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 $\lambda_{i,1}^t+\cdots+\lambda_{i,n_i}^t$, $1\le t\le n_i$ 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

Use (Newton's identities)

$$(x+\lambda_{i,1})(x+\lambda_{i,2})\cdots(x+\lambda_{i,n_i}) = x^{n_i}+e_1x^{n_i-1}+e_2x^{n_i-2}+\cdots+e_{n-1}x+e_n$$

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.

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

$Z(M(n,\mathbb{C}))=\{\lambda I : \lambda\in\mathbb{C}\}$, $I=I_n=\begin{bmatrix}1&&0\\&\ddots&\\0&&1\end{bmatrix}_{n\times n}$

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

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

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

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

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

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 $gz_i = z_i g$
$gz_i g^{-1} = z_i$

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

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

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 $\qquad F$

$F[G] = FG$ 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

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

(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 $M \ncong N$ 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, $R\phi(v_0) = N$.
 $R\phi(v_0) = \phi(Rv_0)$

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, $M \cong M/_{\ker\phi = 0} \cong \phi(M) = N$
This contradicts $M\ncong N$.

(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:

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

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

<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 $\mathbb{C}^n$, $\overset{\mathbb{C}^n}{gv} = \underbrace{\pi'(g)}_{n\times n}\underbrace{v}_{n\times 1} \in \mathbb{C}^n$

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 $\overset{\mathbb{C}^m}{V}$ and $\overset{\mathbb{C}^n}{W}$ 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.

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

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

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 $\underbrace{v}_{3\times 1} \longmapsto \underbrace{A}_{3\times 3}\underbrace{v}_{3\times 1}$.

$$R = \begin{bmatrix} * & 0 & 0 \\ * & 0 & 0 \\ * & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & * & 0 \\ 0 & * & 0 \\ 0 & * & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & * \end{bmatrix} \quad \text{contains} \quad \begin{bmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} [1\ 1\ 0]$$

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.

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

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 $\mathbb{C}$

$\mathrm{End}_R(R) = \{ \underset{\text{into itself}}{R\text{-endomorphisms}} \text{ of } R \}$ 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 $\phi(a) = \phi_a(1) = 0$ so $\underbrace{1a}_{} = 0 \implies a = 0$. 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 $R = \mathbb{C}G$? $\quad \mathrm{End}_R(R) = R^{\circ}$.

$R = I_1 \oplus I_2 \oplus \cdots \oplus I_m$ 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 $\mathbb{C}$

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

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

$M(n_2, \mathbb{C})$

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

$\parallel$

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

$R = \mathbb{C}G$ 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

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

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

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

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

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 $\gamma_i =$ sum of elements in K_i.

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 $\pi_j(\sum_g a_g g) = \sum_g a_g \pi_j(g)$.

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

$Z(\mathbb{Z}G) =$ 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.