Lecture 9.

Final exam: January 14, 15:15-18:15.

Recall: Proposition If V is a finite dimensional representation of G over $\mathbb{C}$, then the symmetric group S_n acts on $V^{\otimes n}$ by permutation of factors. This action commutes with the action $\rho_V^{\otimes n}$ of G on $V^{\otimes n}$. Each S_n-isotypical component in $V^{\otimes n}$ is a G-subrepresentation.

Today: algebraic integers in representation theory.

Consequences: (1) $\dim V$, V irreducible, divides $|G|$

(2) A group of order $p^a q^b$ is solvable (Burnside's theorem).

Algebraic integers.

highest coefficient is 1

Def. $z \in \mathbb{C}$ is an *algebraic integer* if z is a root of a monic polynomial with integer coefficients (Ex: $z^k - 1 = 0$, roots of 1).

Claim z is an algebraic integer $\iff$ z is an eigenvalue of a matrix with integer coefficients.

Proof: z is an eigenvalue $\Rightarrow$ root of the characteristic polynomial, monic with integer coefficients.

If z is a root $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, then it is a root of the characteristic polynomial of

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & \vdots \\ & & 1 & \ddots & \vdots \\ 0 & & & \ddots & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

By induction:
$$\det\begin{pmatrix} \lambda & 0 & a_0 \\ -1 & \lambda & a_1 \\ 0 & -1 & \lambda+a_2 \end{pmatrix} = \lambda^2(\lambda+a_2) + a_0 + a_1\lambda = \lambda^3 + \lambda^2 a_2 + \lambda a_1 + a_0$$

$\blacksquare$

Corollary. The set of algebraic integers $\mathbb{A}$ is a ring.

Proof. Let $\begin{matrix}\alpha\\ \beta\end{matrix}$ be eigenvalues of $\begin{matrix}A\\ B\end{matrix}$ with eigenvectors $\begin{matrix}v\\ w\end{matrix}$

$$Av = \alpha v, \quad Bw = \beta w$$

Then $(A \otimes Id + Id \otimes B)(v \otimes w) = \alpha(v \otimes w) + \beta(v \otimes w) = (\alpha+\beta)(v \otimes w)$

$$A \otimes B (v \otimes w) = \alpha\beta(v \otimes w)$$

$\blacksquare$

Def. Let α be an alg integer, and $p(x)$ the minimal polynomial (monic, integer coeff) s.t. α is a root of $p(x)$. Then other roots of $p(x)$ are called the algebraic conjugates of α.

Claim Algebraic conjugates of $\alpha_1 + \alpha_2 + \dots + \alpha_m$, $\alpha_i \in \mathbb{A}$, are of the form $\alpha_1' + \alpha_2' + \ldots + \alpha_m'$, where α_i' is an alg conjugate to α_i

Proof. α_i is an eigenvalue of A_i $\Rightarrow$ $\alpha_1 + \alpha_2$ is an eigenvalue of $A_1 \otimes Id + Id \otimes A_2$

$\Rightarrow$ Alg conjugates to $(\alpha_1 + \alpha_2)$ are eigenvalues of $A_1 \otimes Id + Id \otimes A_2$

Eigenvalues of $A_1 \otimes Id$ are $v_i \otimes y_i$ $\quad v_i$ eigenvalues of A_1, y_i any vector

$Id \otimes A_2$ $\quad x_i \otimes w_i$ $\quad w_i$ — " — A_2, x_i any vector

$\Rightarrow$ eigenvectors of $A_1 \otimes Id + Id \otimes A_2$ are $v_i \otimes w_j$ $\Rightarrow$

eigenvalues are of the form $\alpha_1' + \alpha_2'$, where α_1' conj to α_1, α_2' conj to α_2. $\boxed{///}$

Proposition. $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Proof Let z be a root of $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ $\quad a_i \in \mathbb{Z}$

Suppose $z = \frac{p}{q} \in \mathbb{Q}$, $\gcd(p,q) = 1$ $\Rightarrow$ $\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \ldots + a_1 \frac{p}{q} + a_0 = 0$

$p, q \in \mathbb{Z}$

$$\underbrace{p^n}_{\not\vdots q} + \underbrace{q a_{n-1} p^{n-1}}_{\vdots q} + \ldots + \underbrace{q^{n-1} a_1 p}_{\vdots q} + \underbrace{q^n a_0}_{\vdots q} = 0$$

$\Rightarrow$ only possible if $q = \pm 1$.

Theorem. Let G be a finite group and V a complex irreducible representation of G. Then $\dim V$ divides $|G|$.

Proof. Let C be a conj class in G, and $R = \sum_{h\in C} h \subset \mathbb{Z}[G]$

Then R is central in $\mathbb{C}[G]$.

$\Rightarrow$ R acts by a scalar in an irreducible V. , $\rho_V(R) = \lambda\, Id_V$.

