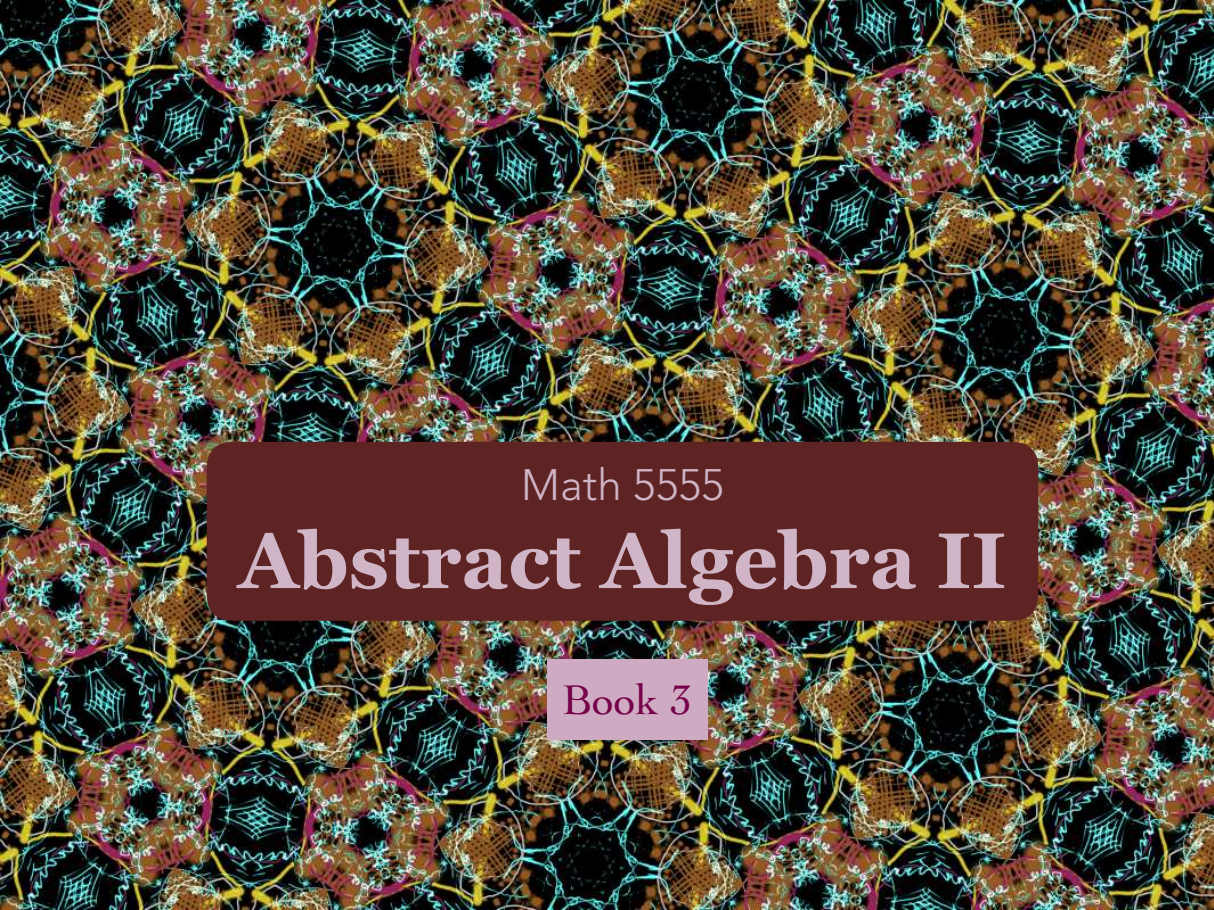


Math 5555

Abstract Algebra II

Book 3

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

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

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

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

$e_j = e_j(\lambda_{i,1}, \dots, \lambda_{i,n_i})$ 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.

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

The center of R (semisimple algebra) is

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

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

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

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

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

($n_1 \times n_1$, $n_2 \times n_2$, $n_k \times n_k$ blocks)

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

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

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

Let $K_1 \cdots K_k \subset G$ be the conj. classes i.e. $G = K_1 \sqcup K_2 \sqcup \cdots \sqcup K_k$

For $1 \le i \le k$, let $z_i = \sum_{g \in K_i} g$ = sum of elements in K_i ($K_1 = \{1\}$)

$z_i \in Z(\mathbb{C}G)$ because $gz_i = z_i g$, $gz_i g^{-1} = z_i$

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

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 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). $C_R(R) = Z(R)$

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 R-simple 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, $R\phi(v_0) = N$.

