Math 5555

Abstract Algebra II

Book 3

For each $i \in \{1, 2, \ldots, k\}$, we solve n_i equations (one for each $t \in \{1, \ldots, n_i\}$)

in n_i unknowns $\lambda_{i,j}$, $j \in \{1, 2, \ldots, n_i\}$.

In general the n_i symmetric polynomials $\lambda_{i,1}^t + \cdots + \lambda_{i,n_i}^t$ $\quad 1 \le t \le n_i$ $\quad$ Use (Newton's identies)

can be re-expressed in terms of the elementary symmetric polynomials

$e_j = e_j(\lambda_{i,1}, \ldots, \lambda_{i,n_i})$ which are the coefficients of

$$(x + \lambda_{i,1})(x + \lambda_{i,2}) \cdots (x + \lambda_{i,n_i}) = x^{n_i} + e_1 x^{n_i - 1} + e_2 x^{n_i - 2} + \cdots + e_{n-1} x + e_n$$

i.e. $e_n = \lambda_{i,1} \lambda_{i,2} \cdots \lambda_{i,n_i}$

$\vdots$

$e_2 = \sum \lambda_{i,r} \lambda_{i,s}$

$e_1 = \lambda_{i,1} + \cdots + \lambda_{i,n_i}$

We will show: if $|G| = n$ then $\mathbb{C}G \cong \bigoplus_{i=1}^{k} M(n_i, \mathbb{C})$ (algebra isomorphism)

where k = number of conjugacy classes in G.

The <u>center</u> of R (semisimple algebra) is

$Z(R) = \{z \in R : zx = xz \text{ for all } x \in R\}$.

$Z(R) \subseteq R$ is a subalgebra: a subspace which is also a subring.

$M(n, \mathbb{C}) = \{n \times n \text{ complex matrices}\}$

$Z(M(n, \mathbb{C})) = \{\lambda I : \lambda \in \mathbb{C}\}$

$I = I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}_{n \times n}$

$$Z\left(\bigoplus_{i=1}^{k} M(n_i, \mathbb{C})\right) = Z\left(\begin{bmatrix} \overset{n_1 \times n_1}{\boxed{*}} & & & 0 \\ & \overset{n_2 \times n_2}{\boxed{*}} & & \\ & & \ddots & \\ 0 & & & \overset{n_k \times n_k}{\boxed{*}} \end{bmatrix}\right) = \left\{ \begin{bmatrix} \boxed{\lambda_1 I_{n_1}} & & & 0 \\ & \boxed{\lambda_2 I_{n_2}} & & \\ & & \ddots & \\ 0 & & & \boxed{\lambda_k I_{n_k}} \end{bmatrix} : \lambda_1, \ldots, \lambda_k \in \mathbb{C} \right\}$$

$\dim \bigoplus_{i=1}^{k} M(n_i, \mathbb{C}) = \sum_{i=1}^{k} n_i^2$; $\quad \dim\left(Z\left(\bigoplus_{i=1}^{k} M(n_i, \mathbb{C})\right)\right) = k$

$\dim \mathbb{C}G = n = |G|$

$\dim Z(\mathbb{C}G) = k =$ no. of conj. classes.

Let $K_1 \cdots K_k \subset G$ be the conj. classes i.e. $G = \underset{\substack{\shortparallel \\ \{1\}}}{K_1} \sqcup K_2 \sqcup \cdots \sqcup K_k$

For $1 \le i \le k$, let $z_i = \sum_{g \in K_i} g$ = sum of elements in K_i

$z_i \in Z(\mathbb{C}G)$ because $gz_i = z_i g$

$gz_ig^{-1} = z_i$

$Z(\mathbb{C}G) = \{ a_1 z_1 + \cdots + a_k z_k \; : \; a_i \in \mathbb{C} \}$

Given $z \in Z(\mathbb{C}G)$, say $z = \sum_{x \in G} a_x x$ $\quad a_x \in \mathbb{C}$

For all $g \in G$, $gz = zg$

$gzg^{-1} = z$

$\mathbb{Z}G$ = integral group ring of G $= \{ \sum_{g \in G} a_g g \; : \; a_g \in \mathbb{Z} \}$

$\mathbb{Q}G$ = rational group algebra .. .. - - - - . $\mathbb{Q}$

$\mathbb{R}G$ = real group algebra - - . $\mathbb{R}$

FG = group algebra of G over F $\quad F$

$F[G] = FG$ when G is a group.

$F[x,y,z]$ = polynomial algebra in x,y,z with coefficients in F (infinite dimensional)
as distinguished from $Fx + Fy + Fz = \langle x,y,z\rangle_F = \{a_x x + a_y y + a_z z : a_x, a_y, a_z \in F\}$
which is a 3-dimensional vector space

If R is an algebra over F and $S \subseteq R$ (any subset) then the centralizer of S in R is

$$C_R(S) = \{z \in R : zs = sz \text{ for all } s \in S\} \subseteq R \text{ subalgebra}$$

(Also called the commutant of S in R). $\qquad C_R(R) = Z(R)$

Schur's Lemma (late 19th century)
Let R be a semisimple algebra over $\mathbb{C}$, e.g. $R = M(n,\mathbb{C})$, or $\bigoplus_{i=1}^{k} M(n_i,\mathbb{C})$, or $\mathbb{C}G$, $|G|<\infty$.
Let M,N be simple R-modules and $\phi : M \to N$ a homomorphism i.e. $\phi(rm + sm') = r\phi(m) + s\phi(m')$ for all $r,s \in R$; $m, m' \in M$.

(i) If $M \not\cong N$ as R-modules then $\phi = 0$. There are no nonzero homomorphisms between simple modules.

(ii) If $M \cong N$, say $M = N$, then $\phi = cI$ for some $c \in \mathbb{C}$.

Proof (i) If $\phi \neq 0$ then there exists $v_0 \in M$ such that $\phi(v_0) \neq 0$, so $R\phi(v_0) \subseteq \phi(M) \subseteq N$ is a nonzero submodule of N. Since N is simple, $\underset{\phi(Rv_0)}{R\phi(v_0)} = N$.

The kernel of $\phi : M \to N$ is a submodule of M.
Since M is simple $\ker\phi = 0$ or M. But $\phi \neq 0$ ($\phi(v_0) \neq 0$) we have $\ker\phi = 0$. By the first isomorphism theorem, $M \cong M/\underset{\ker\phi}{0} \cong \phi(M) = N$
This contradicts $M \not\cong N$.

