

3204/M204 Representation Theory Notes

Based on the 2013 autumn lectures by Mr J Nadim

The Author(s) has made every effort to copy down all the content on the board during lectures. The Author(s) accepts no responsibility whatsoever for mistakes on the notes nor changes to the syllabus for the current year. The Author(s) highly recommends that the reader attends all lectures, making their own notes and to use this document as a reference only.

lectured by a.jamil@ud.ac.uk

office hour - Mon 2pm, Room 603.

Recommended text: Curtis and Reiner, Representations of finite groups and associative algebras. (reference only) James and Liebeck, Group Representations and Characters

COMPLEX REPRESENTATION THEORY.

Goal of course: To represent any finite group G as a group of invertible matrices over \mathbb{F} (i.e. we want to give G the same structure).

Definition A representation is a type of group homomorphism.

Definition let \mathbb{F} be a field. then we define $GL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) : \det A \neq 0\} = \{\text{invertible } n \times n \text{ matrices over } \mathbb{F}\}$.

Recall - $GL_n(\mathbb{F})$ is a group under matrix multiplication.

Definition let \mathbb{F} be a field, G be a finite group and V be an \mathbb{F} -vector space of dimension n (i.e. $V = \mathbb{F}^n$).

Define an \mathbb{F} -representation of G , ρ , as the group homomorphism $\rho: G \rightarrow GL_n(V) = \{\phi: V \rightarrow V \text{ st. } \phi \text{ is an invertible } \mathbb{F}\text{-linear map}\} = \{\text{is an automorphism}\}$

If we choose a basis for V , say $B = \{e_1, \dots, e_n\}$, then $GL_n(V) \cong GL_n(\mathbb{F})$.

so in this way, an \mathbb{F} -representation of G is $\rho: G \rightarrow GL_n(\mathbb{F})$, where ρ is a group homomorphism i.e. $\rho(gh) = \rho(g)\rho(h) \forall g, h \in G$.

Definition If $\dim(V) = n, n \geq 1$, then n is called the degree/dimension of the representation ρ .

Examples of representations -

1. (Trivial representation) let G be any group and define $\rho: G \rightarrow GL_n(\mathbb{C})$ by $\rho(g) = I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \forall g \in G$.

2. (Trivial representation for cyclic groups over \mathbb{C}).

Fix n and let $C_m = \langle x: x^m = 1 \rangle$, then define $\rho: C_m \rightarrow GL_n(\mathbb{C})$ by $\rho(x) = I_n$. Note that we need to know where the generator of our group goes (here, x).
Then $\rho(x^k) = \rho(x) \dots \rho(x) = I_n \dots I_n = I_n \forall k \in [1, m]$.

For instance, take $C_3 = \langle 1, x, x^2 \rangle$ by $\rho(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$ i.e. $\rho: C_3 \rightarrow GL_2(\mathbb{C})$. Then $\rho(x^3) = \rho(x)\rho(x)\rho(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.
(this is well-defined as $x^3 = 1$, so we do expect that $\rho(x^3) = \rho(1) = I_2$.)

3. (A non-trivial representation of cyclic groups)

let $\rho: C_m \rightarrow GL_n(\mathbb{F})$ be defined by $\rho(x) = A$ for some $A \in GL_n(\mathbb{F}) \neq I_n$. For ρ to be a complex representation, A must satisfy the group law:

$x^m = 1$ for C_m , so we need $\rho(x^m) = I_n$ i.e. we need A s.t. $\rho(x^m) = \rho(x)^m = A^m = I_n$.

For instance, we can take $A = \begin{pmatrix} \xi & & 0 \\ & \ddots & \\ 0 & & \xi \end{pmatrix}$, where $\xi = e^{\frac{2\pi i}{m}}$. Then $A^m = I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

4. (Trivial representation for D_{2n}).

$D_{2n} = \langle x, y \mid x^n = y^2 = 1, yx = x^{-1}y \rangle$. Note that D_{2n} has two generators, so we need to determine where each is sent.

Define the trivial representation as $\rho: D_{2n} \rightarrow GL_k(\mathbb{F})$ by $x \mapsto I_k, y \mapsto I_k, \forall g \mapsto I_k$. Note that if $k=1$, this means that $x \mapsto 1, y \mapsto 1, 1 \mapsto 1$.

5. (A non-trivial 1D representation of D_6)

$D_6 = \langle 1, x, x^2, y, xy, x^2y \rangle = \langle x, y \mid x^3 = y^2 = 1, yx = x^2y \rangle$. let $\rho: D_6 \rightarrow GL_1(\mathbb{C}) = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ be defined by $x \mapsto 1, y \mapsto -1, 1 \mapsto 1$.

To verify that this is a representation, we need to check the group laws: i.e. must show $\rho(x^3) = \rho(y^2) = \rho(1) = 1$ and $\rho(yx) = \rho(x^2y)$.

check: $\rho(x^3) = \rho(x)^3 = 1 \times 1 \times 1 = 1 \checkmark$ $\rho(y^2) = \rho(y) \cdot \rho(y) = (-1) \times (-1) = 1 \checkmark$ $\rho(yx) = \rho(y)\rho(x) = (-1) \times (1) = -1, \rho(x^2y) = \rho(x)\rho(x)\rho(y) = 1 \times 1 \times (-1) = -1 \checkmark$

6. (A non-trivial 2D representation of D_6/\mathbb{C}).

Represent D_6 : let $\rho: D_6 \rightarrow GL_2(\mathbb{C})$ by $1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, x \mapsto \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. We need to check that ρ defines a representation:

$\rho(x^3) = \rho(x)^3 = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \checkmark$ $\rho(y^2) = \rho(y)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \checkmark$

$\rho(yx) = \rho(y)\rho(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \rho(x^2y) = \rho(x)^2\rho(y) = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \Rightarrow \rho(yx) = \rho(x^2y) \checkmark$ The necessary group laws are satisfied.

7. (Another non-trivial 2D representation of D_6).

Define $\rho: D_6 \rightarrow GL_2(\mathbb{C})$ by $1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, x \mapsto \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ where $w = e^{\frac{2\pi i}{3}}$. check that ρ defines a representation:

$\rho(x^3) = \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}^3 = \begin{pmatrix} w^3 & 0 \\ 0 & w^6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \checkmark$ $\rho(y^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \checkmark$

$\rho(yx) = \rho(y)\rho(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix} = \begin{pmatrix} 0 & w^2 \\ w & 0 \end{pmatrix}, \rho(x^2y) = \rho(x)^2\rho(y) = \begin{pmatrix} w^2 & 0 \\ 0 & w^4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & w^2 \\ w & 0 \end{pmatrix} = \rho(yx) \checkmark$

8. (A 3D representation of S_n)

Recall - S_n is the group of invertible permutations on $\{1, \dots, n\}$ and $|S_n| = n!$

Take $n=3$, so consider $S_3 = \{1, (12), (13), (23), (123), (132)\}$. Recall that $S_3 \cong D_6$ by setting $(1) \mapsto 1, (123) \mapsto x, (12) \mapsto y$.

We now consider the permutation representation in 3D (works for any n). Let $V = \mathbb{F}^3$ be a 3D vector space with the standard basis $B = \{e_1, e_2, e_3\}$.

Define the representation $\rho: S_3 \rightarrow GL_3(\mathbb{C})$ by $\rho(\sigma) \cdot e_i = e_{\sigma(i)} \forall \sigma \in S_3$. We check that this actually defines a representation.

① $\rho(1) \cdot e_i = e_{(1)(i)} = e_i \forall i \Rightarrow \rho(1) = I_3$ ② $\rho(\sigma\tau) \cdot e_i = e_{\sigma\tau(i)} = e_{\sigma(\tau(i))} = \rho(\sigma) \cdot e_{\tau(i)} = \rho(\sigma) \rho(\tau) \cdot e_i \Rightarrow \rho(\sigma\tau) = \rho(\sigma) \rho(\tau) \forall \sigma, \tau$

So, returning to our example, let $\sigma = (1\ 2\ 3)$, $\tau = (1\ 2)$ be the generators of S_3 . Then, $\sigma^3 = \tau^2 = (1)$ and $\tau\sigma = \sigma^2\tau$.

We next to find the representation $\rho: S_3 \rightarrow GL_3(\mathbb{C})$. Clearly, $\rho(1) = I_3$ by definition. We need to find (1) $\rho(\sigma)$ and (2) $\rho(\tau)$.

(1) For σ , $\rho(\sigma) \cdot e_1 = e_{(1\ 2\ 3)(1)} = e_2$, $\rho(\sigma) \cdot e_2 = e_{(1\ 2\ 3)(2)} = e_3$, $\rho(\sigma) \cdot e_3 = e_{(1\ 2\ 3)(3)} = e_1 \Rightarrow \rho(\sigma) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (e_2\ e_3\ e_1) \in GL_3(\mathbb{C})$.

(2) For τ , $\rho(\tau) \cdot e_1 = e_{(1\ 2)(1)} = e_2$, $\rho(\tau) \cdot e_2 = e_{(1\ 2)(2)} = e_1$, $\rho(\tau) \cdot e_3 = e_{(1\ 2)(3)} = e_3 \Rightarrow \rho(\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (e_2\ e_1\ e_3) \in GL_3(\mathbb{C})$.

To summarise, our representation is $\rho: S_3 \rightarrow GL_3(\mathbb{C})$ with $(1) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(1\ 2\ 3) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $(1\ 2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

For checking that this is a representation, we need $\rho(\sigma^3) = \rho(\tau^2) = I_3$, and $\rho(\tau\sigma) = \rho(\sigma^2\tau)$. This is verifiable by matrix algebra.

Generalised permutation representation.

We can generalise a permutation representation as follows: let G be a group, and let V be a finite-dimensional vector space over \mathbb{F} . Then

- Choose a basis for V
- Let X be a set and choose a basis vector for each element x , say e_x
- Define the group action $G \times X \rightarrow X$ by $(g, x) \rightarrow g \cdot x$ where $1 \cdot x = x$, $g \cdot (h \cdot x) = (g \cdot h) \cdot x \forall x \in X, \forall g, h \in G$.
- Then, let $V = \bigoplus_{x \in X} \mathbb{F} e_x$
- Define $\rho: G \rightarrow GL_n(\mathbb{F})$ by $\rho(g) \cdot e_x = e_{g \cdot x}$ for any group action \circ . (e.g. conjugation $g \cdot h = ghg^{-1}$).

9. We represent D_6 over \mathbb{R} by $\rho: D_6 \rightarrow GL_2(\mathbb{R})$, where $x \mapsto \begin{pmatrix} \cos 2\pi/3 & -\sin 2\pi/3 \\ \sin 2\pi/3 & \cos 2\pi/3 \end{pmatrix}$ corresponding to rotation, and $y \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ corresponding to reflection.

In this course, we will get a complete answer to the question:

How many complex representations are there for G , up to conjugation, where

- (1) G will be always finite (2) $\mathbb{F} = \mathbb{C}, \mathbb{R}, \mathbb{F}_p$ (3) we require that $|G| \nmid \text{char}(\mathbb{F})$.

Note - $\text{char}(\mathbb{F}_2) = 2$ as $1+1=0$ in \mathbb{F}_2 , $\text{char}(\mathbb{F}_p) = p$ as $\underbrace{1+1+\dots+1}_p = 0$ in \mathbb{F}_p , $\text{char}(\mathbb{Q}) = \infty$.