$\phi(Rv_0)$

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, $M \cong M/\ker\phi \cong \phi(M) = N$. 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:

$$\tilde{\phi}(rm) = \phi(rm) - cIrm = r\phi(m) - crm = r(\phi(m) - cm) = r\tilde{\phi}(m)$$
$$\tilde{\phi}(m+m') = \tilde{\phi}(m) + \tilde{\phi}(m'). \qquad (r \in R;\ m, m' \in M)$$

$v_0 \in \ker \tilde{\phi} \neq 0 \Rightarrow \ker \tilde{\phi} = M \Rightarrow \tilde{\phi} = 0 \Rightarrow \phi = cI$. □

Remark 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 RG-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 $gv = \underset{m \times m}{\pi(g)}\, \underset{m \times 1}{v} \in \mathbb{C}^m$

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

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

$$\begin{array}{ccc} \mathbb{C}^m & \xrightarrow{A} & \mathbb{C}^n \\ {\scriptstyle \pi(g)}\downarrow & & \downarrow{\scriptstyle \pi'(g)} \\ \mathbb{C}^m & \xrightarrow[A]{} & \mathbb{C}^n \end{array}$$

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

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

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

$\alpha(Av) = A(\alpha v)$ 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.

$\mathbb{C}^{n_1}$ $\quad\quad$ $\mathbb{C}^{n_k}$

$\pi_1 \quad \dots \quad \pi_k$

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, $\mathbb{C}^3$.

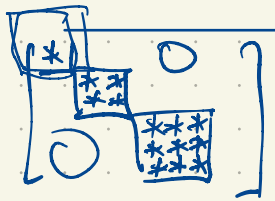
$A \in R$ acts on $V = \mathbb{C}^3$ by $\underset{3\times 1}{v} \longmapsto \underset{3\times 3}{A}\underset{3\times 1}{v}$.

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

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.

$R =$  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.

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

$M_1(R)$ $\quad$ $M_2(R)$ $\quad$ $M_3(R)$

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 $\mathbb{C}$

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

(R-endomorphisms = into itself)

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

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

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

The map $R \to \mathrm{End}_R(R)$, $a \overset{\psi}{\mapsto} \phi_a \in \mathrm{End}_R(R)$ is bijective.

If $a \in R$ such that $\phi_a = 0$ then $\phi_a(1) = 0$ so $1a = 0 \Rightarrow a = 0$. So $a \mapsto \phi_a$ is one-to-one.

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

If G is a group then $a \overset{f}{\mapsto} a^{-1}$ is an anti-automorphism $f(ab) = f(b)f(a)$

Similarly with an algebra.

If R is an algebra then the opposite algebra R° is the algebra with the same elements as R° with same vector space structure; only the multiplication is replaced by $x * y = yx$ ($x * y$ in R°, yx in R)

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

R° is not necessarily isomorphic to R. It is anti-isomorphic.

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

$G \to G \to G^\circ$ (inverse, then $\cdot$)

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:

$\phi(r) =$

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

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

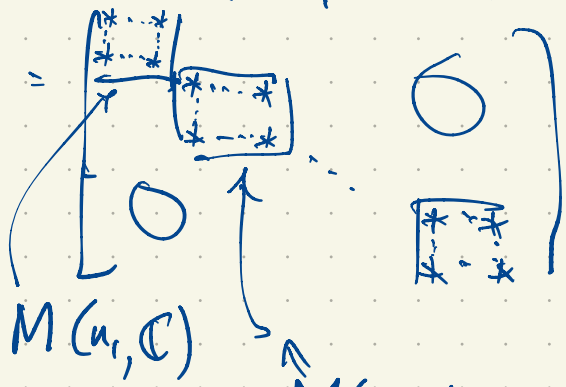
$\phi(r) = \phi(r_1) + \cdots + \phi(r_m)$, decompose each term with respect to our decomposition

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

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

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

$\begin{pmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1m} \\ \vdots & & & \vdots \\ \phi_{m1} & \cdots & \cdots & \phi_{mm} \end{pmatrix} =$



$\in M(n_1, \mathbb{C})$ $\quad \oplus M(n_2, \mathbb{C})$

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

$\| \quad$ anti-iso

$R^\circ \cong R$

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

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

p.29 The Center of the group algebra

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

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

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

$K_1, K_2, \dots, K_k$: conjugacy classes of $G = K_1 \sqcup \dots \sqcup K_k$ (partition)

$K_1 = \{1\}$

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

$\mathrm{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_k\}$ $\qquad n_i = \chi_i(1) = \deg \chi_i$