(ii) Let $\phi: M \to M$ be a homomorphism of the simple R-module M.
In particular ϕ is a $\mathbb{C}$-linear transformation of a finite dimensional complex vector space so there exists $v_0 \in M$, $v_0 \neq 0$ such that $\phi(v_0) = cv_0$ for some $c \in \mathbb{C}$ ($\mathbb{C}$ is alg. closed). Let $\tilde{\phi} = \phi - cI$ so $\tilde{\phi}$ is a homomorphism of R-algebras:

$$\tilde{\phi}(rm) = \phi(rm) - cIrm = r\phi(m) - crm = r(\phi(m) - cm) = r\tilde{\phi}(m).$$
$$\tilde{\phi}(m+m') = \tilde{\phi}(m) + \tilde{\phi}(m'). \qquad (r \in R;\ m, m' \in M)$$
$$v_0 \in \ker \tilde{\phi} \neq 0 \Rightarrow \ker \tilde{\phi} = M \Rightarrow \tilde{\phi} = 0 \Rightarrow \phi = cI. \quad \square$$

<u>Remark</u> If $M \cong N$ as R-modules there is an isomorphism $A: M \to N$
(A invertible $n \times n$ matrix, $n = \dim M = \dim N$)
$A(rm) = rAm$ for all $r \in R$.
then the R-module homomorphisms $M \to N$ all have the form cA, $c \in \mathbb{C}$

The choice of field $\mathbb{C}$ is important for Schur's Lemma e.g.
$G = \{1, g, g^2, g^3\}$ cyclic of order 4, $\pi: G \to GL_2(\mathbb{R})$
$$g \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$
$M = \mathbb{R}^2$ is an $\mathbb{R}G$-module using π

$$\pi(g)\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} b \\ -a \end{bmatrix}$$
π makes M into an R-module for $R = \mathbb{R}G$
M is a simple module but the R-homomorphisms $M \to M$ are more than just $aI = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$; we have $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ $(a, b \in \mathbb{R})$

Recall Schur's lemma:

If $\pi : G \to GL_n(\mathbb{C})$ is an irreducible representation then the only $n\times n$ matrices commuting with $\pi(g)$, for all $g \in G$ are the scalar matrices λI_n $(\lambda \in \mathbb{C})$.

If π, π' are representations of, $\pi : G \to GL_m(\mathbb{C})$, $\pi' : G \to GL_n(\mathbb{C})$ then π defines an action of G on $\mathbb{C}^m$. $g \in G$ acts on $v \in \mathbb{C}^m$ ($m\times 1$ column vector) as $gv = \underbrace{\pi(g)}_{m\times m}\underbrace{v}_{m\times 1} \in \mathbb{C}^m$

and π' defines an action of G on $\mathbb{C}^n$, $g\overset{\mathbb{C}^n}{v} = \underbrace{\pi'(g)}_{n\times n}\underbrace{v}_{n\times 1} \in \mathbb{C}^n$

then a $\mathbb{C}G$-homomorphism of the corresponding modules is (concretely) an $n\times m$ matrix $A \in \mathbb{C}^{n\times m} : \mathbb{C}^m \to \mathbb{C}^n$ such that

$$\begin{tikzcd} \mathbb{C}^m \arrow[r, "A"] \arrow[d, "\pi(g)"'] & \mathbb{C}^n \arrow[d, "\pi'(g)"] \\ \mathbb{C}^m \arrow[r, "A"'] & \mathbb{C}^n \end{tikzcd}$$

commutes for every $g \in G$ i.e. $\underbrace{\pi'(g)}_{n\times n}\underbrace{A}_{n\times m} = \underbrace{A}_{n\times m}\underbrace{\pi(g)}_{m\times m}$ for all $g \in G$

Such a matrix $A \in \mathbb{C}^{n\times m}$ is an <u>intertwining operator</u> (a linear transformation which respects/preserves the action of G).

i.e. $\alpha A = A\alpha$ for all $\alpha \in \mathbb{C}G$.

$\alpha(Av) = A(\alpha v)$ $\quad$ A is a homomorphism of $\mathbb{C}G$-modules.

If V "$\mathbb{C}^m$" and W "$\mathbb{C}^n$" are irreducible (simple) $\mathbb{C}G$-modules (π, π' irred. representations):

(i) inequivalent $\Rightarrow$ $A = 0$

(ii) π,π' equivalent $\Rightarrow$ $A = \lambda\cdot$ fixed invertible $n\times n$ matrix.

p.10 of handout. Theorem 4.4 (Wedderburn's Theorem)

Let $R = \mathbb{C}G$, $|G| < \infty$. Let $M_1, \dots, M_k$ be the distinct R-modules up to isomorphism.

$$\begin{array}{ccc} M_1 & \cdots & M_k \\ \uparrow & & \uparrow \\ \mathbb{C}^{n_1} & & \mathbb{C}^{n_k} \\ \pi_1 & \cdots & \pi_k \end{array}$$

The M_i-homogeneous part of R is the sum of all the left ideals of R isomorphic to M_i.

---

eg. $R = M(3, \mathbb{C})$. has only one simple module up to isomorphism, $\mathbb{C}^3$.

$A \in R$ acts on $V = \mathbb{C}^3$ by $\underbrace{v}_{3\times 1} \longmapsto \underbrace{A}_{3\times 3}\underbrace{v}_{3\times 1}$.

$$R = \begin{bmatrix} * & 0 & 0 \\ * & 0 & 0 \\ * & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & * & 0 \\ 0 & * & 0 \\ 0 & * & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \end{bmatrix}$$

contains $\begin{bmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} [1\ 1\ 0]$

minimal simple Submodules (left ideals) of the regular representation are all isomorphic to $\mathbb{C}^3$ as R-modules.

The $\mathbb{C}^3$-homogeneous part of this module is all of R.

$$R = \begin{bmatrix} * & & 0 \\ & \begin{smallmatrix} * & * \\ * & * \end{smallmatrix} & \\ 0 & & \begin{smallmatrix} * & * & * \\ * & * & * \\ * & * & * \end{smallmatrix} \end{bmatrix}$$

semisimple of dimension 14.

$\dim M_i = n_i$

$\dim M_i(R) = n_i^2$

R has three iso. types of simple modules of dimension 1, 2, 3.

$$R = \underbrace{\begin{bmatrix} * & & 0 \\ & \boxed{0} & \\ 0 & & \boxed{0} \end{bmatrix}}_{M_1(R)} \oplus \underbrace{\begin{bmatrix} 0 & & \\ & \begin{smallmatrix} * & * \\ * & * \end{smallmatrix} & \\ & & \boxed{0} \end{bmatrix}}_{M_2(R)} \oplus \underbrace{\begin{bmatrix} 0 & & \\ & \boxed{0} & \\ & & \begin{smallmatrix} * & * & * \\ * & * & * \\ * & * & * \end{smallmatrix} \end{bmatrix}}_{M_3(R)}$$

If $n_i = \dim M_i$ then the M_i-homo. part of $R = \mathbb{C}G$ is the sum of all submodules isomorphic to M_i.

R semisimple algebra over $\mathbb{C}$

$\mathrm{End}_R(R) = \{R\text{-}\underbrace{\text{endomorphisms}}_{\text{into itself}} \text{ of } R\}$ is the set of maps $\phi : R \to R$ such that $\phi(rx) = r\phi(x)$ for all $r, x \in R$

<u>Lemma</u> $\mathrm{End}_R(R)$ is anti-isomorphic to R.

For every $a \in R$ we have $\phi_a : R \to R$, $\phi_a(x) = xa$.