(4) when $\mathbb{F} = \mathbb{C}$, then every matrix is diagonalisable.

$\forall g \in G, \exists n$ st: $g^n = 1$, so $\rho(g)^n = I_n \Rightarrow$ the matrix has characteristic polynomial $x^n - 1$, and over \mathbb{C} , $x^n - 1 = \prod (x - \xi_i)$ where ξ_i are roots of unity.

\Rightarrow the polynomial splits into distinct linear factors \Rightarrow every g has a minimal polynomial $\Rightarrow \rho(g)$ is diagonalisable.

Note - $x^n - 1$ does not generally split for \mathbb{R} , e.g. $x^2 - 1 = (x-1)(x+1)$.

(5) The theory breaks down for infinite groups. If $\rho: \mathbb{Z} \rightarrow GL_2(\mathbb{C})$. If $n \neq 0$, then $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ is not diagonalisable.

If $x \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, then $m(x) = (x-1)^2$.

Ex) Define the 3D representations $\sigma, \tau: D_6 \rightarrow GL_3(\mathbb{C})$ by $\sigma(x) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $\sigma(y) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $\tau(x) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\tau(y) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Show that σ and τ are the same representation.

Soln. Let $V = \mathbb{F}^3 = \text{span}_{\mathbb{F}} \{e_1, e_2, e_3\}$ where $\{e_1, e_2, e_3\}$ is the canonical basis. Now define a new basis $\{\phi_1, \phi_2, \phi_3\}$ by

$\phi_1 = e_1 + \frac{1}{2}e_3$, $\phi_2 = e_2 + \frac{1}{2}e_3$, $\phi_3 = -e_1 - e_2 - \frac{1}{2}e_3$.

(1) Apply $\tau(x)$ to $\{e_1, e_2, e_3\}$. $\tau(x)(e_1) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = e_2$, $\tau(x)(e_2) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} = -e_1 - e_2$, $\tau(x)(e_3) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = e_3$.

(2) Apply $\tau(x)$ to $\{\phi_1, \phi_2, \phi_3\}$. $\tau(x)(\phi_1) = \tau(x)(e_1 + \frac{1}{2}e_3) = \tau(x)(e_1) + \frac{1}{2}\tau(x)(e_3) = e_2 + \frac{1}{2}e_3 = \phi_2$, $\tau(x)(\phi_2) = \dots = \phi_3$, $\tau(x)(\phi_3) = \dots = \phi_1$.

\Rightarrow the matrix representation of $\tau(x)$ w.r.t. new basis $\{\phi_1, \phi_2, \phi_3\}$ is $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, so $\tau(x)$ on $\{\phi_1, \phi_2, \phi_3\}$ is the same as $\sigma(x)$ on $\{e_1, e_2, e_3\}$.

We check the same for y : then

(3) Apply $\tau(y)$ to $\{e_1, e_2, e_3\}$. $\tau(y)(e_1) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = e_2$, $\tau(y)(e_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = e_1$, $\tau(y)(e_3) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = e_3$.

(4) Apply $\tau(y)$ to $\{\phi_1, \phi_2, \phi_3\}$. $\tau(y)(\phi_1) = e_2 + \frac{1}{2}e_3 = \phi_2$, $\tau(y)(\phi_2) = \tau(y)(e_2 + \frac{1}{2}e_3) = e_1 + \frac{1}{2}e_3 = \phi_1$, $\tau(y)(\phi_3) = -e_2 - e_1 - \frac{1}{2}e_3 = \phi_3$.

Thus, the matrix representation of $\tau(y)$ w.r.t. new basis $\{\phi_1, \phi_2, \phi_3\}$ is $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ q.e.d.

Recall - when you choose a vector space V , you implicitly select a standard basis, $\{e_1, \dots, e_n\}$. We change the basis with conjugating matrix P .

This is an invertible automorphism of V .

Definition Let $A, B \in M_n(\mathbb{F})$. Then A is conjugate to B if $\exists T \in GL_n(\mathbb{F})$ s.t. $B = TAT^{-1} = T^{-1}AT$.

Definition Given two representations of G , $\rho: G \rightarrow GL_n(\mathbb{F})$ and $\rho': G \rightarrow GL_n(\mathbb{F})$, of degree n , we say that ρ' is conjugate/isomorphic/equiv. if $\exists T \in GL_n(\mathbb{F})$ s.t. $\rho'(g) = T\rho(g)T^{-1} \quad \forall g \in G$.

Examples -

1. Let $G = D_8$, $\mathbb{F} = \mathbb{C}$, and define $\rho: D_8 \rightarrow GL_2(\mathbb{C})$ by $x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $y \mapsto \begin{pmatrix} b & 0 \\ 0 & -1 \end{pmatrix}$. Take $T = \sqrt{2} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$. We have $T^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Then $\rho'(x) = T^{-1}\rho(x)T = \frac{1}{4} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} =$

2. Let $G = C_2 = \langle x \mid x^2 = 1 \rangle$, $\rho: C_2 \rightarrow GL_2(\mathbb{C})$ by $x \mapsto \begin{pmatrix} -5 & 12 \\ -2 & 5 \end{pmatrix} = A$ s.t. $A^2 = I_2$. Let $T = \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}$, so $T^{-1} = \frac{1}{-2+3} \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix}$.

Then $T^{-1}AT = \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} -5 & 12 \\ -2 & 5 \end{pmatrix} \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then let $\rho': C_2 \rightarrow GL_2(\mathbb{C})$ be given by $\rho'(x) = T^{-1}AT$.

Check the group law: $\rho'(x^2) = \rho'(x)\rho'(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I_2 \Rightarrow$ representations are equivalent.

Definition Let $\rho: G \rightarrow GL_n(\mathbb{F})$ be a representation. The kernel of the representation is $\text{Ker}(\rho) = \{g \in G \mid \rho(g) = I_n\}$.

Note - If $\text{Ker}(\rho) \triangleleft G$, then by the first isomorphism theorem, $G/\text{Ker}(\rho) \cong \text{Im}(\rho) \leq GL_n(\mathbb{F})$.

If $\text{Ker}(\rho) = \langle 1 \rangle$, then $G/\langle 1 \rangle \cong G \cong GL_n(\mathbb{F})$ is the trivial kernel.

Definition If $\text{Ker}(\rho) = \langle 1 \rangle$, then ρ is a faithful representation.

Note - If $\rho: G \rightarrow GL_n(\mathbb{F})$, by definition $1 \mapsto I_n$, so all other elements map to matrices different from identity $\Rightarrow \rho$ is injective.

Examples of faithful/non-faithful representations -

1. Trivial representation $\rho: G \rightarrow GL_n(\mathbb{F})$ by $\rho(g) = I_n \quad \forall g \in G$ is not faithful - all elements map to I_n .

2. 2D representation of D_8 over \mathbb{R} is faithful: $\rho: D_8 \rightarrow GL_2(\mathbb{R})$ by $x \mapsto \begin{pmatrix} \cos 2\pi/8 & -\sin 2\pi/8 \\ \sin 2\pi/8 & \cos 2\pi/8 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

since the transformations do not fix the vertices, we cannot get an identity transformation by construction.

3. The permutation representation of S_n , $\rho: S_n \rightarrow GL_n(\mathbb{C})$ by $\rho(\sigma) \cdot e_i = e_{\sigma(i)}$ is faithful.

To establish that it is faithful, we must show that $\text{Ker}(\rho) = \langle 1 \rangle$. Let $\sigma \in S_n$ and suppose $\rho(\sigma) \cdot e_i = e_{\sigma(i)} = e_i \quad \forall i \Leftrightarrow \sigma(i) = i \quad \forall i \Leftrightarrow \sigma = (1) \Leftrightarrow \text{Ker}(\rho) = \langle 1 \rangle$.

4. The representation $\rho: D_{2n} \rightarrow GL_n(\mathbb{F})$ by $x \mapsto 1, y \mapsto -1$ is not faithful. In fact, $\text{Ker}(\rho) = \langle 1, x, \dots, x^{n-1} \rangle \cong C_n$.

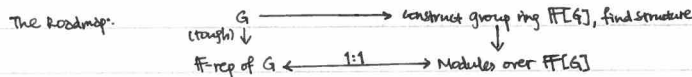
Let $g \in D_{2n}$, $g = x^i y^j$ for $0 \leq i < n, 0 \leq j < 1$. $\rho(x^i y^j) = \rho(x)^i \rho(y)^j = 1^i (-1)^j = 1 \Leftrightarrow j = 0 \Leftrightarrow g = x^i$ i.e. $g \in C_n \Leftrightarrow \text{Ker}(\rho) = C_n$.

4 October 2013
Mr. Jamil NADIM.
Maths 500.

Outline of Topics:

① Constructing all \mathbb{C} -representations of finite G up to conjugacy. ② Character Theory ③ Tensor products.

④ Real Representation Theory ⑤ Frobenius reciprocity.



RINGS, MODULES AND ALGEBRAS.

Definition A ring R is a set with 2 operations $(R, +, \cdot, 0, 1)$ satisfying the following axioms.

- (1) $a+b = b+a$ (2) $a+(b+c) = (a+b)+c = a+b+c$ (3) $\exists 0 \in R$, s.t. $\forall a, a+0 = 0+a = a$ (4) $\forall a \in R, \exists (-a) \in R$ s.t. $a+(-a) = 0$

Axioms (1)-(4) yield that $(R, +, 0)$ is an abelian group.

- (5) $\exists 1 \in R$ s.t. $a \cdot 1 = a = 1 \cdot a$ (6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (7) $a(b+c) = a \cdot b + a \cdot c$ (8) $(a+b) \cdot c = a \cdot c + b \cdot c$.

(9) If $a \cdot b = b \cdot a$, then R is also called a commutative ring.

Note - Rings in general are not commutative. In this course they may be non-commutative.

Examples of rings -

1. Commutative Rings: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \mathbb{F}[X], \mathbb{F}_p, \mathbb{F}[X]/I$

2. Non-commutative rings: Let R be a ring, define $M_n(R) = \{ (a_{ij}) \mid 1 \leq i, j \leq n; a_{ij} \in R \} = n \times n$ matrices over R .

Then for $n \geq 2$, $M_n(R)$ is not commutative, even if R is a field i.e. $M_n(\mathbb{F})$.

$M_n(R)$ is a ring: (addition) $(\alpha + \beta)_{ij} = \alpha_{ij} + \beta_{ij}$ (multiplication) $(\alpha\beta)_{ij} = \sum_{k=1}^n \alpha_{ik} \beta_{kj}$ (unit) $(1)_{ij} = I_n$ (zero) $(0)_{ij} = \{0 \quad \forall i, j\}$.

Note - The standard basis for $M_n(R)$, $(E_{ij})_{i,j} = \delta_{ij}$ do not have inverses.

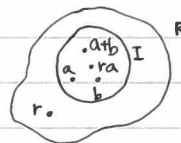
3. Upper triangular matrix rings $U_n(R) = \left\{ \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix} : a_{ij} \in R \right\}$. It is non-commutative so $U_n(R) \subset M_n(R)$.

Definition Let R, S be two rings. Define product $R \times S$ as a ring by

- ① A set $R \times S = \{(r, s) : r \in R, s \in S\}$ with operations
 (addition) $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$
 (multiplication) $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$
 (identity) $"1" = (1, 1)$
 (zero) $"0" = (0, 0)$.