This λ is an algebraic integer : R satisfies a monic polynomial equation in $\mathbb{Z}[G]$ since it satisfies the characteristic polynomial of matrix of action of R in $\mathbb{Z}[G]$ $\Rightarrow$ monic with integer coefficients.

Ex.

$$G = S_3 \simeq D_3 = \{1, r, r^2, s, rs, r^2 s\} = \{1, (123), (132), (12), (23), (13)\}$$

$C = \{r, r^2\}$ $\Rightarrow$ $R = r + r^2$: in the basis $\{1, r, r^2, s, rs, r^2 s\}$

$$\begin{pmatrix} 0&1&1&&&\\ 1&0&1&&&\\ 1&1&0&&&\\ &&&0&1&1\\ &&&1&0&1\\ &&&1&1&0 \end{pmatrix} \to \det \begin{pmatrix} -\lambda&1&1&&&\\ 1&-\lambda&1&&&\\ 1&1&-\lambda&&&\\ &&&-\lambda&1&1\\ &&&1&-\lambda&1\\ &&&1&1&-\lambda \end{pmatrix} = \left(-\lambda^3+1+1+\lambda+\lambda+\lambda\right)^2 =$$

$$= \left(-\lambda^3+3\lambda+2\right)^2$$

$$(r+r^2)^3 = 3(r+r^2)+2 \quad : \quad \big((123)+(132)\big)^3 = 3\big((123)+(132)\big)+2 \in \mathbb{Z}[S_3]$$

$\Rightarrow$ $\lambda\, Id$ acting on V satisfies a monic polynomial equation with integer coefficients.

So λ is an algebraic integer. Taking the trace of $R = \sum_{h\in C} h$

$$|C|\,\chi_V(g) = \lambda \dim V \Rightarrow \lambda = \frac{|C|\,\chi_V(g)}{\dim V} \in A.$$

Let C_i conj classes, $g_{c_i} \in C_i$

Consider $\sum_i \lambda_i \overline{\chi_V(g_{c_i})} \in A$ Because: (1) $\lambda_i \in A$

(2) $\overline{\chi_V(g_{c_i})}$ are sums of roots of unity

(3) A is a ring

$$\sum_i \lambda_i \overline{\chi_V(g_{C_i})} = \sum_i \frac{|C_i|\,\chi_V(g_{C_i})}{\dim V}\,\overline{\chi_V(g_{C_i})} =$$

$$= \sum_{g\in G} \frac{\chi_V(g)\,\overline{\chi_V(g)}}{\dim V} = \frac{|G|}{\dim V}(\chi_V,\chi_V) = \frac{|G|}{\dim V} \begin{matrix}\in \mathbb{Q} \\ \in A\end{matrix}$$

$$\Longrightarrow \quad \frac{|G|}{\dim V} \in A \cap \mathbb{Q} = \mathbb{Z}. \qquad \blacksquare$$

Burnside's theorem

Def. G is solvable if $\exists$ a series of nested subgroups

$$\{e\} = G_1 \lhd G_2 \lhd \dots \lhd G_n = G \quad \text{such that}$$

$G_i \lhd G_{i+1}$ is normal, and G_{i+1}/G_i is abelian.

Theorem. Any group of order $p^a q^b$, where p, q are primes, is solvable.

Proposition. In particular, if $|G| = p^a$, it is solvable.

Proof: Induction on a; $a = 0 = G = \langle e \rangle$, $a = 1 \Rightarrow G = C_p$ abelian

If $|G| = p^a \Rightarrow$ class equation $\underset{\vdots p}{|G|} = \underset{\geq 1}{|Z(G)|} + \sum_i \underbrace{[G : G_i]}_{>1} \vdots p$

$G_i \subset G$ centralizer subgroups

$\Rightarrow |Z(G)| \vdots p \Rightarrow |G/Z(G)| = p^b$, $b < a$

which is solvable by induction hypothesis $\blacksquare$

Proposition 1 Let V be an irreducible representation of a finite group G and C a conjugacy class in G s.t. $\gcd(|C|, \dim V) = 1$.

Then
$$\begin{cases} \text{either } \chi_V(g) = 0 & \forall g \in C \\ \text{or } \rho_V(g) = \lambda \cdot Id, \ g \text{ acts as a scalar in } V & \forall g \in C. \end{cases}$$

Proof. Consider again $\sum_{g\in C} \chi_V(g) \frac{|C|}{\dim V} \in \mathbb{A}$ as before.

If $\gcd(|C|, \dim V) = 1 \Rightarrow \exists\, a, b \in \mathbb{Z}$ s.t. $a|C| + b\cdot \dim V = 1$

$\Rightarrow$ multiply by $\frac{\chi_V(g)}{\dim V}$:

$$\underbrace{\frac{a\,|C|\,\chi_V(g)}{\dim V}}_{\in \mathbb{A}} + \underbrace{\frac{b\,\chi_V(g)\,\cancel{\dim V}}{\cancel{\dim V}}}_{\in \mathbb{A}} = \frac{\chi_V(g)}{\dim V} \in \mathbb{A}$$

$\Rightarrow$ Let $n = \dim V \Rightarrow \frac{\chi_V(g)}{n} = \frac{(\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n)}{n} = t$ where ε_i are roots of 1.