$\phi_a(rx) = rxa = r\phi_a(x) \implies \phi_a \in \mathrm{End}_R(R)$.

The map $R \longrightarrow \mathrm{End}_R(R)$, $\underset{R}{\overset{\in}{a}} \longmapsto \phi_a \in \mathrm{End}_R(R)$ is bijective.

If $a \in R$ such that $\phi_a = 0$ then $\phi(a) = \underbrace{\phi_a(1)}_{1a} = 0$ so $1a = 0 \implies a = 0$. So $a \mapsto \phi_a$ is one-to-one.

$\phi_{ab}(r) = rab = \phi_b(ra) = \phi_b(\phi_a(r)) = \phi_b \circ \phi_a(r) \implies \phi_b \circ \phi_a = \phi_{ab}$

If G is a group then $a \xrightarrow{f} a^{-1}$ is an antiautomorphism $f(ab) = f(b)f(a)$

Similarly with an algebra.

If R is an algebra then the <u>opposite algebra</u> R° is the algebra with the same elements as R° with same vector space structure; only the multiplication is replaced by $\underbrace{x * y}_{\text{in } R^\circ} = \underbrace{yx}_{\text{in } R}$

$x(yz) = x * (y * z) = (zy)x = z(yx) = (x*y)*z$

R° is not necessarily isomorphic to R. It is antiisomorphic.

$G^\circ \cong G$ because we can compose two anti-isomorphisms to get an isomorphism

$G \xrightarrow[\text{inverse}]{} G \xrightarrow[\circ]{} G^\circ$

If R is a division algebra then $R^\circ \cong R$ in the same way.

What are the R-endomorphisms of $R = \mathbb{C}G$? $\mathrm{End}_R(R) = R^\circ$.

$R = I_1 \oplus I_2 \oplus \cdots \oplus I_m$ as a direct sum of minimal left ideals.

If $\phi \in \mathrm{End}_R(R)$ then we can represent ϕ using an $m \times m$ matrix over R:

$\phi(r) =$

$$r = \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \quad r_i \in I_i$$

$r = r_1 + \cdots + r_m$ unique choice of $r_i \in I_i$

$\phi(r) = \phi(r_1) + \cdots + \phi(r_m)$, decompose each term with respect to our decomposition

$$= \sum_{i=1}^{m} \left(\sum_{j=1}^{m} \phi_{ij}(r_j) \right)$$

$$\phi_{ij} \in \mathrm{Hom}_R(I_i, I_j) = \begin{cases} 0 & \text{if } I_i \not\cong I_j \\ \mathbb{C} I_{n_i} & \text{if } I_i \cong I_j \end{cases}$$ Schur's Lemma

ϕ is represented by $n \times n$ matrix over $\mathbb{C}$

$$\begin{bmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1m} \\ \vdots & & & \vdots \\ \phi_{m1} & \cdots & \cdots & \phi_{mm} \end{bmatrix} = \begin{bmatrix} \underbrace{\boxed{*}}_{\in M(n_1, \mathbb{C})} & & 0 \\ & \underbrace{\boxed{*}}_{M(n_2, \mathbb{C})} & \\ 0 & & \ddots \quad \boxed{*} \end{bmatrix}$$

$\mathrm{End}_R(R)$ anti-iso to $\bigoplus_{i=1}^{k} M(n_i, \mathbb{C})$

$\|$

$R^\circ \overset{\text{anti-iso}}{=} R$

$R = \mathbb{C}G$ has an anti-isomorphism $\sum a_g g \longmapsto \sum a_g g^{-1}$

$$R \cong \bigoplus_{i=1}^{k} M(n_i, \mathbb{C})$$

p. 29 The Center of the group algebra

G finite group $\qquad n = |G| = \dim \mathbb{C}G$

$Z(\mathbb{C}G) = \{\alpha \in \mathbb{C}G : \alpha\gamma = \gamma\alpha \text{ for all } \gamma \in \mathbb{C}G\} \subseteq \mathbb{C}G$ subalgebra

$\dim Z(\mathbb{C}G) = k$ = number of conjugacy classes of G

$K_1, K_2, \dots K_k$: conjugacy classes of $G = \underbrace{K_1 \sqcup \cdots \sqcup K_k}_{\text{partition}}$ $\qquad K_1 = \{1\}$

$K_1 = \{1\}$ $\qquad \sum_{i=1}^{k} |K_i| = n = |G|$

$\mathrm{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_k\}$, $\chi_1 = 1_G$ principal character $\qquad n_i = \chi_i(1) = \deg \chi_i$ $\qquad n_1^2 + n_2^2 + \cdots + n_k^2 = n$

Moreover $n_i \mid n$ which we will prove today or Monday.

Irr. Reps. of G are $\pi_j : G \to GL_{n_j}(\mathbb{C})$

Basis for $Z(\mathbb{C}G)$ is $\{\gamma_1, \gamma_2, \dots, \gamma_k\}$ where γ_i = sum of elements in K_i. $\qquad$ Reps of $K_1, \dots, K_k$ are $g_1, \dots, g_k$, $g_1 = 1$

$$\mathbb{C}G \cong \bigoplus_{i=1}^{k} M(n_i, \mathbb{C}) = \begin{bmatrix} \boxed{*} & & & 0 \\ & \boxed{*} & & \\ & & \ddots & \\ 0 & & & \boxed{*} \end{bmatrix}$$

$n_1 \times n_1$ $\qquad n_2 \times n_2$ $\qquad n_k \times n_k$

$$Z(\mathbb{C}G) \cong Z\left(\bigoplus M(n_i, \mathbb{C})\right) = \left\{ \begin{bmatrix} \boxed{\omega_1 I_{n_1}} & & & 0 \\ & \boxed{\omega_2 I_{n_2}} & & \\ & & \ddots & \\ 0 & & & \boxed{\omega_k I_{n_k}} \end{bmatrix} : \omega_1, \dots, \omega_k \in \mathbb{C} \right\}$$

The iso. $\mathbb{C}G \longrightarrow \bigoplus_{i=1}^{k} M(n_i, \mathbb{C})$ is defined on our basis $g \mapsto \begin{bmatrix} \boxed{\pi_1(g)} & & & 0 \\ & \boxed{\pi_2(g)} & & \\ & & \ddots & \\ 0 & & & \boxed{\pi_k(g)} \end{bmatrix}$

$\pi_j : G \to GL_{n_j}(\mathbb{C})$ is a group homo. extending to algebra homo.

$\pi_j : \mathbb{C}G \to M(n_j, \mathbb{C})$, defined by $\pi_j\left(\sum_g a_g g\right) = \sum_g a_g \pi_j(g)$.

Restrict to $z \in Z(\mathbb{C}G)$. $zg = gz$ for all $g \in G$

$\Rightarrow \pi_j(z)\pi_j(g) = \pi_j(zg) = \pi_j(gz) = \pi_j(g)\pi_j(z) \Rightarrow \pi_j(z) = c I_{n_j}$, some $c \in \mathbb{C}$ by Schur's Lemma.