Definition A subset $I \triangleleft R$ is called an ideal if

- ① $(I, +, 0)$ is an additive group i.e. $\forall a, b \in I, a+b \in I$, and obeys
 ② Absorbency: $\forall a \in I, \forall r \in R, r \cdot a \in I$



Examples of ideals -

1. If $R = \mathbb{Z}$. $0\mathbb{Z} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Z}$ (obvious). Also, $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal e.g. $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$.
 2. $(p) \subseteq \mathbb{F}[x]$, $(x^2-2) \subseteq \mathbb{Q}[x]$.

Definition Let R, S be two rings, then a ring homomorphism is a map $\phi: R \rightarrow S$ s.t.

- ① $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ ② $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$ } preserve $+$,
 ③ $\phi(0_R) = 0_S$

Note - $\phi(1_R) = 1_S$ does not always hold. For instance, in example of embedding: $\phi: M_2(\mathbb{R}) \rightarrow M_3(\mathbb{R}), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}, I_2 \mapsto I_3$.

- ④ $\phi(1_R) = 1_S$ if S is an integral domain or ϕ is an epimorphism (surjective).
 ⑤ If ϕ is bijective, then ϕ is called a ring isomorphism i.e. ϕ injective $\Leftrightarrow \text{Ker } \phi = \{0\} \Leftrightarrow \phi(a) = \phi(b) \Rightarrow a = b$
 ϕ surjective $\Leftrightarrow \text{Im } \phi = S \Leftrightarrow \forall b \in S \exists a \in R$ s.t. $\phi(a) = b$.

Examples of ring homomorphisms -

1. $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n, a \mapsto a \pmod n = \bar{a}$ is a ring homomorphism every ideal is the kernel of some ring homomorphism / every normal subgroup is the kernel of some group homo.
 $\text{Ker}(\phi) = n\mathbb{Z}, \text{Im}(\phi) = \mathbb{Z}_n$.
 2. There is no ring homomorphism $\phi: \mathbb{Z}_n \rightarrow \mathbb{Z}$.

Definition Let R be a ring. Then a left module M over R is an abelian group $(M, +, \cdot)$ endowed with a map which is a left ring action, $\psi: R \times M \rightarrow M$
 $(r, m) \mapsto r \cdot m$ s.t. the following axioms are satisfied:

- ① $r(m+n) = rm + rn$ ② $1 \cdot m = m$ ③ $r \cdot (sm) = (rs)m = rsm$ ④ $(r+s)m = rm + sm \quad \forall r, s \in R, \forall m, n \in M$.

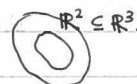
Remark - Think of a module over R as a vector space over R , but there is no basis theorem in this degree of generality.

Definition The (external) direct sum of modules, $M \oplus N$ is defined as a module, for M, N being two modules over R , by

- ① $M \oplus N = M \times N$ as sets, ② $(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$ ③ $\lambda(m, n) = (\lambda m, \lambda n)$ ④ $0 = (0, 0)$

Definition Let $N \subseteq M$ be a subset, then N is called a submodule of M , written $N \subseteq M$, if

- ① $0 \in N, N \neq \emptyset$ ② $\forall n_1, n_2 \in N, n_1 + n_2 \in N$ ③ $\forall r \in R, \forall n \in N, r \cdot n \in N$



Examples of modules -

1. Any vector space over a field \mathbb{F} is a left module.
 2. \mathbb{R}^n is an \mathbb{R} -module $\psi: \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$
 3. \mathbb{Q} is a \mathbb{Z} -module. $\psi: \mathbb{Z} \times \mathbb{Q} \rightarrow \mathbb{Q}, (z, q) \mapsto z \cdot q$
 4. Any abelian group $A = \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \stackrel{\text{Chinese Remainder Thm}}{\cong} \mathbb{Z}^r \times \mathbb{Z}_{k_1} \times \dots \times \mathbb{Z}_{k_s}$ (Smith Normal Form) with $k_1 | k_2 | \dots | k_s$ (r is rank)
 is a \mathbb{Z} -module. $\psi: \mathbb{Z} \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3 = A = \{0, 1, 2\}$.
 5. Let R be a ring, then the principal ideal generated by $a \in R$ is $(a) = \{r \cdot a : r \in R\} = Ra$.
 Then by defining R -action, it is a R -submodule $Ra \subseteq R$, e.g. $(2) = 2\mathbb{Z} \subseteq \mathbb{Z}$ is a \mathbb{Z} -submodule.
 6. Let $I \triangleleft R$ be an ideal, then I is an R -submodule of R .
 7. $M_n(R)$ is an R -module and an $M_n(R)$ -module [Think of $M_n(R)$ as vectors]
 8. The quaternions \mathbb{H} is a real dimensional vector space = \mathbb{R} -module. $\mathbb{H} = \{a + b i + c j + d k : i, j, k \text{ basis, } a, b, c, d \in \mathbb{R}\}$.
 is an \mathbb{R} -module of dimension 4 and \mathbb{C} -module of dimension 2. $i^2 = j^2 = k^2 = -1, ij = k = -ji$
 If $z = a + bi, h = a + bi + c j + d k = a + bi + (c + di)j = \mathbb{C} \oplus \mathbb{C} j \Rightarrow$ basis $\{1, j\}$ over \mathbb{C} .
 Check $j \bar{z} = \bar{z} j$, so not commutative.

Definition An R -module M is called finitely generated if $\exists \{m_1, \dots, m_k\}$ s.t. $\forall m \in M, m = \sum_{i=1}^k \lambda_i m_i, \forall \lambda_i \in R$.

Examples of finitely generated modules -

- Any vector space V of finite dimension over $\mathbb{F} \equiv$ modules over "division rings"
- $M_n(\mathbb{F})$ is finitely generated over \mathbb{F} by E_{ij} .
- Any abelian group $A = \mathbb{Z}^r \times \mathbb{Z}q_1 \times \dots \times \mathbb{Z}q_s \cong$ a finitely generated \mathbb{Z} -module.
- $\mathbb{F}[x]$ as an \mathbb{F} -module is not finitely generated.
- \mathbb{Q} as a \mathbb{Z} -module is not finitely generated. $\varphi: \mathbb{Z} \times \mathbb{Q} \rightarrow \mathbb{Q}$. Suppose $\{q_1, q_2, \dots, q_s\}$ is a generated set of \mathbb{Q} . Choose n s.t. n is coprime to all denominators. Then $\frac{1}{n}$ cannot be expressed as a linear combination of $\{q_1, \dots, q_s\}$.

Note - Modules in this course will be finitely generated.

Definition Let N be an R -submodule of M . Then M/N is the quotient module, where $M/N = \{m+N : m \in M\}$.

M/N is a R -module.

Proof - (+) since $(m_1+N) + (m_2+N) = (m_1+m_2)+N$. We can add cosets, so we have an abelian group

(scalar mult.) Under R -action, $\lambda(m+N) = \lambda m+N$ for $\lambda \in R$. To determine if action is well-defined, we need rule of equality for cosets, i.e.

$$|x+N = y+N \iff x-y \in N|. \text{ Thus, action is well defined: } x+N = y+N \iff x-y \in N \iff \lambda(x-y) \in N \text{ by absorbency of submodule.}$$

$$\iff \lambda x - \lambda y \in N \iff \lambda x + N = \lambda y + N, \text{ q.e.d.}$$

Example of quotient module -

Let $I \triangleleft R$ be an ideal of R , R/I is an additive group which becomes an R -module via the action $r \cdot (a+I) = ra+I$.

For instance, for $\mathbb{Z} \triangleleft \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} = \{0, \bar{1}\} = \{0+2\mathbb{Z}, 1+2\mathbb{Z}\}$. We define \mathbb{Z} -action $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z} \times \{0, \bar{1}\} \mapsto \{0, \bar{1}\}$.

Definition Let N_1, N_2 be R -submodules of M . Then $N_1 + N_2$ is defined to be $N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}$.

If $N_1 \cap N_2 = \{0\}$, then the sum is the (internal) direct sum, $N_1 \oplus N_2$.

Definition Let $N \leq M$ be an R -submodule. Then, we say N is a direct summand of M if $\exists N'$ s.t. $N \oplus N' = M$.

Definition Let I be an ideal / R -submodule of R . If I is a left and right ideal simultaneously, then I is called a 2-sided ideal. [i.e. $R \cdot I \subseteq I, I \cdot R \subseteq I$].

Definition A ring R is called a simple ring if its only 2-sided ideals are $\{0\}$ and R .

Proposition Let R be a ring, I an ideal. $I \triangleleft R$. Then the 2-sided ideals of $M_n(R)$ are of the form $M_n(I)$, where I has to be 2-sided.

Proof - see Ex 2.

consequences -

(I) If R is a field, then the only 2-sided ideals of \mathbb{F} are $\{0\}$ and \mathbb{F} . \therefore The only 2-sided ideals of $M_n(\mathbb{F})$ are $M_n(\mathbb{F})$ and $\{0\}$.

$\Rightarrow M_n(\mathbb{F})$ is a simple ring.

(II) If $R=D$ is a division ring, then $M_n(D)$ is also a simple ring.

(III) Does $M_n(\mathbb{F})$ have non-trivial left ideals? Yes. Take $C_j = \left\{ \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} : a_{ij} \in \mathbb{F} \right\}$. Then $M_n(\mathbb{F}) \times C_j \rightarrow C_j$, $A \times \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \mapsto$

trivial - $M_2(\mathbb{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{F} \right\}$. Left ideals are $C_1 = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} : a, c \in \mathbb{F} \right\} \triangleleft M_2(\mathbb{F})$, $C_2 = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} : b, d \in \mathbb{F} \right\} \triangleleft M_2(\mathbb{F})$
 $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} + \begin{pmatrix} a' & 0 \\ c' & 0 \end{pmatrix} \in C_1$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & 0 \\ c' & 0 \end{pmatrix} \in C_1$.

Do not confuse ideals with subrings. $S = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \subset \begin{pmatrix} a & b \\ c & d \end{pmatrix} = M_2(\mathbb{F})$. S is a subring, but not a left ideal: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & 0 \\ c' & 0 \end{pmatrix} \notin S$.

\therefore every ideal is a subring, but not every subring is an ideal.

$\therefore M_n(\mathbb{F}) \cdot C_j \subseteq C_j \therefore C_j$ absorbs $M_n(\mathbb{F})$ -action and is a left $M_n(\mathbb{F})$ module. Corresponding right $M_n(\mathbb{F})$ -modules are η_i .

Definition (left) M An R -module is called simple if its only submodules are 0 and M .

Definition (left) M An R -module M is called semisimple if $M = \bigoplus_{i \in I} M_i$ where each M_i is simple for every $i \in I$, where I could be a finite or infinite indexing set.

i.e. $M_i \cap M_j = \{0\} \forall i \neq j$.

Examples of R -modules -

- \mathbb{F} as an \mathbb{F} -vector space is a simple module, as it is 1-dimensional.
- \mathbb{F}^n as an \mathbb{F} -module is semisimple. We choose a basis for \mathbb{F}^n , say $\{e_1, \dots, e_n\}$. Then $\mathbb{F}^n = \mathbb{F}e_1 \oplus \dots \oplus \mathbb{F}e_n = \bigoplus_{i=1}^n \mathbb{F}e_i$.
- C_j are simple $M_n(\mathbb{F})$ -modules. \Rightarrow 4. $M_n(\mathbb{F})$ is semisimple as an $M_n(\mathbb{F})$ -module. $\Rightarrow M_n(\mathbb{F}) = \bigoplus_{j=1}^n C_j$, e.g. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}$.
- C_j is not simple as an \mathbb{F} -module. $\mathbb{F} \times C_j \rightarrow C_j$. C_j is semi-simple as \mathbb{F} -module, since we identify C_j with $\mathbb{F}^n = \bigoplus \mathbb{F}e_i$.
 $C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \mapsto \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} = a_{1j}e_1 + \dots + a_{nj}e_n \cong \mathbb{F}^n$, which is semisimple over \mathbb{F} .