If all ε_i are equal $\Rightarrow \rho_V(g) = \varepsilon\, Id_V$ acts as a scalar.

If not, $|t| < 1$; consider the algebraic conjugates to t:

they are sums $t' = \frac{(\varepsilon_1' + \varepsilon_2' + \ldots + \varepsilon_n')}{n}$ where ε_i' is alg conjugate to ε_i
also roots of unity

$\Rightarrow$ all $|t'| < 1 \Rightarrow$ product of all alg conjugates has the absolute value $< 1 \Rightarrow$ this is the free term of the polynomial equation satisfied by $t \Rightarrow = 0 \Rightarrow t = 0 = \frac{\chi_V(g)}{n}$ ▨

Proposition 2. Let G be a finite group and C a conjugacy class of order p^k, where p is a prime and $k>0$. Then G has a proper nontrivial normal subgroup.

Proof. Let $g \in C \Rightarrow g \neq 1$, $|C| = p^k$

2nd orthogonality relation $\Rightarrow \sum_{V \in Irr} \overline{\chi_V(1)} \cdot \chi_V(g) = 0$ since g is not conjugate to 1.

$$\sum_{V \in Irr} \dim V \cdot \chi_V(g) = 0.$$

$$Irr\, G = \begin{cases} V_0 & \text{trivial} \\ D: \ V: & p \text{ divides } \dim V \\ N: \ V: & p \text{ does not divide } \dim V \end{cases}$$

$$\Rightarrow \sum_{V \in Irr} \dim V \cdot \chi_V(g) = \underbrace{\chi_{V_0}(g)}_{1} + \underbrace{\sum_{V \in D} \dim V\, \chi_V(g)}_{= p \cdot a\text{, where } a \in \mathbb{A}} + \sum_{V \in N} \dim V\, \chi_V(g) = 0.$$

If $V \in D \Rightarrow \underbrace{\frac{1}{p}\dim V}_{\in \mathbb{Z}} \chi_V(g) \in A$

$$\Rightarrow \quad 1 + pa + \sum_{V \in N} \dim V \, \chi_V(g) = 0 \Rightarrow \sum_{V \in N} \dim V \, \chi_V(g) \neq 0$$

Otherwise, $1 + pa = 0 \Rightarrow a = -\frac{1}{p} \in \mathbb{Q}$, but $a \in A$, contradiction

$\Rightarrow \quad \exists g \in C$: and $V \in N$: $\chi_V(g) \neq 0$.

we have: $\gcd(\underbrace{|C|}_{=p^k}, \underbrace{\dim V}_{\not\vdots p}) = 1 \Rightarrow$ Proposition 1 $\left[\begin{array}{l} \chi_V(g) = 0 \\ \rho_V(g) \text{ acts by a scalar} \end{array}\right.$

Since $\chi_V(g) \neq 0 \Rightarrow \rho_V(g) = \lambda \, Id$ in V.

Let $H = \langle ab^{-1}, a, b \in C \rangle \subset G$. It is normal: $\underbrace{gag^{-1}}_{a'} \underbrace{gb^{-1}g^{-1}}_{} = a'b'^{-1} \in H$, $a, b \in C$

subgp gen. by

H is nontrivial: $|C| = p^k$, $k > 0$ $\quad ab^{-1} = 1 \Leftrightarrow a = b$

H is proper: H acts trivially $\underbrace{\rho(ab^{-1})}_{} = \rho(a)\rho(b^{-1}) = \lambda \cdot \lambda^{-1} Id_V = Id_V$

Since $V \neq V_0 \Rightarrow \exists k \in G$: k acts nontrivially in $V \Rightarrow H \neq G$. $\square$

Burnside's theorem. Any group of order $p^a q^b$, p, q primes, is solvable.

Proof: Let G be the smallest counter-example.

Then G is simple: if not, it has a proper normal subgroup and the quotient has the order $p^c q^d$, $p^c q^d < p^a q^b$, which is solvable. $\Rightarrow$ G is solvable. $\{e\} \lhd N \lhd \ldots \lhd G$

If G is simple $\Rightarrow$ it cannot have a conjugacy class of order p^k or q^k, $k \geq 1$ by Proposition 2. $\Rightarrow$

Any conj class $\left[\begin{array}{l} \text{either } |C| = 1 \\ \text{or } \quad |C| \text{ is divisible by } pq \end{array}\right.$

$$\underset{\vdots pq}{|G|} = \underset{\geq 1}{|Z(G)|} + \underset{\vdots pq}{\sum |C_i|} \Rightarrow |Z(G)| \text{ is divisible by } pq$$

$\Rightarrow$ G has a nontrivial center

$\Rightarrow$ G is not simple. $\square$