In particular $\pi_j(\gamma_i) = \underbrace{\omega_j(\gamma_i)}_{\in \mathbb{C}} I_{n_j}$ since $\gamma_i \in Z(\mathbb{C}G)$

$1 \le i \le k$
$1 \le j \le k$

Denote $\omega(\gamma_i) = \omega_j(\gamma_i) = \omega_\chi(\gamma_i)$ where $\chi = \chi_j = \operatorname{tr} \pi_j$.

$\pi_j(\gamma_i) = \omega_j(\gamma_i) I_{n_j}$ Take trace on both sides. $\gamma_i = \sum_{g \in K_i} g$

$|K_i| \operatorname{tr} \pi_j(g_i) = |K_i| \chi_j(g_i) = n_j \omega_j(\gamma_i) = \chi_j(1)\omega_j(\gamma_i)$

$$\boxed{\omega_\chi(\gamma_i) = \frac{|K_i|\chi(g_i)}{\chi(1)}}$$

(p. 30) We will see that these values $\omega_\chi(\gamma_i)$ are algebraic integers.

pos. integers

algebraic integer
i.e. root of monic poly. with coeffs in $\mathbb{Z}$.

To show $\frac{n}{n_i} \in \mathbb{Z}$, show it's an algebraic integer and a rational number.

Use $\{\text{alg. integers}\} \cap \mathbb{Q} = \mathbb{Z}$

$Z(\mathbb{C}G)$ is an algebra. (subalgebra)

In particular $\gamma_i\gamma_j \in Z(\mathbb{C}G) \implies \gamma_i\gamma_j = \sum_{l=1}^{k} a_{ijl}\gamma_l$ $\quad a_{ijk} \in \mathbb{Z}$

a_{ijl} $(i,j,l \in \{1,2,\dots,k\})$ are the structure constants of $Z(\mathbb{C}G)$.

Additively, $Z(\mathbb{C}G) \cong \mathbb{C}^k$
$\sum_{j=1}^{k} b_j\gamma_j$

$Z(\mathbb{Z}G) =$ algebra gen. by $\gamma_1,\dots,\gamma_k$ over $\mathbb{Z}$
$= \{\sum_j b_j\gamma_j : b_j \in \mathbb{Z}\}$

Additively: $\mathbb{Z}^k$

The multiplicative structure is entirely described by the struct. constants a_{ijl}.

$a_{ijl} =$ ~~formula~~ determined using the char. table of G.

Eg. $G = S_3 = \underbrace{\{()\}}_{K_1} \sqcup \underbrace{\{(12),(13),(23)\}}_{K_2} \sqcup \underbrace{\{(123),(132)\}}_{K_3}$

In $\mathbb{Z}G \subset \mathbb{C}G$

$\gamma_1 = ()$, $\gamma_2 = (12)+(13)+(23)$, $\gamma_3 = (123)+(132)$

$\gamma_1\gamma_2 = \gamma_2$, $\gamma_1\gamma_3 = \gamma_3$, $\gamma_1\gamma_1 = \gamma_1$

$\gamma_2\gamma_2 = ((12)+(13)+(23))((12)+(13)+(23)) = 3() + 3(123) + 3(132) = 3\gamma_1 + 3\gamma_3$

$\gamma_3\gamma_3 = ((123)+(132))((123)+(132)) = 2() + (123) + (132) = 2\gamma_1 + \gamma_3$

$\gamma_2\gamma_3 = \gamma_3\gamma_2 = ((12)+(13)+(23))((123)+(132)) = 2\gamma_2$

In a large group, these expansions look unmanageable this way but: we can compute a_{ijk} directly from the character table of G.

In S_3, each 3-cycle can be expressed as a product of two transpositions in exactly $a_{223} = 3$ different ways.

$\pi(z) = \omega_\chi(z) I$ for all $z \in Z(\mathbb{C}G)$, where $\pi : G \to GL_n(\mathbb{C})$ irred. rep. with character χ

$\omega_\chi(\gamma_i) = \dfrac{|K_i|\chi(g_i)}{\chi(1)}$. $\quad \omega_\chi : Z(\mathbb{C}G) \to \mathbb{C}$ is an algebra homo; $\omega_\chi(zz') = \omega_\chi(z)\omega_\chi(z')$ for all $z, z' \in Z(\mathbb{C}G)$.

__Theorem__ The structure constants of $Z(\mathbb{C}G)$ are $a_{ij\ell} = \dfrac{|K_i||K_j|}{|G|} \displaystyle\sum_{\chi \in \mathrm{Irr}\,G} \dfrac{\chi(g_i)\chi(g_j)\overline{\chi(g_\ell)}}{\chi(1)}$. (non-negative integers)

__Proof__ $\gamma_i \gamma_j = \sum_{\ell=1}^{k} a_{ij\ell}\gamma_\ell$. $\quad \omega_\chi(\gamma_i) = \dfrac{|K_i|\chi(g_i)}{\chi(1)}$. Apply this homomorphism to $Z(\mathbb{C}G)$ on both sides:

$$\frac{|K_i|\chi(g_i)}{\chi(1)} \cdot \frac{|K_j|\chi(g_j)}{\chi(1)} = \sum_{\ell=1}^{k} a_{ij\ell} \frac{|K_\ell|\chi(g_\ell)}{\chi(1)}.$$

Now multiply both sides by $\chi(1)\overline{\chi(g_s)}$ $(s = 1, 2, \cdots, k)$ to get

$$\sum_\chi \frac{|K_i||K_j|\chi(g_i)\chi(g_j)\overline{\chi(g_s)}}{\chi(1)} = \sum_\chi \sum_{\ell=1}^{k} a_{ij\ell}|K_\ell|\chi(g_\ell)\overline{\chi(g_s)}$$

Sum over $\chi \in \mathrm{Irr}(G)$ and use col. orthogonality of char table of G

$$\sum_{\chi \in \mathrm{Irr}\,G} \chi(g_\ell)\overline{\chi(g_s)} = \begin{cases} 0, & \text{if } \ell \neq s \\ |C_G(g_\ell)| & \text{if } \ell = s \end{cases} \qquad |C_G(g_\ell)| = \frac{|G|}{|K_\ell|}$$

$$= \sum_{\ell=1}^{k} a_{ij\ell} \cancel{|K_\ell|} \underbrace{\sum_\chi \chi(g_\ell)\overline{\chi(g_s)}}_{\delta_{\ell s}\frac{|G|}{\cancel{|K_\ell|}}}$$

$$= |G| a_{ijs} \qquad \square$$

So why are $\omega_\chi(\gamma_i) \in \mathbb{Z}$?

$$\gamma_i \gamma_j = \sum_{l=1}^{k} a_{ijl}\gamma_l$$

$$\omega_\chi(\gamma_i)\,\omega_\chi(\gamma_j) = \sum_{l=1}^{k} a_{ijl}\,\omega_\chi(\gamma_l)$$

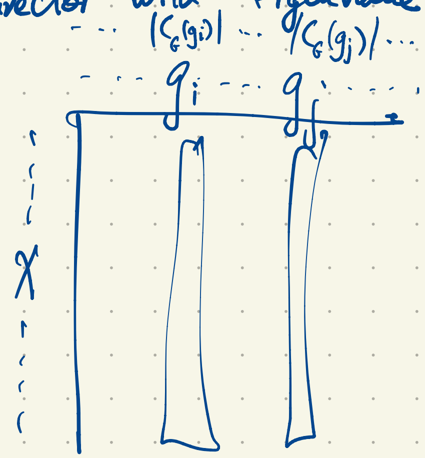
In $Z(\mathbb{C}G)$, we consider left-multiplication by $\omega_\chi(\gamma_i)$ (fixed i) as a linear transformation with $k \times k$ matrix

$$A_i = A = [a_{ijl}]_{j,l=1,\dots,k}$$

$\det(tI_k - A)$ is a monic poly. with integer coeffs.