6. \mathbb{Z} as a \mathbb{Z} -module is not simple nor semisimple. Not semisimple: has ideals/submodules such as $2\mathbb{Z} \subset \mathbb{Z}$.

It is not simple as $\mathbb{Z} = \bigoplus \mathbb{Z}i$

Beware! Some modules are neither simple nor semisimple. e.g. $\mathbb{Z}/4\mathbb{Z}$ as a \mathbb{Z} -module, $2\mathbb{Z}/4\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z}$ but $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$?

Distinguish between rings and modules over rings: For instance,

- $M_n(\mathbb{F})$ is a simple ring, with only two 2-sided ideals. No action here. However,
- $M_n(\mathbb{F})$ over $M_n(\mathbb{F})$ is a semi-simple module, with scalar action.

Definition Let M and N be left R -modules, then an R -module homomorphism $\varphi: M \rightarrow N$ satisfies

(1) $\varphi(0) = 0$ (2) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ (3) $\varphi(\lambda m) = \lambda \varphi(m) \quad \forall m, m_1, m_2 \in M, \lambda \in R$.

Definition The kernel, $\text{Ker}(\varphi) = \{m \in M : \varphi(m) = 0\}$. If $\text{Ker}(\varphi) = \{0\}$, φ is injective. (Ker measures φ 's injectivity).

The image, $\text{Im}(\varphi) = \{\varphi(m) \in N : m \in M\}$. If $\text{Im}(\varphi) = N$, φ is surjective.

Proposition $\text{Ker}(\varphi) \leq M$ and $\text{Im}(\varphi) \leq N$ are R -submodules.

Proof - (1) $\varphi(0) = 0 \Rightarrow 0 \in \text{Ker}(\varphi), 0 \in \text{Im}(\varphi)$

(2) Let $a, b \in \text{Ker}(\varphi) \Rightarrow \varphi(a) = 0, \varphi(b) = 0$. Then $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0 \Rightarrow a+b \in \text{Ker}(\varphi)$. [module homomorphism]

Let $\alpha, \beta \in \text{Im}(\varphi) \Rightarrow \exists a, b \in M$ s.t. $\varphi(a) = \alpha, \varphi(b) = \beta$. $\varphi(a+b) = \varphi(a) + \varphi(b) = \alpha + \beta \Rightarrow \alpha + \beta \in \text{Im}(\varphi)$.

(3) Let $\lambda \in R, \varphi(\lambda a) = \lambda \cdot \varphi(a) = \lambda \cdot 0 = 0 \Rightarrow \lambda a \in \text{Ker}(\varphi)$. $\varphi(\lambda a) = \lambda \varphi(a) = \lambda \alpha \in \text{Im}(\varphi) \therefore \text{Im}(\varphi) \leq N$ q.e.d.

Lemma (Schur's lemma, version 1)

Let M and N be two non-zero simple left R -modules. Then $\varphi: M \rightarrow N$ is either

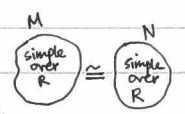
- ① $\varphi = 0$ map i.e. $0: M \rightarrow N, m \mapsto 0$ s.t. $0(m) = 0$ or ② φ is an isomorphism (i.e. φ invertible, $M \cong N$).

Proof - Suffices to prove that if $\varphi \neq 0$, then φ is an isomorphism (NTP: module homomorphism, injective, surjective).

(Injectivity) Since $\text{Ker}(\varphi) \leq M$ is an R -submodule, M is simple module $\Rightarrow \text{Ker}(\varphi) = \{0\}$ or M . Since $\varphi \neq 0, \text{Ker}(\varphi) \neq M$.

$\Rightarrow \text{Ker}(\varphi) = \{0\} \Rightarrow \varphi$ is injective.

(Surjectivity) $\text{Im}(\varphi) \leq N$ is an R -submodule. By simplicity of $N, \text{Im}(\varphi) = \{0\}$ or N . Since $\varphi \neq 0, \text{Im}(\varphi) \neq 0 \Rightarrow \text{Im}(\varphi) = N \Rightarrow \varphi$ is surjective q.e.d.



Definition Let R be a ring, M be an R -module. We define the endomorphism ring, $\text{End}_R(M) = \text{Hom}_R(M, M) = \{\alpha: M \rightarrow M \mid \alpha \text{ is an } R\text{-module homomorphism}\}$.

Proposition $\text{End}_R(M)$ is naturally a ring.

Proof - Let $\alpha, \beta \in \text{End}_R(M)$; $(\alpha + \beta)(m) = \alpha(m) + \beta(m)$ for $m \in M$. Define composition of maps, $(\alpha \circ \beta)(m) = \alpha(\beta(m))$.

(1) zero map $0(m) = 0$ (1) identity map $\text{Id}(m) = m \quad \forall m \in M$ q.e.d. [check ring axioms].

Note - $\text{Hom}_R(M, N)$ is an abelian group (add maps) which becomes an R -module $R \times \text{Hom}(M, N) \rightarrow \text{Hom}(M, N)$ if R is a commutative ring.

$\therefore \text{End}_R(M)$ is an R -module if R is commutative $R \times \text{End}_R(M) \rightarrow \text{End}_R(M)$.

Definition A ring D is called a division ring if $\forall x \in D, x \neq 0, \exists y$ s.t. $xy = 1$. [Nomenclature: these are also called skew-fields]

Note - Here, every element has an inverse (except 0). Unlike fields however, it is not necessarily commutative.

Examples -

1. Any field \mathbb{F} is a division ring.
2. \mathbb{Z} is a ring, but not division ring. $\{ \pm 1 \} \in \mathbb{Z}$ are only elements with inverses.
3. $M_n(\mathbb{F})$ is not a division ring - E_{ij} has no inverse. $ij = k = -ji$.
4. Quaternions $\mathbb{H} = \{ a \cdot 1 + b \cdot i + c \cdot j + d \cdot k \}$ is a division ring (non-commutative).
Let $\alpha \in \mathbb{H}, \alpha = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$. Let $\alpha \neq 0$. Define $\bar{\alpha} = a \cdot 1 - b \cdot i - c \cdot j - d \cdot k$. Then let $N(\alpha) = \alpha^2 + b^2 + c^2 + d^2$. $\therefore \alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}, \forall \alpha, \exists \alpha^{-1}$.
5. $(\frac{-1 \pm i\sqrt{3}}{2})$ is a division ring = \mathbb{Q} -vector space with basis $\{1, i, j, k\}$.

Lemma (Schur's lemma, version 2).

Let M be a simple R -module, then $\text{End}_R(M)$ is a division ring.

Proof - Let $\alpha \in \text{End}_R(M)$. Suppose $\alpha \neq 0$, since M is simple, by Schur's lemma $\forall 1, \alpha: M \rightarrow M \Rightarrow \alpha$ is an isomorphism

$\Rightarrow \exists \alpha^{-1}: M \rightarrow M$ s.t. $\alpha \alpha^{-1} = \text{Id}$ and $\alpha^{-1} \alpha = \text{Id}$. $\therefore \forall \alpha \in \text{End}_R(M)$, an inverse exists $\Rightarrow \text{End}_R(M)$ is a division ring q.e.d.

$\text{End}_R(M)$ is a tool for measuring the simplicity of M . As an application,

1. Let F be a field, and consider the F -module F . Let $\varphi_\lambda: F \rightarrow F$ be F -linear module homomorphisms defined by $x \mapsto \lambda x$ for some $\lambda \in F$.

$\text{End}_F(F) = \{f: F \rightarrow F \mid f \text{ is } F\text{-linear}\} \cong F = \text{division ring} \Rightarrow F \text{ is a simple } F\text{-module.}$

2. Let $M = F^2$ over F . compute $\text{End}_F(F^2) \cong \{f: F^2 \rightarrow F^2 \mid f \text{ is } F\text{-linear}\} \cong M_2(F)$, which is not a division ring since E_{ij} have no inverse.

clearly, F^2 is not simple because $F \leq F^2$ is a non-trivial submodule.

3. Recall: $C_j = \{ \sum_{k=1}^n c_k E_{kj} \mid c_k \in F \}$ is an $M_n(F)$ module. $M_n(F) \times C_j \rightarrow C_j$.

Proposition C_j is a simple $M_n(F)$ -module.

Proof - compute $\text{End}_{M_n(F)}(C_j) = \{f: C_j \rightarrow C_j \mid f \text{ is } M_n(F)\text{-linear}\} = \{ \begin{matrix} f(x+y) = f(x)+f(y) \\ f(Ax) = Af(x) \end{matrix} \mid \begin{matrix} x, y \in C_j \\ A \in M_n(F) \end{matrix} \}$, which we hope is isomorphic to $F = \text{division ring}$.

① choose canonical basis for F^n , say $\{e_1, \dots, e_n\}$. s.t. $F^n \cong FE_1 \oplus \dots \oplus FE_n$.

② Define f linear maps to identify C_j with F^n , $f: C_j \rightarrow F^n$, $\begin{pmatrix} 0 & \dots & a_{ij} & \dots & 0 \end{pmatrix} \mapsto \begin{pmatrix} a_{ij} \\ \vdots \\ a_{nj} \end{pmatrix} = \sum_{i=1}^n a_{ij} e_i$

③ Use $f(Ax) = Af(x)$. since f is a linear map, \exists matrix $\Phi = (\varphi_{ij})$ s.t. $f_\lambda: F^n \rightarrow F^n$, $\begin{pmatrix} \varphi_{11} & \dots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{n1} & \dots & \varphi_{nn} \end{pmatrix} \begin{pmatrix} a_{ij} \\ \vdots \\ a_{nj} \end{pmatrix} = \begin{pmatrix} \lambda a_{ij} \\ \vdots \\ \lambda a_{nj} \end{pmatrix}$ for some $\lambda \in F$.

$\Rightarrow \Phi A = A \Phi$ using $f(Ax) = Af(x)$.

④ $\text{End}_{M_n(F)}(C_j) = \{f: C_j \rightarrow C_j \mid f \text{ commutes with all } A \in M_n(F)\} = \{B \in M_n(F) \mid AB = BA\} = \{\text{diag}(\lambda, \dots, \lambda) \mid \lambda \in F\} \cong F, \text{ division ring.}$

$\therefore C_j$ is a simple $M_n(F)$ -module. $\Rightarrow M_n(F) = \bigoplus_{j=1}^n C_j$ is semisimple as an $M_n(F)$ -module, q.e.d.

The converse of Schur's lemma $\forall 2$ does not hold in general. $\text{End}_R(M) = \text{division ring} \not\Rightarrow M$ is simple.

4. \mathbb{Q} is a \mathbb{Z} -module. $\mathbb{Z} \times \mathbb{Q} \rightarrow \mathbb{Q}$. It is obviously not simple, as $\mathbb{Z} \leq \mathbb{Q}$ is a non-trivial submodule. $\therefore \mathbb{Q}$ is not simple, but $\text{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ which is a division ring.