$\chi_1 = 1_G$ principal character

$n_1^2 + n_2^2 + \dots + n_k^2 = n$

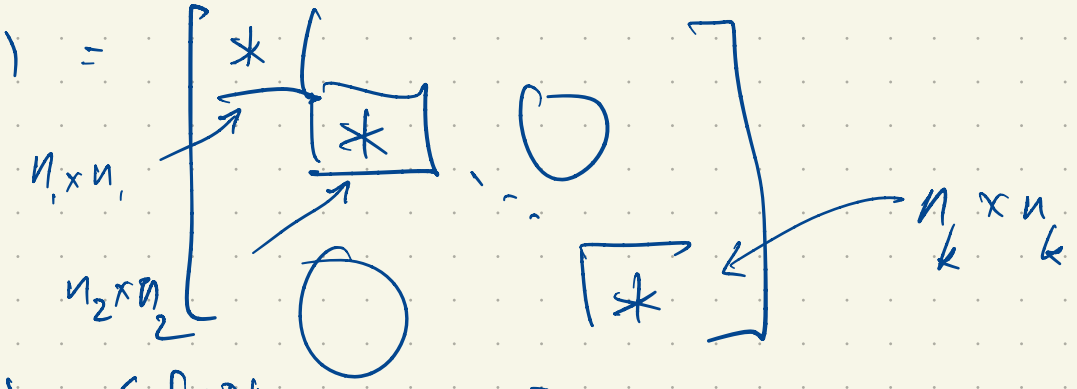
Moreover $n_i \mid n$ which we will prove today or Monday.

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

Reps of $K_1, \dots, K_k$ are $g_1, \dots, g_k$

Basis for $Z(\mathbb{C}G)$ is $\{\gamma_1, \gamma_2, \dots, \gamma_k\}$ where γ_i = sum of elements in K_i.

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



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

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

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

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

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 $c \in \mathbb{C}$

In particular $\pi_j(\gamma_i) = \underbrace{\omega_j(\gamma_i)}_{\in \mathbb{C}} I_{n_j}$ since $\gamma_i \in Z(\mathbb{C}G)$ by Schur's lemma.

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

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

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

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

$$\omega_\chi(\gamma_i) = \frac{|K_i|\chi(g_i)}{\chi(1)} \qquad (p.30)$$

pos. integers

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

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

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

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

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

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

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

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

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

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 different ways. $a_{223} = 3$

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

$\omega_\chi(\gamma_i) = \frac{|K_i|\chi(g_i)}{\chi(1)}$. $\omega_\chi: Z(\mathbb{C}G) \to \mathbb{C}$ 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 $a_{ijl} = \frac{|K_i||K_j|}{|G|} \sum_{\chi \in \mathrm{Irr}G} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_l)}}{\chi(1)}$. (non-negative integers)

Proof $\gamma_i \gamma_j = \sum_{l=1}^{k} a_{ijl} \gamma_l$. $\omega_\chi(\gamma_i) = \frac{|K_i|\chi(g_i)}{\chi(1)}$. Apply this homomorphism to $Z(\mathbb{C}G)$ on both sides:

$$\frac{|K_i|\chi(g_i)}{\chi(1)} \cdot \frac{|K_j|\chi(g_j)}{\chi(1)} = \sum_{l=1}^{k} a_{ijl} \frac{|K_l|\chi(g_l)}{\chi(1)}.$$

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

$$\sum_\chi \frac{|K_i||K_j|\chi(g_i)\chi(g_j)\overline{\chi(g_s)}}{\chi(1)} = \sum_\chi \sum_{l=1}^{k} a_{ijl}|K_l|\chi(g_l)\overline{\chi(g_s)}$$

$$= \sum_{l=1}^{k} a_{ijl}|K_l| \underbrace{\sum_\chi \chi(g_l)\overline{\chi(g_s)}}_{\delta_{ls}\frac{|G|}{|K_l|}}$$

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

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

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

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

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

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

(fixed i)

In $Z(\mathbb{C}G)$, we consider left-multiplication by $\omega_\chi(\gamma_i)$ 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 $\omega_\chi(\gamma_1) = |K_1|\,\omega_\chi(g_1)$, $g_1 = 1$, $|K_1| = 1$

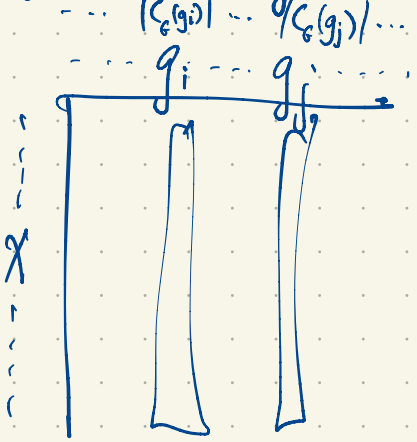
Column orthogonality of char. table of G:

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

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

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

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



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

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

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

$$= \sum_{\chi\in\mathrm{Irr}G} \chi(1)\,\omega_\chi(\gamma_i)\,\overline{\chi(g_i)}$$

($\chi(1)$: alg. int.; $\omega_\chi(\gamma_i)$: alg. int.; $\overline{\chi(g_i)}$: alg. int.)

is an alg. int.

$$\frac{|G|}{|\chi(1)|} = \sum_\chi [\text{alg. int.}]$$

is an alg. int. Also in $\mathbb{Q}$.

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

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

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. $G = \{1, g, \cdots, g^6\}$ 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. Also a diff. set in the cyclic gp. of order 21.

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

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

$D+1 = \{2, 3, 5\}$

$D+2 = \{3, 4, 6\}$