$\Rightarrow \omega_\chi(\gamma_i)$ is an alg. integer

If $v = \begin{bmatrix} \omega_\chi(\gamma_1) \\ \vdots \\ \omega_\chi(\gamma_k) \end{bmatrix}$ then $Av = \omega_\chi(\gamma_i)v$ so v is an eigenvector with eigenvalue $\omega_\chi(\gamma_i)$.



Check $v \neq 0$: on Wednesday. First entry $\omega_\chi(\gamma_1) = |K_1|\,\omega_\chi(g_1)$

$g_1 = 1$, $|K_1| = 1$

$\pi(1) = \pi(g_1) = \omega_\chi(1) I_{n_j}$, $\deg \pi = \deg \chi = \chi(1)$

Column orthogonality of char. table of G:

$$\sum_{\chi \in \mathrm{Irr}\,G} \chi(g_i)\overline{\chi(g_j)} = |C_G(g_i)|\,\delta_{ij}$$

For $i = j$: $\sum_{\chi \in \mathrm{Irr}\,G} \chi(g_i)\overline{\chi(g_i)} = |C_G(g_i)| = \dfrac{|G|}{|K_i|}$

$|K_i| = [G : C_G(g_i)]$

$$\omega_\chi(\gamma_i) = \frac{|K_i|\,\chi(g_i)}{\chi(1)}$$

$$\chi(1)\,\omega_\chi(\gamma_i) = |K_i|\,\chi(g_i)$$

$$|G| = \sum_\chi |K_i|\,\chi(g_i)\overline{\chi(g_i)}$$

$$= \sum_{\chi \in \mathrm{Irr}\,G} \chi(1)\,\underbrace{\omega_\chi(\gamma_i)}_{\text{alg. int}}\,\underbrace{\overline{\chi(g_i)}}_{\text{alg. int.}} \quad \text{is an}$$

$$\frac{|G|}{|\chi(1)|} = \sum_\chi [\text{alg. int}]$$ is an alg. int. Also in $\mathbb{Q}$.

$\Rightarrow \dfrac{|G|}{\chi(1)} \in \mathbb{Z}$

$\Rightarrow \chi(1) \mid |G|$.

The order of every irred. rep. of G divides $|G|$.

$\omega_\chi(\gamma_i) \in \mathbb{Z}$.

Burnside's Theorem Every group of order $p^a q^b$ (p, q prime; $a, b \geq 0$ integers) is solvable.

There are no nonabelian simple groups of order $p^a q^b$.

The proof (see notes) requires char. theory.

In a finite group G, a difference set is a subset $D \subset G$ such that every nonidentity element $g \in G$ can be expressed as $g = d_1 d_2^{-1}$ ($d_1, d_2 \in D$) in exactly r ways.

Eg. $G = \{1, g, \dots, g^6\}$ cyclic of order 7.

$D = \{g, g^2, g^4\}$

$$g^2 g^{-1} = g$$
$$g^4 (g^2)^{-1} = g^2$$
$$g^4 g^{-1} = g^3$$
$$g (g^4)^{-1} = g^4$$
$$g^2 (g^4)^{-1} = g^5$$
$$g (g^2)^{-1} = g^6$$

In $\mathbb{Z}/7\mathbb{Z}$, $D = \{1, 2, 4\}$

$2-1 = 1$
$4-2 = 2$
$4-1 = 3$
$1-4 = 4$
$2-4 = 5$
$1-2 = 6$

$(7,3,1)$-diff set in C_7.

If $|G| = v$ and $|D| = k$ then $k(k-1) = r(v-1)$. D is a (v,k,r)-diff. set in G.

$3 \cdot 2 = 1 \cdot (7-1)$
$6 = 6$.

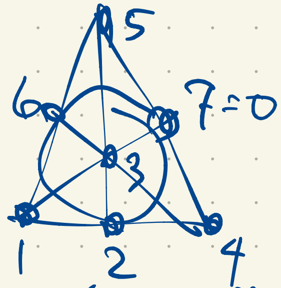
When does a (v,k,r)-diff. set exist in a group of order v?
Techniques work best when G is abelian. But there are nontrivial diff. sets in some nonabelian groups. Eg. G = Frob. gp. of order 21 (the nonabel. gp. of order 21) has a nontriv. $(21,5,1)$-diff. set.

$5 \cdot (5-1) = 1 \cdot (21-1)$
$20 = 20$

Also a diff. set in the cyclic gp. of order 21.
Both examples arise from the proj. plane of order 21.

If D is a (v,k,r)-diff. set in a gp G then $\{Dg : g \in G\}$ (the v blocks of the design) form a (v,k,r) symmetric design:
v subsets of size k in a set of size v
Any two of them intersect in r points
any two pts are in exactly r blocks.

$D = \{1,2,4\}$ in C_7
$D+1 = \{2,3,5\}$
$D+2 = \{3,4,6\}$



The fact that $D \subset G$ is a (v,k,r)-diff. set can be expressed succinctly in the group ring $\mathbb{Z}G$:

$\gamma = \sum_{g\in G} g$, $\quad \delta = \sum_{d \in D} d$. $\quad \mathbb{Z}G$ has an involutory anti-automorphism $\alpha \mapsto \alpha^*$ $\quad (\alpha^*)^* = \alpha$, $\quad (\alpha\beta)^* = \beta^*\alpha^*$

If $\alpha = \sum_{g\in G} a_g g$ then $\alpha^* = \sum_{g\in G} a_g g^{-1}$

$\delta\delta^* = n + r\gamma$ where $n = k - r$ $\quad$ n = order of the design (or the difference set)

$= k + r(\gamma - 1) = \underbrace{(k-r)}_{n} + r\gamma$

Eg. $D = \{g, g^2, g^4\}$ in $G = \{1, g, g^2, \dots, g^6\}$ cyclic of order 7 $\quad$ $(7,3,1)$-diff. set of order 2

$\delta = g + g^2 + g^4$

$\delta\delta^* = (g+g^2+g^4)(g^{-1}+g^{-2}+g^{-4}) = 3 + g+g^2+g^3+g^4+g^5+g^6 = 2+\gamma$

	1	g	g^2	$\cdots$	g^6
χ_1	1	1	1	$\cdots$	1
χ_2	1	ζ	ζ^2	$\cdots$	ζ^6
$\vdots$	1	ζ^2	ζ^4	$\cdots$	ζ^5
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_7	1	ζ^6	ζ^5	$\cdots$	ζ

$\zeta = e^{2\pi i/7}$

Let $\chi \in \operatorname{Irr} G$. So $\chi(1) = 1$.