$\text{End}_{\mathbb{Z}}(\mathbb{Q}) = \{f: \mathbb{Q} \rightarrow \mathbb{Q} \mid f \text{ is } \mathbb{Z}\text{-linear}\} = \{f: \mathbb{Q} \rightarrow \mathbb{Q} \mid \begin{matrix} f(m_1+m_2) = f(m_1) + f(m_2) \\ f(zm) = z f(m) \end{matrix} \mid z \in \mathbb{Z}\}$. let $f \in \text{End}_{\mathbb{Z}}(\mathbb{Q})$ be an element.

then $f(n) = f(n \cdot 1) = n f(1)$, $n \in \mathbb{Z}$; $f(\frac{1}{n}) = \frac{1}{n} f(1) \therefore f(1) = f(\frac{n}{n}) = n f(\frac{1}{n}) \Rightarrow f(\frac{m}{n}) = m f(\frac{1}{n}) = \frac{m}{n} f(1)$.

$\therefore \forall q \in \mathbb{Q}$, $f(q) = q f(1) \Rightarrow f: \mathbb{Q} \rightarrow \mathbb{Q}$ is solely determined by $f(1)$. $\Rightarrow \text{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$, where $f \mapsto f(1)$ defines ring isomorphism.

$\Rightarrow \mathbb{Z} \leq \mathbb{Q}$ is not simple but $\text{End}_{\mathbb{Z}}(\mathbb{Q})$ is division ring.

Remark - there is a more powerful version of Schur's lemma, $\forall 3$ which applies to $[F[G]]$ modules. Then $\text{End}_{F[G]}(M) = \text{division ring} \Rightarrow M$ is simple.

Definition Let M be a simple R -module. Then $M \cong Rm$ for some $m \neq 0$, $m \in M$. Such a module is called a cyclic module.

Proposition

Proof - clearly $Rm \leq M$, since $m \neq 0$ and M is simple, $Rm \neq \{0\} \Rightarrow Rm = M$, q.e.d.

conversely, if $\forall m \in M$, we have $M = Rm \Rightarrow M$ is simple. If $M = Rm$, $M \cong R/I$ where $I = \{r \in R \mid rm = 0\} \triangleleft R$.

Example - classifying all simple \mathbb{Z} -modules -

let M be a simple \mathbb{Z} -module. Define $\varphi: \mathbb{Z} \rightarrow M$, $n \mapsto n \cdot m$ for $n \in \mathbb{Z}$. Since $\text{Ker}(\varphi) \leq \mathbb{Z}$, $\text{Ker}(\varphi) = n\mathbb{Z}$. Thus, by 1st isomorphism theorem,

φ induces a map $\varphi^*: \frac{\mathbb{Z}}{\text{Ker}(\varphi)} \rightarrow \text{Im}(\varphi) \leq M$ ($= M$ since M is simple) $\Rightarrow \varphi^*: \frac{\mathbb{Z}}{n\mathbb{Z}} \xrightarrow{\cong} M$

Case 1: If $n = n_1 n_2$, $(n_1, n_2) = 1$ coprime. Then $M \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$. Is M simple in this case? No, $\mathbb{Z}/n_1\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$.

Case 2: If $n = p^k$, p is prime, $k > 1$. Then $M \cong \mathbb{Z}/p^k\mathbb{Z}$ is not simple because $\mathbb{Z}/p\mathbb{Z} \leq \mathbb{Z}/p^k\mathbb{Z}$.

Case 3: If $n = p$, then $M \cong \mathbb{Z}/p\mathbb{Z}$, which is a simple \mathbb{Z} -module as $\{0\}$ and $\mathbb{Z}/p\mathbb{Z}$ are the only submodules.

Thus, semisimple \mathbb{Z} -modules look like $M = \mathbb{Z}/p_1\mathbb{Z} \oplus \mathbb{Z}/p_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_n\mathbb{Z}$ (could continue on, but would not be finitely generated).

For instance, $\mathbb{Z}/2\mathbb{Z}$ is simple, $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is semisimple, $\mathbb{Z}/4\mathbb{Z}$ is neither.

Theorem (Classification Theorem of Semisimple Modules)

let M be an R -module, then the following are equivalent:

(1) M is semisimple $[M = \bigoplus_{i \in I} M_i, M_i \text{ simple}]$; (2) $\forall N \leq M \exists N' \leq M$ s.t. $M = N \oplus N'$

Example - $M = F^n$, then $\forall N = F^a, \exists N' = F^b$ s.t. $F^n \cong F^a \oplus F^b$, $a+b=n$.

Proof - (1) \Rightarrow (2): Suppose M is semisimple, $M = \bigoplus_{i \in I} M_i$, I is a finite indexing set. let $J \subseteq I$ be a non-empty maximal subset $J = \emptyset$ which exists by Zorn's lemma.

let $N \leq M$ be a non-zero submodule. Define $M^* = N \oplus \bigoplus_{i \in J} M_i$ and show $M = M^*$. \Rightarrow then you can take $N = \bigoplus_{i \in J} M_i$.

let $i \in I \setminus J$, consider $N \cap M_i$. If $N \cap M_i = \{0\}$, contradicts maximality of J , can add it. $\therefore N \cap M_i = M_i \Rightarrow M_i \subset N \subset M \Rightarrow M \neq M^*$ contradiction.

$\therefore M = M^*$, q.e.d.

(2) \Rightarrow (1): To do this we need to first introduce a vital lemma, which we will not yet prove until later:

"Any non-zero finitely generated module contains a simple submodule, which is also non-zero".

Suppose $M = N \oplus N' \Rightarrow$ both N and N' are semisimple. Let $M_0 \leq M$, where $M_0 =$ sum of all simple submodules.
 Show that $M_0 = M$: Suppose $M_0 \neq M$, let $W \leq M$, so $W \not\subseteq M_0 \Rightarrow M = W \oplus M_0 \Rightarrow W$ contains a simple submodule
 by the vital lemma, which contradicts the definition of $M_0 \Rightarrow M = M_0 = \bigoplus_{i \in I} M_i$. The sum is finite as M is finitely generated, q.e.d.

Definition Let $N \leq M$. Then N is called a maximal submodule if $\forall K \leq M$ s.t. $N \leq K \leq M$, $K=N$ or $K=M$.

Example - Let R be an R -module. Then any maximal ideal $I \triangleleft R$ is a maximal R -module. For instance, \mathbb{Z} is a \mathbb{Z} -module, then maximal ideal of \mathbb{Z} is $p\mathbb{Z}$.

Facts about maximal submodules:

1. Submodule $N \leq M$ is maximal $\Rightarrow M/N$ is simple. e.g. $p\mathbb{Z} \leq \mathbb{Z} \Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ is a simple \mathbb{Z} -module and maximal ideal \Leftrightarrow quotient is a field.
2. Any proper submodule of a finitely-generated module is contained in a maximal submodule. This fails if M is not finitely generated, so we need axiom of choice.

Lemma (Vital lemma)

Any non-zero finitely generated module contains a simple submodule, which is also non-zero.

Proof - let M be such that $\forall N \leq M, \exists N' \text{ s.t. } M = N \oplus N'$. Take $v \in M, v \neq 0$ and consider the homomorphism $\varphi: R \rightarrow R \cdot v \leq M$ by $\lambda \mapsto \lambda v \forall \lambda \in R$. (cyclic)

then φ is surjective $\Rightarrow \text{Im}(\varphi) = R \cdot v$, and we know $\text{Ker}(\varphi) \leq R$. By fact 2 about maximal submodules, $\text{Ker}(\varphi) \leq I$ for some maximal

ideal $I \triangleleft R$. By definition, Iv is a maximal submodule of $R \cdot v$. By construction, $M = Iv \oplus M'$ as a direct sum, $m = xv + y \forall m \in M$ uniquely.

Intersect with Rv : $M \cap Rv = Iv \cap Rv \oplus M' \cap Rv = Iv \oplus M' \cap Rv$. Then $M' \cap Rv \cong Rv/Iv \cong R/I$, which is simple by fact 1, q.e.d.

Proposition Every submodule and every quotient module of a semi-simple module is semisimple.

Proof - let M be semisimple and let $N \leq M$. let $W \leq N \Rightarrow W \leq M \Rightarrow$ by simplicity of $M, \exists W' \text{ s.t. } M = W \oplus W'$.

Intersect with $N \Rightarrow M \cap N = W \cap N \oplus W' \cap N$. Now, $M \cap N = N, W \cap N = W$, so $N = W \oplus W' \cap N$. $\therefore N$ is semisimple by characterisation theorem

of semisimple modules, so $N = \bigoplus M_i$, q.e.d.

Now assume $N = W \oplus W'$. let $N \leq W \leq M \Rightarrow W/N \leq M/N$ since $M = W \oplus W' \Rightarrow M \cap N = W \cap N \oplus W' \cap N, M/N \cong W/N \oplus \frac{W'}{W \cap N}$

$\Rightarrow M/N$ is semisimple by the characterisation theorem.

ALGEBRAS.

Definition By an algebra A over \mathbb{F} we mean a ring with a vector space structure satisfying

- (in ring) (as vectors)
 (1) $a + b = b + a$ (2) $(\lambda a)b = \lambda(ab) = a(\lambda b) \forall a, b \in A, \forall \lambda \in \mathbb{F}$.

We call it an \mathbb{F} -algebra. By an \mathbb{F} -algebra we mean a ring which is automatically a vector space over \mathbb{F} .

More generally, an R -algebra is a module over a ring R [i.e. we can look at all modules over a ring A]

[we classify all semi-simple algebras over $\mathbb{F}(s) = \bigoplus M_{n_i}(D_i)$]

Examples of algebras -

1. \mathbb{F} is an \mathbb{F} -algebra.
2. $\mathbb{F}[x]$ is an \mathbb{F} -algebra.
3. $\mathbb{F}[x]/I$ is an \mathbb{F} -algebra.
4. $M_n(\mathbb{F})$ is an \mathbb{F} -algebra. The scalars are scalar diagonal matrices, $\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$
5. Any ring is a \mathbb{Z} -algebra.
6. $\text{End}_R(M)$ is an R -algebra if R is commutative, due to the map $\varphi: R \rightarrow \text{End}_R(M)$.
7. \mathbb{H} is an \mathbb{R} -algebra but not a \mathbb{C} -algebra: $\mathbb{H} = \text{span}_{\mathbb{R}} \{1, j, k, i\}$, \mathbb{H} has $j^2 = -1$ in \mathbb{C} , so it is not a \mathbb{C} -algebra.

Definition An algebra A is finite-dimensional if it is finite-dimensional as a vector space over \mathbb{F} .

It is semisimple if every finitely-generated module over A is semisimple.

Example - \mathbb{F} is an \mathbb{F} -algebra, but \mathbb{F} is semisimple because every finitely generated module over \mathbb{F} is isomorphic to \mathbb{F}^n .

(Characterisation of semisimple algebras)

Proposition A is semisimple $\Leftrightarrow A$ viewed as an A -module is semisimple.

Proof - (\Rightarrow) Trivial by definition.

(\Leftarrow) Suppose A is a semi-simple A -module, and let $M \neq \{0\}$ be an A -module. Choose a generating set $\{m_1, \dots, m_k\} \subset M$.

