{\frac{2\pi i}{n}}$, $n \in \mathbb{Z}^+$: eigenvalue of $\begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$ ($n \times n$ matrix)
· root of $x^n - 1$.

Let $\mathbb{A}$ denote the set of algebraic integers

Thm: If $\lambda, \mu \in \mathbb{A}$, then $\lambda\mu$, $\lambda+\mu \in \mathbb{A}$.

Pf: Let A and B be integer valued matrices such that:
$A\vec{u} = \lambda\vec{u}$ for some $\vec{u} \in \mathbb{C}^m$,
$B\vec{v} = \mu\vec{v}$ for some $\vec{v} \in \mathbb{C}^n$.
Let $\vec{e}_1, \dots, \vec{e}_m$ and $\vec{f}_1, \dots, \vec{f}_n$ be the standard bases of $\mathbb{C}^m$ and $\mathbb{C}^n$. Then define $A \otimes B : \mathbb{C}^m \otimes \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^n$ by
$(A \otimes B)(\vec{e}_i \otimes \vec{f}_j) = (A\vec{e}_i) \otimes (B\vec{f}_j)$
and extending linearly. Then
$(A \otimes B)(\vec{u} \otimes \vec{v}) = (\lambda\vec{u}) \otimes (\mu\vec{v}) = (\lambda\mu)(\vec{u} \otimes \vec{v})$
and
$(A \otimes I_n + I_m \otimes B)(\vec{u} \otimes \vec{v}) = \lambda(\vec{u} \otimes \vec{v}) + \mu(\vec{u} \otimes \vec{v}) = (\lambda+\mu)(\vec{u} \otimes \vec{v})$.
Thus, $\lambda\mu$ and $\lambda+\mu$ are algebraic integers. □

Cor: If χ is a character of a group G, and $g \in G$, then $\chi(g) \in \mathbb{A}$.

Pf: We have seen that $\chi(g)$ is the sum of roots of unity, and each root of unity is an algebraic integer. □

Prop: If $\lambda \in \mathbb{Q}$ and $\lambda \in \mathbb{A}$, then $\lambda \in \mathbb{Z}$.

Pf: Suppose $\lambda \in \mathbb{Q} - \mathbb{Z}$. (We will show $\lambda \notin \mathbb{A}$.) Then $\lambda = \frac{r}{s}$ where $(r,s) = 1$ and $s \neq \pm 1$. Let p be a prime such that p divides s. Let A be an $n \times n$ integer entry matrix. Then sA has all entries divisible by p, so $\det(sA - rI_n) = (-r)^n + mp$ for some $m \in \mathbb{Z}$. Since $p \nmid r$, $\det(sA - rI_n) \neq 0$, and so $\det(A - \lambda I_n) = (\frac{1}{s})^n \det(sA - rI_n) \neq 0$. Therefore, λ is not an algebraic integer. □

Cor: For every character χ of G and $\forall g \in G$, if $\chi(g) \in \mathbb{Q}$, then $\chi(g) \in \mathbb{Z}$.

We now apply the previous proposition to show that the degree of an irreducible character χ of G must divide $|G|$.

Defn: Let $g \in G$, and let $C = \bar{g}$ be a conjugacy class. Then let $\overline{C} = \sum_{x \in C} x$. We call $\overline{C}$ a class sum.

Lemma: Let $g \in G$ and let $C = \bar{g}$. Let U be an irreducible $\mathbb{C}[G]$-module with character χ. Then there exists $\lambda \in \mathbb{C}$ such that $\overline{C}\vec{u} = \lambda \vec{u}$ for all $\vec{u} \in U$, where $\lambda = \frac{|G|}{|Z(g)|} \frac{\chi(g)}{\chi(e)}$.