$\chi : \mathbb{Z}G \to \mathbb{C}$ is an (ring) algebra homo.

$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$

If $\chi = \chi_1$ = principal character then $\chi(\sum a_g g) = \sum a_g$ "augmentation map"

$\chi(\delta) = k, \quad \chi(\gamma) = v$

$\delta\delta^* = n + r\gamma \Rightarrow k^2 = n + rv \Rightarrow n = k - r = k^2 - rv$

$rv - r = k^2 - k$

$(v-1)r = k(k-1)$

To prove this without characters, just a double counting argument:
Count ordered pairs $d_1 \neq d_2$ in D. $\quad k(k-1) = r(v-1)$

choices for $d_1 \in D$ $\quad$ choices for $1 \neq d_2 \in D$

Now let χ be nonprincipal.

$\chi(\delta)\overline{\chi(\delta)} = n + r\cancel{\chi(\gamma)}$ 0

$|\chi(\delta)|^2 = n \Rightarrow |\chi(\delta)| = \sqrt{n}$

$\chi(\sum_g a_g g) = \sum_g a_g \chi(g)$

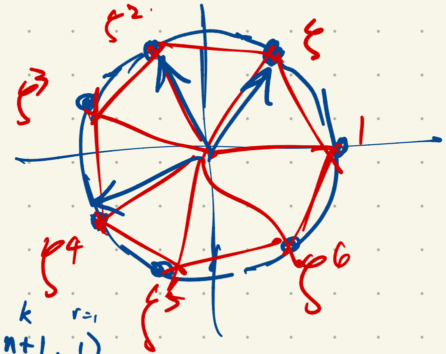
$\chi((\sum_g a_g g)^*) = \chi(\sum a_g g^{-1}) = \sum a_g \chi(g)^{-1} = \overline{\sum a_g \chi(g)}$

eg. $D = \{g, g^2, g^4\}$

$\delta = g + g^2 + g^4$

$\chi(\delta) = \xi + \xi^2 + \xi^4 \quad , \quad \xi = e^{2\pi i/7}$

$|\chi(\delta)| = \sqrt{7}$



In $G = C_n$, $|D| = n+1$, $D \subset G$ is a $(\overset{v}{n^2+n+1}, \overset{k}{n+1}, \overset{r=1}{1})$ diff. set iff $|\chi(\delta)| = \sqrt{n}$ for all nonprincipal characters of C_n.

Given a finite group G with $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, $\chi_1, \dots, \chi_k$ form a basis for all class functions $G \to \mathbb{C}$.

$\chi_i + \chi_j$ is a class function.

$\chi_i \chi_j$ - - — - - $\Rightarrow \chi_i \chi_j =$ linear comb. of irred. chars of G.

$\chi_i(g) = \mathrm{tr}\, \pi_i(g)$

$\chi_j(g) = \mathrm{tr}\, \pi_j(g)$

$(\chi_i + \chi_j)(g) = \mathrm{tr} \left[\begin{array}{c|c} \pi_i(g) & 0 \\ \hline 0 & \pi_j(g) \end{array}\right]$

$\chi_i(1) + \chi_j(1)$

$\underbrace{\chi_i(1)}_{n_i} \underbrace{\chi_j(1)}_{n_j}$

$(\chi_i \chi_j)(g) = \chi_i(g)\chi_j(g) = \mathrm{tr} \begin{bmatrix} ? \end{bmatrix}$

what representation has $\chi_i \chi_j$ as ~~its~~ character

i.e. trace

If A, A' are $m \times m$, B, B' are $n \times n$

$(A \otimes B)(A' \otimes B') = (AA') \otimes (BB')$

then $A \otimes B$ is $mn \times mn$:

$$A \otimes B = \left[\begin{array}{c|c|c|c} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \hline a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \hline \vdots & \vdots & \ddots & \\ \hline a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{array}\right]$$

$\mathrm{tr}(A \otimes B) = (a_{11} + a_{22} + \cdots + a_{mm})\,\mathrm{tr}\, B = (\mathrm{tr}\, A)(\mathrm{tr}\, B)$

Character table of S_5 using newer content on representations

$\lvert C_G(g)\rvert$	120	12	8	6	4	5	6
g	$()$	(12)	$(12)(34)$	(123)	(1234)	(12345)	$(123)(45)$
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	1	-1
χ_3	4	2	0	1	0	-1	-1
χ_4	4	-2	0	1	0	-1	1
χ_5	5	1	1	-1	-1	0	1
χ_6	5	-1	1	-1	1	0	-1
χ_7	6	0	-2	0	0	1	0
χ	5	3	1	2	1	0	0
$\chi_i = \chi - \chi_1$	4	2	0	1	0	-1	-1

$[\chi_i, \chi_i] = 1$. Check!

$$[\chi_1, \chi_1] = \frac{1}{120} + \frac{1}{12} + \frac{1}{8} + \frac{1}{6} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = 1$$

$$[\chi, \chi] = \frac{\cancel{25}^{\,5}}{\cancel{120}_{\,24}} + \frac{\cancel{9}^{\,3}}{\cancel{12}_{\,4}} + \frac{1}{8} + \frac{4}{6} + \frac{1}{4} + 0 + 0$$

$$= \frac{5 + 18 + 3 + 16 + 6 + 0 + 0}{24}$$

$$= \frac{48}{24} = 2.$$

$[\chi, \chi_1] = 1$ as before

$\chi = \chi_1 + \chi_i$, $\chi_i \neq \chi_1$

$\chi = \sum a_i \chi_i$

$[\chi, \chi] = \sum a_i^2$

Another way to know χ_i $(= \chi - \chi_1)$ is irreducible: χ is a perm. character of a doubly trans. perm. group. We'll prove this later!

$$120 = 1^2 + 1^2 + 4^2 + 4^2 + \overbrace{n_5^2 + n_6^2}^{50} + \overset{36}{n_7^2}$$
$$\underbrace{n_5^2 + n_6^2 + n_7^2}_{86}$$

$n_i \mid |G|$

$n_5, n_6, n_7 \in \{2, 3, 4, 5, 6, \cancel{7}\}$

$n_5^2, n_6^2, n_7^2 \in \{4, 9, 16, 25, 36, \cancel{49}\}$

Col. orthogonality: $1 + 1 + 4 + 4 + a^2 + a^2 = 12 \Rightarrow a^2 = 1 \Rightarrow a = \pm 1$

Col. orthogonality: $1 + 1 + 0 + 0 + 5a + 5a + 6b = 0 \Rightarrow 2 + 10a + 6b = 0 \Rightarrow 1 + 5a + 3b = 0$

$b = -\frac{1}{3}(1 + 5a)$

$a, b \in \mathbb{R}$ since $\chi((12)(34)) = \chi([(12)(34)]^{-1}) = \overline{\chi((12)(34))}$

$1 + 1 + 0 + 0 + a^2 + a^2 + b^2 = 8 \Rightarrow 2 + 2a^2 + b^2 = 8 \Rightarrow 2a^2 + b^2 = 6 \Rightarrow 2a^2 + \frac{1}{9}(1 + 5a)^2 = 6$

$18a^2 + 1 + 10a + 25a^2 = 54$

$43a^2 + 10a - 53 = 0$

$(43a + 53)(a - 1) = 0$

$a = 1$ or $\cancel{-\frac{53}{43}}$. But char. values are alg integers.