$[A \oplus \dots \oplus A]$ (direct sum)

let $\varphi: A^k \rightarrow M$ be a homomorphism of A -modules by $(a_1, \dots, a_k) \mapsto \sum a_i m_i$. Since A is semi-simple, we can write $A = S_1 \oplus \dots \oplus S_t$ where S_i are simple A -modules.

$\therefore A^k$ is semi-simple, because $A^k = \overbrace{(S_1 \oplus \dots \oplus S_t)}^k \oplus \dots \oplus \overbrace{(S_1 \oplus \dots \oplus S_t)}^k$. Since φ is surjective, so the m_i generate M over A .

By 1st isomorphism theorem, $\text{Im}(\varphi) = M \cong A^k / \text{Ker}(\varphi)$ is semisimple as it is a quotient of semi-simple module $\Rightarrow A$ is semisimple by definition, q.e.d.

Examples and Consequences -

1. D is a division algebra $\Rightarrow M_n(D)$ is semisimple so a D -algebra.
2. if $A = \mathbb{Z}/p^2\mathbb{Z}$ is an \mathbb{F}_p -algebra, then A is not semisimple because $\mathbb{Z}/p^2\mathbb{Z}$ has no complement.

Proposition Let A be a semisimple algebra over \mathbb{F} s.t. $A = A_1 \oplus \dots \oplus A_t$ is a sum of simple submodules. Then any simple A -module is isomorphic to an A_i for some i .

Proof - let S be a simple module over A , then show $S \cong A_i$ for some i . Take $s \in S, s \neq 0$. Consider the linear map $\varphi: A \rightarrow a \cdot s \in S$ (where $A = \bigoplus_{i=1}^t A_i$) by $a \mapsto a \cdot s$. $\varphi \neq 0$ because $s \neq 0$, so restrict φ . let $\varphi_i = \varphi|_{A_i}: A_i \rightarrow A_i \cdot s \in S$. $\text{Im}(\varphi) \subseteq S$, but S is simple, so $A_i \cdot s = S$. Since $\varphi_i \neq 0 \forall i$, $\varphi_i: A_i \rightarrow S$ is always an isomorphism by Schur's Lemma $\forall i$. $\varphi \neq 0$ because $s \neq 0$, so restrict φ . let $\varphi_i = \varphi|_{A_i}: A_i \rightarrow A_i \cdot s \in S$. $\text{Im}(\varphi) \subseteq S$, but S is simple, so $A_i \cdot s = S$. Since $\varphi_i \neq 0 \forall i$, $\varphi_i: A_i \rightarrow S$ is always an isomorphism by Schur's Lemma $\forall i$.

Proposition Let A be a semisimple algebra and let $\{S_i\}$ be a collection of simple A -modules. Let M be an A -module. Then M is semisimple i.e. $M = S_1^{n_1} \oplus \dots \oplus S_r^{n_r}$

and the decomposition is unique \therefore if $M = T_1^{m_1} \oplus \dots \oplus T_s^{m_s}$, then $r = s, T_i \cong S_i \forall i$.

Definition A division algebra D is a division ring with a vector space structure, i.e. every non-zero element has an inverse: $\forall x \in D, \exists x^{-1}$ s.t. $x \cdot x^{-1} = 1$.

Examples of division algebras -

1. \mathbb{F} over \mathbb{F}
2. \mathbb{H} over \mathbb{R}
3. $M_n(\mathbb{F})$ is not
4. $D_1 \times D_2$ is not a division algebra, so $(d_1, 0)^{-1}$ does not exist.

Theorem (Frobenius Theorem on algebras)

If D is a finite dimensional division algebra over \mathbb{R} , then:

- (1) $D \cong \mathbb{R}$ (dim 1 over \mathbb{R}) or
 - (2) $D \cong \mathbb{C}$ (dim 2 over \mathbb{R}) or
 - (3) $D \cong \mathbb{H}$ (dim 4 over \mathbb{R})
- Useful for R[G].

Proof - beyond the scope of this course; omitted.

Let D be a finite-dimensional \mathbb{F} -algebra. Then $\forall n, M_n(D)$ is an \mathbb{F} -algebra and has dimension $n^2 \dim(D)$. For instance, $D = \mathbb{H}$, then $\dim_{\mathbb{F}}(M_n(\mathbb{H})) = n^2 \dim(\mathbb{H}) = 4n^2$.

Proposition Let D be a division algebra and $n \geq 1$, with $M_n(D)$ defined as usual. Then

- (1) Any simple $M_n(D)$ module is isomorphic to $C_j \cong D^n$
- (2) $M_n(D) \cong \bigoplus C_j = \bigoplus D^n, \therefore M_n(D)$ is semisimple.

Proof - Easy, previously seen.

Definition A field \mathbb{F} is algebraically closed if every polynomial $f(x) \in \mathbb{F}[x]$ of $\deg(f) \geq 1$ has a root in \mathbb{F} . We denote this by $\overline{\mathbb{F}}$.

Examples of algebraically closed fields -

1. $\mathbb{C} = \overline{\mathbb{R}}, \overline{\mathbb{Q}}, \overline{\mathbb{F}_p}$.
2. \mathbb{R} is not closed so $x^2 + 1 \in \mathbb{R}[x]$ but has no root in \mathbb{R} (so we close \mathbb{R} with \mathbb{C}).

Theorem (Burnside's theorem)

Let S be a simple module over A , i.e. an algebra over \mathbb{F} . Then $\text{End}_A(S) \cong \overline{\mathbb{F}}$.

Proof - let $\varphi \in \text{End}_A(S)$ s.t. $\varphi \neq 0$. S is an \mathbb{F} -vector space, φ is a linear map. Let $\text{ch}_\varphi(x) \in \mathbb{F}[x]$ be the characteristic polynomial of φ . Then,

$$(\varphi - \lambda \text{Id})v = 0$$

since $\overline{\mathbb{F}}$ is algebraically closed, then $\text{ch}_\varphi(x)$ has a root/eigenvalue in $\overline{\mathbb{F}}, \lambda$. By definition, $\varphi - \lambda \text{Id} \in \text{End}_A(S)$ is not invertible as an \mathbb{F} -linear map.

By Schur's Lemma, φ is invertible since $\varphi = \lambda \text{Id}_S$, because $\varphi - \lambda \text{Id}_S = 0$. Define $\mathbb{F}: \text{End}_A(S) \rightarrow \overline{\mathbb{F}}$ as an isomorphism by $\varphi \mapsto \lambda$.

Definition Let A be an algebra. We define the opposite algebra, A^{op} , by

- (1) $A^{\text{op}} = A$ as a set,
- (2) $+ \text{ in } A^{\text{op}} = + \text{ in } A$ i.e. $(A, +, 0) \cong (A^{\text{op}}, +, 0)$
- (3) $\cdot = *$ is different in A^{op} , so $a * b = b \cdot a$ in A^{op} .

Obviously, $(A^{\text{op}}, +, *)$ is an algebra.

Proposition 1. A is a division algebra $\iff A^{\text{op}}$ is a division algebra.

2. $(A^{\text{op}})^{\text{op}} = A, ((a * b)^{\text{op}})^{\text{op}} = (ba)^{\text{op}} = ab$.

Lemma If B is an algebra, then $M_n(B)^{\text{op}} \cong M_n(B^{\text{op}})$

Proof - define $\Psi: M_n(B)^{\text{op}} \rightarrow M_n(B^{\text{op}})$ by $X \mapsto X^T$. It is clear that Ψ is bijective, since $\text{Ker}(\Psi) = 0, \text{Im}(\Psi)$ is all matrices.

$$\Psi(X * Y) = (YX)^T = X^T Y^T = \Psi(X) \Psi(Y) \Rightarrow \Psi \text{ is a bijective morphism of algebras.}$$

Lemma Let S be a simple A -module, where A is an algebra. Then $\forall n, \text{End}_A(S) \cong M_n(\text{End}(S))$.

Proof - see Exercise 3.

Example - $\text{End}_{\mathbb{F}}(\mathbb{F}^n) \cong M_n(\mathbb{F})$ because \mathbb{F} is a simple algebra over \mathbb{F} .

Lemma If $U_1, U_2 \leq M$ are submodules of M st. $U_1 \cup U_2 = \{0\}$, then $\text{End}(U_1 \oplus U_2) \cong \text{End}(U_1) \oplus \text{End}(U_2)$.

Proof - see Ex. 3.

Theorem (Wedderburn Decomposition Theorem)

← same as \oplus by finiteness.

An algebra A is semisimple over $\mathbb{F} \Leftrightarrow A \cong M_{n_1}(\mathbb{D}_1) \times \dots \times M_{n_k}(\mathbb{D}_k)$ where \mathbb{D}_i are division algebras over \mathbb{F} .

Proof - (\Leftarrow) Trivial, since A is a direct sum of simple modules \Rightarrow semisimple by definition.

(\Rightarrow) Suppose A is semisimple. Then $A = S_1^{m_1} \oplus \dots \oplus S_k^{m_k}$ where S_i are simple modules of dimension n_i . $A^{\text{op}} = \text{End}_A(A) = \text{End}_A(S_1^{m_1} \oplus \dots \oplus S_k^{m_k})$.

Since $S_i \cap S_j = \{0\}$, $A^{\text{op}} = \text{End}_A(S_1^{m_1}) \oplus \dots \oplus \text{End}_A(S_k^{m_k}) = M_{n_1}(\text{End}_A(S_1)) \oplus \dots \oplus M_{n_k}(\text{End}_A(S_k))$. Then taking opposite rings,

$$A = (A^{\text{op}})^{\text{op}} = [M_{n_1}(\text{End}_A(S_1)) \oplus \dots \oplus M_{n_k}(\text{End}_A(S_k))]^{\text{op}} = M_{n_1}(\text{End}_A(S_1)^{\text{op}}) \oplus \dots \oplus M_{n_k}(\text{End}_A(S_k)^{\text{op}})$$

Since S_i are simple, by Schur's lemma $\forall i$, $\text{End}(S_i)$ and $\text{End}(S_i^{\text{op}})$ are division rings, so let $\mathbb{D}_i = \text{End}(S_i^{\text{op}})$

$\therefore A \cong M_{n_1}(\mathbb{D}_1) \oplus \dots \oplus M_{n_k}(\mathbb{D}_k)$ for some division rings \mathbb{D}_i q.e.d.

Consequences -

If \mathbb{F} is algebraically closed (hint: $\mathbb{C} = \mathbb{F}$), then $A \cong M_{n_1}(\mathbb{C}) \oplus \dots \oplus M_{n_k}(\mathbb{C})$; if A is a simple algebra, then $A \cong M_{n_1}(\mathbb{C})$ as rings.

Group ring / Group algebras

Definition By a group ring / group algebra $\mathbb{F}[G] = \left\{ \sum_{g \in G} \lambda_g g : g \in G, \lambda_g \in \mathbb{F} \right\}$ i.e. formal linear combinations of group elements as a basis with \mathbb{F} coefficients.

Proposition $\mathbb{F}[G]$ is a ring.

Proof - (addition) $\sum_{g \in G} \lambda_g g + \sum_{g \in G} \mu_g g = \sum_{g \in G} (\lambda_g + \mu_g) g$ (multiplication) $(\sum_{g \in G} \lambda_g g)(\sum_{h \in G} \mu_h h) = \sum_{g, h} (\lambda_g \mu_h) gh = \sum_{g, h} \lambda_g \mu_h g h$

(zero) Since all $g \neq 0$ in G , $0 = \sum \lambda_g g$ where $\lambda_g = 0 \forall g$. (unit) $1 = 1_{\mathbb{F}} \cdot 1_G \checkmark$ q.e.d.