Pf: For any $h \in G$:
$\bar{C}h = \sum_{x \in C} xh = \sum_{y \in C} hy = h\bar{C}$.
Therefore, by Schur's Lemma, $\exists \lambda \in \mathbb{C}$ such that $\bar{C}\vec{u} = \lambda \vec{u}$, and so $\sum_{x \in G} x = \lambda 1_u$. Taking the trace of both sides, we get:
$\chi(e)\lambda = \sum_{x \in G} \chi(x) = |C|\chi(g) = \frac{|G|}{|Z(g)|}\chi(g)$. □

Lemma: Let $r = \sum_{g \in G} \alpha_g g \in \mathbb{Z}[G] \subset \mathbb{C}[G]$. Let u be a nonzero element in $\mathbb{C}[G]$ such that $ru = \lambda u$ for some $\lambda \in \mathbb{C}$. Then $\lambda \in A$.

Pf: Let $G = \{g_1, \dots, g_r\}$. Then
$r \cdot g_i = \sum_{j=1}^{r} a_{ij} g_j$ where $a_{ij} = \alpha_{g_i g_j^{-1}} \in \mathbb{Z}$,
and so λ is an eigenvalue of $A = [a_{ij}]$. □

Cor: For all $g \in G$ and any irreducible char χ,
$\frac{|G|}{|Z(g)|}\frac{\chi(g)}{\chi(e)} \in A$.

Thm: For any irreducible char χ of G, $\chi(e) \mid |G|$.

Pf: Let $g_1, \dots, g_k$ be the representatives of the conjugacy classes of G. Then $\forall i$, $\frac{|G|}{|Z(g_i)|}\frac{\chi(g_i)}{\chi(e)}$ and $\chi(g_i)^*$ are algebraic integers. Thus,
$\sum_{i=1}^{k} \frac{|G|}{|Z(g_i)|}\frac{\chi(g_i)\chi(g_i)^*}{\chi(e)} \in A$.
By character table row-orthogonality:
$\frac{|G|}{\chi(e)} \sum_{i=1}^{k} \frac{\chi(g_i)\chi(g_i)^*}{\chi(e)} = \frac{|G|}{\chi(e)}$,
and so $\frac{|G|}{\chi(e)} \in A$. But we also have $\frac{|G|}{\chi(e)} \in \mathbb{Q}$, and therefore $\frac{|G|}{\chi(e)} \in \mathbb{Z}$. □

Examples: 1) Suppose $|G| = p^n$, where p is prime.
Then for all irreducible χ, $\chi(e) = p^k$ for $0 \le k < \frac{n}{2}$.
The upper bound ($k < \frac{n}{2}$) comes from the sum of squares formula, together with the fact that G has to have a repn of degree 1 (ie the trivial repn).

a) $|G| = p^2$
Then all irreducible repns have degree 1, which implies that G is abelian.

b) $|G| = p^3$.
Either G is abelian, or G has a nonlinear irreducible character. If $|G'| = p$, then $|G/G'| = p^2$, which would give p^2 linear characters, and therefore $(p-1)$ irred chars of degree p.

2) Suppose $|G| = 2p$. Then either all irreducible chars are linear, or G has 2 linear chars and $\frac{p-1}{2}$ irred. chars of degree 2.

Prop: No simple group has an irred. char. of degree 2.

Pf: Suppose G is a simple gp with an irred char χ of degree 2. Then G is nonabelian and $2 \mid |G|$. Let $\rho: G \to GL(2, \mathbb{C})$ be a repn with char χ. Then $\ker \rho \trianglelefteq G$, so $\ker \rho = \{e\}$, so ρ is faithful. Also $G' \neq \{e\}$, so $G' = G$. Thus, the only linear char of G is the trivial char.

Now note $g \mapsto \det \rho(g)$ is a lin. char. of G, and so $\det(\rho(g)) = 1 \ \forall g \in G$. Since $2 \mid |G|$, $\exists x \in G$ such that $o(x) = 2$. So $\rho(x) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$, and therefore $\rho(x)$ commutes with $\rho(g) \ \forall g \in G$. Since ρ is faithful, this implies $xg = gx \ \forall g \in G$, and so $x \in Z(G)$, and so $\langle x \rangle \trianglelefteq G$.

□