$b = -2$

Character table of S_5 using newer content on representations

$\lvert C_G(g)\rvert$	120	12	8	6	4	5	6
g	$()$	(12)	$(12)(34)$	(123)	(1234)	(12345)	$(123)(45)$
χ_1	1	1	1	1	1	1	1
χ_2	1	−1	1	1	−1	1	−1
χ_3	4	2	0	1	0	−1	−1
χ_4	4	−2	0	1	0	−1	1
χ_5	5	1	1	−1	−1	0	1
χ_6	5	−1	1	−1	1	0	−1
χ_7	6	0	−2	0	0	1	0

Standard perm. module

Standard perm. repn. of S_5 (of degree 5) has perm. char. $\chi_1 + \chi_3$.

We also get an irred. rep. of degree 5 from $S_5 \cong PGL_2(\mathbb{F}_5)$ frac. linear transf. on $\mathbb{F}_5 \cup \{\infty\}$ (six points) $0,1,2,3,4,\infty$ which is also doubly trans. so its perm. char of degree 6 is χ_1 + irred. of degree 5.

It's actually $\chi_1 + \chi_6$. Then $\chi_6\chi_2 = \chi_5$.

Where does χ_7 (irred of degree 6) come from? One answer: Use Specht modules for rep. theory of S_n.

Another approach: S_5 has an irred. rep. of degree 4 coming from the standard module V, $\dim V = 4$.

S_5 permutes $\mathbb{C}^5$ naturally by permuting: $\sigma: (x_1, \dots, x_5)^T \longrightarrow (x_{\sigma(1)}, \dots, x_{\sigma(5)})^T$ with $\langle (1,1,1,1,1)^T \rangle$ invariant.

$V = \mathbb{C}^5 / \langle (1,1,1,1,1)^T \rangle$. Basis for $\mathbb{C}^5$ is $e_1, \dots, e_5$. Then for V use $e_1, e_2, e_3, e_4, e_5 = -e_1 - e_2 - e_3 - e_4$.

$$\pi_3((12345)) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix}, \quad \operatorname{tr} \pi_3((12345)) = \chi_3((12345)) = -1$$

The module for π_7, χ_7 is the exterior square $V \wedge V = \Lambda^2 V$.

Think of $V \wedge V$ as skew-symmetric 4×4 matrices S

I will use right-to-left composition in S_5 to be consistent with linear transformations of V (right-to-left composition, acting on column vectors)

Action of $\sigma \in S_5$ on such matrices is $\pi_7(\sigma) \cdot S = \pi_3(\sigma)\, S\, \pi_3(\sigma)^T$

invertible 4×4 matrices

$$S = \begin{bmatrix} 0 & \alpha & \beta & \gamma \\ -\alpha & 0 & \delta & \varepsilon \\ -\beta & -\delta & 0 & \eta \\ -\gamma & -\varepsilon & -\eta & 0 \end{bmatrix} \qquad S^T = -S$$

If $\sigma, \tau \in S_5$ then $\pi_3(\sigma\tau) = \pi_3(\sigma)\pi_3(\tau)$ so

$$\pi_7(\sigma\tau)\cdot S = \pi_3(\sigma\tau) S \pi_3(\sigma\tau)^T = \pi_3(\sigma)\pi_3(\tau) S (\pi_3(\sigma)\pi_3(\tau))^T = \pi_3(\sigma)\pi_3(\tau) S \pi_3(\tau)^T \pi_3(\sigma)^T = \pi_7(\sigma)(\pi_7(\tau) S)$$

Exterior product $V \wedge V = \langle e_i \wedge e_j : 1 \le i < j \le 4 \rangle$ $\qquad u \wedge v = -v \wedge u$

Basis for $V \wedge V$ is $e_{12}, e_{13}, e_{14}, e_{23}, e_{24}, e_{34}$ where $e_{ij} = -e_{ji} = e_i \wedge e_j$

How does $(12345) \in S_5$ act on $V \wedge V$?

$$\begin{aligned}
e_{12} &= e_1 \wedge e_2 \longmapsto e_2 \wedge e_3 = e_{23} \\
e_{13} &= e_1 \wedge e_3 \longmapsto e_2 \wedge e_4 = e_{24} \\
e_{14} &= e_1 \wedge e_4 \longmapsto e_2 \wedge e_5 = e_2 \wedge (-e_1 - e_2 - e_3 - e_4) = e_{12} - e_{23} - e_{24} \\
e_{23} &= e_2 \wedge e_3 \longmapsto e_3 \wedge e_4 = e_{34} \\
e_{24} &= e_2 \wedge e_4 \longmapsto e_3 \wedge e_5 = e_3 \wedge (-e_1 - e_2 - e_3 - e_4) = e_{13} + e_{23} - e_{34} \\
e_{34} &= e_3 \wedge e_4 \longmapsto e_4 \wedge e_5 = e_4 \wedge (-e_1 - e_2 - e_3 - e_4) = e_{14} + e_{24} + e_{34}
\end{aligned}$$

Matrix of $\pi_7((12345))$ is

$$\begin{array}{c|c}
 & \begin{matrix} 12 & 13 & 14 & 23 & 24 & 34 \end{matrix} \\
\begin{matrix} 12 \\ 13 \\ 14 \\ 23 \\ 24 \\ 34 \end{matrix} & \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 & 1 \end{bmatrix}
\end{array}$$

$\chi_7((12345)) = \operatorname{tr} \pi_7((12345)) = 1$

There is also a symmetric square S^2V.

If $\dim V = n$ then the alternating square $V \wedge V = \Lambda^2 V$ has dimension $\binom{n}{2}$; the symm. square S^2V has dimension $\binom{n+1}{2}$.

For $n=4$, $\dim V = 4$ with basis e_1, e_2, e_3, e_4, S^2V has basis e_{ij}, $1 \le i \le j \le 4$.

$$\begin{bmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \varepsilon & \eta & \lambda \\ \gamma & \eta & \mu & \nu \\ \delta & \lambda & \nu & \rho \end{bmatrix}$$

If $V = \mathbb{C}^2$ then take $\{x, y\}$ basis for V;

S^kV has basis $\{x^k, x^{k-1}y, x^{k-2}y^2, \dots, y^k\}$

↑ homogeneous polys in x, y of degree k.