Note - The set $(\mathbb{F}[G], +, \cdot, 0, 1)$ is a ring.

Ex Show that $\mathbb{F}[G]$ is an algebra over \mathbb{F} with basis elements the group elements $\{1, g, \dots, g^{n-1}\}$ and scalar multiplication from \mathbb{F} .

Soln. $\lambda g \cdot g = g \cdot \lambda g \forall g$, $\mathbb{F}[G]$ is an \mathbb{F} -algebra. $\lambda \cdot (\sum \lambda_g g) = \sum \lambda \lambda_g g$

Note - The algebra $\mathbb{F}[G]$ is not commutative unless G is commutative.

Ex Show that $\mathbb{F}[C_2] = \{a + bx : a, b \in \mathbb{F}, 1, x \in C_2 = \langle x | x^2 = 1 \rangle\}$ is a group ring.

Soln. (1) $(2+6x) + (3+9x) = 5+3x$ (say). (2) $(2+x) \cdot (3-4x) = 6-5x-4x^2 = 6-5x-4 = 2-5x \in \mathbb{F}[C_2]$.

Note - Is $(1+x)$ invertible? G is commutative $\Rightarrow \mathbb{F}[C_2]$ is a commutative ring $\Rightarrow (a+bx) \cdot (1+x) = 1 \Rightarrow$ no $a+bx$ exists, $\mathbb{F}[C_2]$ is not a field.

Lemma If $|G| > 1$, then $\mathbb{F}[G]$ is not a division ring / algebra.

Proof - $|G| = 1 \Rightarrow \mathbb{F}[G] = \mathbb{F}[1] = \mathbb{F}$, which is a division ring. So suppose $|G| > 1$, G is finite $\Rightarrow \exists n$ st. $g^n = 1 \forall g$, then we get the expression:

$$(1-g)(1+g+\dots+g^{n-1}) = 1-g^n = 1-1=0 \Rightarrow 1-g, 1+g+\dots+g^{n-1} \text{ are non-zero divisors of zero, which cannot exist in an integral domain, q.e.d.}$$

Definition By an $\mathbb{F}[G]$ -module V , I will always mean a finitely generated module.

Example -

$\mathbb{F}[G]$ as an $\mathbb{F}[G]$ -module acting on its basis elements (group elements) by left-multiplication $\varphi: \mathbb{F}[G] \times \mathbb{F}[G] \rightarrow \mathbb{F}[G]$ ring v.s. v.s.

Definition Let V, W be two $\mathbb{F}[G]$ -modules. Then a $\mathbb{F}[G]$ -module homomorphism is a map $\varphi: V \rightarrow W$ that satisfies

(1) $\varphi(v+v') = \varphi(v) + \varphi(v')$, and (2) $\varphi(\lambda v) = \lambda \varphi(v) \quad \forall \lambda \in \mathbb{F}[G], \forall v, v' \in V$. Moreover,

(3) $\varphi(gv) = g \varphi(v) \quad \forall g \in G \quad \forall v \in V$.

As before, $\text{Ker}(\varphi) \leq V$ and $\text{Im}(\varphi) \leq W$ are $\mathbb{F}[G]$ -submodules.

Theorem (Correspondence Theorem)

Let G be a finite group, V a finite dimensional vector space over \mathbb{F} , $\rho: G \rightarrow GL(V)$ be an \mathbb{F} -representation. Then \exists 1-1 correspondence (bijection) between representations G and finitely generated left $\mathbb{F}[G]$ modules. [i.e. $\rho: G \rightarrow GL(V) \leftrightarrow \rho$ modules over $\mathbb{F}[G]$]

Proof - (\Leftarrow) Let V be an $\mathbb{F}[G]$ -module $\Rightarrow V$ is an \mathbb{F} -vector space. Now $\forall g \in G$, define an automorphism (linear map) $\psi: V \rightarrow V, v \mapsto g \cdot v$

$\forall v \in V = \text{span}\{b_1, \dots, b_n\}$. Write the map ψ as a matrix, $\therefore [\psi]_{\mathcal{B}} = \rho(g)$. We check that $\rho(g)$ defines a representation: $\rho(gh)$

(1) $\rho(g)(\lambda v + w) = g \cdot (\lambda v + w) = \lambda g \cdot v + g \cdot w = \lambda \rho(g) \cdot v + \rho(g) \cdot w$ (2) Check $\rho(g)$ is a homomorphism: factorive $\begin{matrix} \rho(gh) \\ \downarrow \\ V \end{matrix} \xrightarrow{\rho(h)} \begin{matrix} \rho(g) \\ \downarrow \\ V \end{matrix}$

$\rho(gh) \cdot v = g \cdot (h \cdot v) = \rho(g) \cdot (h \cdot v) = \rho(g) \rho(h) \cdot v$, which is a composition of linear maps \equiv matrix multiplication.

21 October 2013
Gordon St (15) D103
Mr Javed NADIM

(3) $\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ corresponds to identity map $\text{Id}: V \rightarrow V$. (4) $\rho(g) \in \text{GL}_n(\mathbb{F})$ is invertible, $1 = g \cdot g^{-1}$ in $\mathbb{F}[G]$ and in G , factorise $\rho(g^{-1})\rho(g) \cdot v = \rho(g^{-1})g \cdot v = g^{-1}g \cdot v = v = \text{Id}(v) \therefore \mathbb{F}[G]$ modules give \mathbb{F} -map of G .

(\Rightarrow) let $\rho: G \rightarrow \text{GL}(V) = \text{GL}_n(\mathbb{F})$ for some $B = \{b_1, \dots, b_n\} \subset V = \mathbb{F}^n$. then associate to ρ an $\mathbb{F}[G]$ module constructed from $V = \mathbb{F}^n$ by keeping the same addition, and do scalar multiplication on it by letting $\alpha = \sum \lambda_g g \in \mathbb{F}[G]$, $\alpha \cdot v = (\sum \lambda_g g) \cdot v = \sum \lambda_g (g \cdot v) = \sum \lambda_g \rho(g) v \therefore \mathbb{F}^n$ becomes an $\mathbb{F}[G]$ -module, q.e.d.

Examples -

- let $G = D_8 = \langle x, y \mid x^4 = y^2 = 1, yx = x^3y \rangle$ and $\mathbb{F} = \mathbb{R}$. Define $\rho: D_8 \rightarrow \text{GL}_2(\mathbb{R})$, $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. let $V = \mathbb{R}^2 = \text{span}_{\mathbb{R}} \{e_1, e_2\}$. Apply matrices: $\rho(x) \cdot e_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1$, $\rho(x) \cdot e_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -e_2$. $\rho(y) \cdot e_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e_2$, $\rho(y) \cdot e_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1$. This is the module information, which defines the structure of $V = \mathbb{R}^2$ as an $\mathbb{R}[D_8]$ module.
- let $G = S_n$, define $\rho: S_n \rightarrow \text{GL}_n(\mathbb{C})$, which is the permutation representation on $V = \mathbb{C}^n$, $\rho(\sigma)(e_i) = e_{\sigma(i)}$ is the module definition. This gives a matrix/representation from the $\mathbb{C}[S_n]$ -module $V = \mathbb{C}^n$. For instance, if $n=4$, $\rho: S_4 \rightarrow \text{GL}_4(\mathbb{C})$. let $V = \mathbb{C}^4 = \langle e_1, \dots, e_4 \rangle$. let $\sigma = (1\ 2) = S_4$. Then $\rho(\sigma) \cdot e_1 = e_{\sigma(1)} = e_2$, $\rho(\sigma) \cdot e_2 = e_1$, $\rho(\sigma) \cdot e_3 = e_3$, $\rho(\sigma) \cdot e_4 = e_4 \iff \rho(\sigma) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Definition let G be a finite group, V be a finite dimensional vector space over \mathbb{F} . An \mathbb{F} -representation (matrix) $\rho: G \rightarrow \text{GL}(V)$ is called **irreducible** \equiv simple module of $V \neq \{0\}$, and the only invariant subspaces of V under ρ are $\{0\}$ and V . The representation is **reducible** (semisimple) if $\exists W \subseteq V$, $W \neq \{0\}$ s.t. $\rho(g) \cdot W \subseteq W \forall g \in G$.
i.e. W is $\rho(g)$ -stable / invariant subspace of V .

Hence, by correspondence theorem, $\rho: G \rightarrow \text{GL}(V)$ is irreducible $\iff V$ is a simple $\mathbb{F}[G]$ module.

How do we recognise reducible representations?

Definition An \mathbb{F} -representation $\rho: G \rightarrow \text{GL}_n(\mathbb{F})$ is called **reducible** if $\exists T \in \text{GL}_n(\mathbb{F})$ s.t. $\forall g \in G$, we have equivalent matrices of the form $\rho'(g) = T^{-1} \rho(g) T = \begin{pmatrix} \chi_g & \gamma_g \\ 0 & \zeta_g \end{pmatrix}$ where χ_g is a $\dim W \times \dim W$ matrix.

Examples of irreducible / reducible maps -

- $\rho: D_8 \rightarrow \text{GL}_2(\mathbb{R})$ is irreducible, $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Suppose ρ is reducible, then $\exists W \subseteq V = \mathbb{R}^2$ s.t. W is a $\mathbb{R}[D_8]$ -invariant submodule of V , where $\dim_{\mathbb{R}}(W) = 1$. Suppose $W = \text{span}_{\mathbb{R}} \langle \lambda v_1 + \mu v_2 \rangle \subseteq V$. Apply $\rho(g)$ to W : let $w = \lambda v_1 + \mu v_2$, $\rho(x) \cdot w = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} \lambda \\ -\mu \end{pmatrix} = \mu v_1 - \lambda v_2 = \alpha(\lambda v_1 + \mu v_2)$. solve system to get $\lambda = 0$ or $\alpha = \beta$. Then we see that:
If $\lambda = 0$, $w = \mu v_2 = \text{span} \langle v_2 \rangle$ and this is not stable by $\rho(y)$ since $\rho(y) \cdot v_2 = v_1 \notin W$. Thus $\alpha = \beta$, but if $\mu \neq 0$, $w = \lambda v_1 = \text{span} \langle v_1 \rangle$, which is not stable. $\Rightarrow W = \{0\}$ since $\alpha = \beta = 0$, $\therefore \rho$ is irreducible. We will instead compute $\text{End}_{\mathbb{R}[D_8]}(\rho)$ = division ring (in the future).
- If $\mathbb{F} = \mathbb{F}_2$, then $W = \text{span}_{\mathbb{R}} \langle v_1 + v_2 \rangle \subseteq \mathbb{R}^2$ is $\rho(D_8)$ -stable. $\rho(x) \cdot w = \rho(x)(v_1 + v_2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = w$ in \mathbb{F}_2 . $\rho(y) \cdot w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = w$. Hence, ρ is reducible over \mathbb{F}_2 into direct sum of 1-dimensional representations.

Note - Reducibility depends on field chosen, as seen - $\rho: D_8 \rightarrow \text{GL}_2(\mathbb{R})$ is irreducible with above representation, but $\rho: D_8 \rightarrow \text{GL}_2(\mathbb{F}_2)$ can. $V = \mathbb{F}_2^2 = \text{span} \langle v_1, v_2 \rangle$.