$\dim(S^kV) = \binom{n+k-1}{k}$

Eg. the group $G = GL_2(F)$ (char $F \ne 2$) has an irreducible representation of degree 3 given by S^2V where G acts naturally on $V = F^2$.

$A \longmapsto \left[\begin{array}{c|c} A & \begin{matrix} 0 \\ 0 \end{matrix} \\ \hline \begin{matrix} 0 & 0 \end{matrix} & 1 \end{array}\right]$ is reducible.
2×2

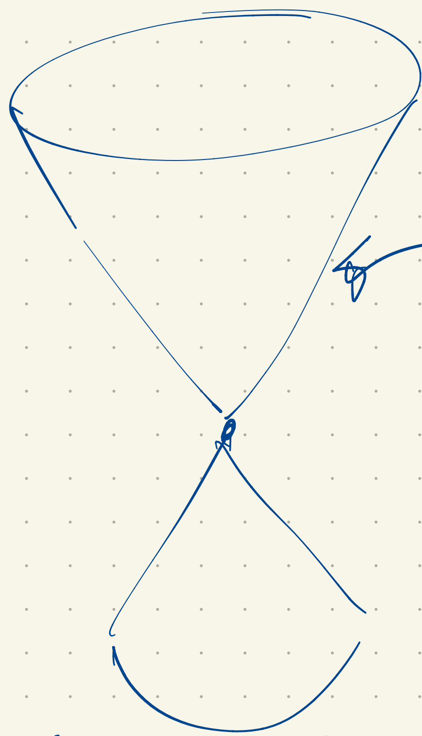
$A : \begin{bmatrix} x \\ y \end{bmatrix} \longmapsto A \begin{bmatrix} x \\ y \end{bmatrix}$ $\qquad \begin{bmatrix} x^2 \\ xy \\ y^2 \end{bmatrix} \longmapsto \begin{bmatrix} \cdots \\ \cdots \\ \cdots \end{bmatrix}$

There is no nontrivial invariant subspace but there is an invariant subset which is a cone.

$S^2V = \{\alpha x^2 + \beta xy + \gamma y^2 : \alpha, \beta, \gamma \in F\}$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \begin{bmatrix} x \\ y \end{bmatrix} \longmapsto \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}$$

$$A(\underbrace{\alpha x^2 + \beta xy + \gamma y^2}_{\substack{\uparrow \\ S^2V}}) = \alpha(ax+by)^2 + \beta(ax+by)(cx+dy) + \gamma(cx+dy)^2 = (\quad)x^2 + (\quad)xy + (\quad)y^2$$



$$\{\alpha x^2 + \beta xy + \gamma y^2 \;:\; \beta^2 - 4\alpha\gamma = 0\}$$

Mini-goal: Why you cannot hear the shape of a drum (necessarily). GWW Theorem

Let G (finite group) act on a (finite) set X. Every $g \in G$ gives a permutation on X which we write as $x \mapsto x^g$.

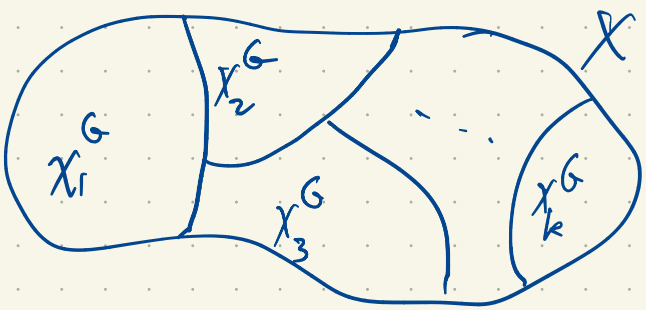
So $x \xrightarrow{g} x^g \xrightarrow{h} (x^g)^h = x^{gh}$ (left-to-right composition of maps). The map $G \to \mathrm{Sym}\,X = \{\text{permutations of } X\}$ is a homomorphism, not necessarily injective. (If so then the action is faithful.)

In general every $x \in X$ has a stabilizer $G_x = \{g \in G : x^g = x\} \leq G$. The orbit of x is $x^G = \{x^g : g \in G\} \subseteq X$.

$|x^G| = [G : G_x] = \dfrac{|G|}{|G_x|}$. There is a one-to-one correspondence

$$x^G \longleftrightarrow G_x \backslash G = \{\text{right cosets of } G_x\}$$
$$x^g \longleftrightarrow G_x g$$
$$x \longleftrightarrow G_x$$

Orbit-counting formula. If G has k orbits on X, say $X = x_1^G \sqcup x_2^G \sqcup \cdots \sqcup x_k^G$.



Then $k =$ average number of fixed points of $g \in G$.

Let $\chi(g) =$ number of points of X fixed by g i.e.

$= |\{x \in X : x^g = x\}|$. This is the permutation character of our action of G on X.

Theorem $k = \frac{1}{|G|}\sum_{g\in G} \chi(g)$.

Proof Count in two different ways the number of pairs $(x,g) \in X \times G$ such that $x^g = x$.
One one hand, the number of such pairs is $\sum_{g\in G}\chi(g)$. On the other hand, this equals

$$\sum_{x\in X} |\{g\in G : x^g = x\}| = \sum_{x\in X}|G_x| = \sum_{i=1}^k \sum_{x\in x_i^G} |G_x| = \sum_{i=1}^k \sum_{x \in x_i^G} \frac{|G|}{|x_i^G|} = \sum_{i=1}^k \cancel{|x_i^G|}\cdot\frac{|G|}{\cancel{|x_i^G|}} = k|G|. \qquad \square$$

$$|G_{x_i}| = \frac{|G|}{|x_i^G|}$$

If G permutes X transitively, so that there is just 1 orbit, fix a point $1 \in X$ and let $H = G_1 \le G$. Then the action of G on X is the same as G acting on right cosets of H i.e. $H\backslash G = \{Hg : g \in G\}$.
There are $[G:H] = |H\backslash G| = \frac{|G|}{|H|}$ such right cosets. Then the permutation character $\chi = 1_H^G$ = induced character
(1_H = principal character on H; induce it up to G). Let k be the number of orbits of H on X.
The number of orbits of G on $X \times X$ by the diagonal action i.e. $\underset{\in X\times X}{(x,y)} \xrightarrow{\;g\,\in G\;} (x^g, y^g)$ is ? (at least two unless $|X|=1$.)
Note: the diagonal $\{(x,x) : x \in X\}$ is one such orbit. $(x,x)^g = (x^g, x^g)$

Theorem The following quantities are the same:

(i) The number of orbits of H on X.

(ii) " " " " G on $X \times X$.

(iii) $[\chi,\chi]_G$.

First show (i) = (ii): Each orbit of G on $X \times X$ has a representative $(1,y)$, $y \in X$, so it suffices to consider only orbit representatives of this type. But two points $(1,y), (1,y') \in X \times X$ are in the same G-orbit iff $(1,y)^g = (1,y')$ for some $g \in G$, iff $y^h = y'$ for some $h \in H$. This proves (i) = (ii).