- let $G = G_3$ and define the permutation representation $\rho: G \rightarrow \text{GL}_3(\mathbb{R})$, $e_i \mapsto g \cdot e_i$ for $g \in G$, $G = \langle x \mid x^3 = 1 \rangle$. $\rho(x) \cdot e_1 = x \cdot 1 = x = e_2$, $\rho(x) \cdot e_2 = x \cdot x = x^2 = e_3$, $\rho(x) \cdot e_3 = x \cdot x^2 = x^3 = 1 = e_1 \Rightarrow \rho(x) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. $\rho(x)$ is a reducible representation i.e. $\exists \mathbb{R}[G]$ -invariant subspaces.
i.e. V is a semisimple $\mathbb{R}[G]$ -module = direct sum of simple modules. Let $W = \text{span}_{\mathbb{R}} \langle w \rangle = \text{span} \langle e_1 + e_2 + e_3 \rangle = \text{span} \langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle$. W is $\mathbb{R}[G]$ -invariant subspace.
i.e. $\rho(x) \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $\rho(x^2) \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $\rho(g) \cdot w \subseteq \mathbb{R} \cdot w$. choose new basis $B' = \text{span} \langle w, e_2, e_3 \rangle$. Apply $\rho(x) \cdot w = w$, $\rho(x) \cdot e_2 = e_3$, $\rho(x) \cdot e_3 = w - e_2 - e_3$.
Thus, $\rho'(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. $\therefore \exists T \in \text{GL}_3(\mathbb{R})$ s.t. $\rho'(x) = T^{-1} \rho(x) T$, $T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

Projections.

If $V = U \oplus W$, then we can construct a special automorphism of V that depends on the expression $V = U \oplus W$.

Proposition suppose $V = U \oplus W$, define $\Pi: V \rightarrow U \subseteq V$, $v = u + w \mapsto u \forall u \in U, w \in W$. Then Π is an endomorphism of V and $\text{Ker}(\Pi) = W$, $\text{Im}(\Pi) = U$ and $\Pi^2 = \Pi$.

Definition An endomorphism Π of a vector space V which satisfies $\Pi^2 = \Pi$ is called a **projection**.

Proposition Suppose Π is a projection of V , then $V = \text{Ker}(\Pi) \oplus \text{Im}(\Pi)$.

Theorem (Maschke's theorem) (version important, but proof omitted) $\text{char}(\mathbb{F}) \nmid n \Rightarrow \underbrace{1 + 1 + \dots + 1}_n = 0$, n minimal.

Suppose G is a finite group, \mathbb{F} a field s.t. $\text{char}(\mathbb{F}) \nmid |G|$. Let V be an $\mathbb{F}[G]$ module, then for any $U \subseteq V$ where U is an $\mathbb{F}[G]$ -submodule. $\exists W \subseteq V$, an $\mathbb{F}[G]$ -submodule s.t. $V \cong U \oplus W$.

Remark - In our course, this tells us that any $\mathbb{F}[G]$ -module V with the above conditions is semisimple. i.e. $V = S_1 \oplus \dots \oplus S_n$ where each S_i is a simple $\mathbb{F}[G]$ -submodule.

Definition Let A, B, C be R -modules. A sequence of homomorphisms $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is exact at B if $\text{Ker}(\psi) = \text{Im}(\varphi)$.
 A sequence $A_{n+1} \xrightarrow{\varphi_{n+1}} A_n \xrightarrow{\varphi_n} A_{n-1} \xrightarrow{\varphi_{n-1}} \dots$ is exact everywhere if $\forall n \text{Ker}(\varphi_n) = \text{Im}(\varphi_{n+1})$. i.e. exact at every A_i .

Example - let A, C be R -modules, then $0 \rightarrow A \xrightarrow{i} A \oplus C \xrightarrow{p} C \rightarrow 0$ is an exact sequence. Here, the mappings are $i(a) = (a, 0)$, $p(a, c) = c$.
 $\dim: \text{Ker}(p) = \text{Im}(i)$. $p(a, c) = 0 \iff c = 0$ i.e. $(a, 0) \in \text{Ker}(p) \iff (a, 0) = i(a) \implies (a, 0) \in \text{Im}(i)$, q.e.d.
 \therefore sequence is exact at $A \oplus C$.

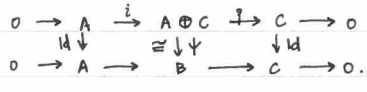
$\dim: 0 \rightarrow A \xrightarrow{i} A \oplus C \xrightarrow{p} C \rightarrow 0$ is exact at every module if i injective, p surjective $\iff \text{Ker}(p) = \text{Im}(i)$

Definition A short exact sequence $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$ means that:

- (1) $\text{Ker}(i) = \text{Im}(0 \rightarrow A) = 0$ is injective
- (2) $\text{Ker}(p) = \text{Im}(i)$
- (3) $\text{Ker}(C \rightarrow 0) = C = \text{Im}(p)$, p is surjective.

Definition The split exact sequence is a sequence s.t. if A, C are R -modules, then $0 \rightarrow A \xrightarrow{i} A \oplus C \xrightarrow{p} C \rightarrow 0$ is always exact; $i(a) = (a, 0)$, $p(a, c) = c$, $\text{Ker}(p) = \{ (a, c) : c = 0 \} = \{ (a, 0) : a \in A \} = \text{Im}(i)$.

Definition A short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ splits if \exists isomorphism of R -modules $\psi: A \oplus C \rightarrow B$ s.t. the following diagram commutes:



Note - short exact sequences usually do not split!

Examples -

1. Consider the \mathbb{Z} -module short exact sequence: $0 \rightarrow \mathbb{Z} \xrightarrow{x2} \mathbb{Z} \xrightarrow{[\cdot]} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$.
 $\mathbb{Z} \xrightarrow{x2} \mathbb{Z} \xrightarrow{[\cdot]} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$. This is exact, so $\text{Ker}([\cdot]) = \text{Im}(x2)$.
 Check: $\text{Ker}(\mathbb{Z}/2\mathbb{Z} \rightarrow 0) = \text{Im}(\mathbb{Z} \xrightarrow{[\cdot]} \mathbb{Z}/2\mathbb{Z})$. Suppose sequence splits, $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. This is a contradiction, as RHS contains element of finite order $\therefore (1, 0) = 0$, whereas LHS has no element of finite order.
2. $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{x2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{(\text{mod } 2)} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$. Then $\mathbb{Z}/2\mathbb{Z} \xrightarrow{x2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{(\text{mod } 2)} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$.
 $\mathbb{Z}/2\mathbb{Z} \xrightarrow{x2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{(\text{mod } 2)} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$. This is exact as $\text{Ker}((\text{mod } 2)) = \text{Im}(x2)$. However, this does not split since we observe that $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
3. The SES $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$ is split exact by definition.
4. The SES $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \rightarrow 0$ is split exact by the fact that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.
 i.e. $\exists \psi: \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ which is an isomorphism.

25 October 2013
Mr. Jamil NADIM
Maths 500

Theorem (Basis Theorem for Vector Spaces)

Let \mathbb{F} be a field. then every short exact sequence of vector spaces over \mathbb{F} splits.

Proof - Let $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$ be a SES of \mathbb{F} -vector spaces. 1. Let e_1, \dots, e_n be a basis for C (assume C is finite). 2. Choose $b_i \in B$ s.t. $p(b_i) = e_i$, for since p is surjective, we can hit all e_i . Define $s: C \rightarrow B$ by $s(e_i) = b_i$. 3. Check $pos = \text{Id}_C$. $\therefore pos(e_i) = p(b_i) = e_i$. 4. Check $pos = \text{Id}_C$. $\therefore pos(e_i) = p(b_i) = e_i$.
 Construct a splitting map $\psi: A \oplus C \rightarrow B$, by $\psi(a, c) = i(a) + s(c) \in B$. Claim: ψ is an isomorphism. ψ is obviously \mathbb{F} -linear because i and s are both \mathbb{F} -linear. 5. For surjectivity, let $b \in B$, define $\alpha = b - s(p(b))$. Apply $p(\alpha) = p(b) - p(s(p(b))) = p(b) - \text{Id}_C p(b) = p(b) - p(b) = 0$.
 $\implies \alpha \in \text{Ker}(p) = \text{Im}(i)$ by exactness. $\therefore \alpha = i(a)$ for some $a \in A$. Plug in and rearrange: $b = \alpha + s(p(b)) = i(a) + s(p(b)) = \psi(a, p(b))$ by definition of ψ .
 $\therefore \psi$ is surjective as every b is hit. 6. For injectivity, suppose $\psi(a, c) = 0 \implies i(a) + s(c) = 0 \implies s(c) = -i(a) \in \text{Im}(i) = \text{Ker}(p)$.
 Hence, $p(s(c)) = p(-i(a)) = 0 \implies (pos)(c) = \text{Id}_C(c) = 0 \implies c = 0$. $\therefore i(a) + s(0) = 0 \implies i(a) = 0 \implies a = 0$ since i is injective. $\implies (a, c) = (0, 0)$.
 $\therefore \psi$ is injective. Then ψ is an isomorphism that splits our SES, q.e.d.

Theorem (Maschke's Theorem, Version 2: Modern Form)

Let G be a finite group; let \mathbb{F} be a field in which $|G| \neq 0$ (e.g. if $G = \mathbb{Z}$, don't want $\mathbb{F} = \mathbb{F}_3$ as $|G| = 3 \equiv 0$ in \mathbb{F}_3). If $E = (0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0)$ is a SES of $\mathbb{F}[G]$ modules, then E splits. i.e. \exists an $\mathbb{F}[G]$ module isomorphism $\psi: A \oplus C \rightarrow B$ s.t. for $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$, the diagram commutes.

Proof - We need a homomorphism of $\mathbb{F}[G]$ -modules, $\psi: A \oplus C \rightarrow B$ s.t. $\psi(\lambda(a, c)) = \lambda\psi(a, c) \forall \lambda \in \mathbb{F}$, and $\psi(g(a, c)) = g\psi(a, c) \forall g \in G$.
 To start, let A, B, C be vector spaces over \mathbb{F} . (forget about G in $\mathbb{F}[G]$ for the moment). $0 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 0$. From the basis theorem, $\exists \mathbb{F}$ -linear map $\sigma: C \rightarrow B$ s.t. $pos = \text{Id}_C$. Need to produce a linear map s s.t. $pos = \text{Id}_C$ and s commutes with $g \in G$ as well.
 Maschke's trick: $\forall g \in G$, define $\sigma_g: C \rightarrow B$ by $\sigma_g(c) = g^{-1} \sigma(gc)$. Then $\sigma_g(hc) = g^{-1} \sigma(g(hc)) = h^{-1} g^{-1} \sigma(g(hc)) = h^{-1} (gh)^{-1} \sigma(g(hc)) = h^{-1} \sigma_g(hc)$ for $h \in G$.
 Put $\hat{s}: C \rightarrow B$. then $\hat{s}(c) = \sum_{g \in G} \sigma_g(c)$, the sum over all group elements. Then $\hat{s}(hc) = \sum_{g \in G} \sigma_g(hc) = \sum_{g \in G} h \sigma_{gh}(c) = h \left(\sum_{g \in G} \sigma_g(c) \right)$ by linearity, $= h\hat{s}(c)$. Now $\hat{s}: C \rightarrow B$ is $\mathbb{F}[G]$ -linear. However, $pos(c) = \sum_{g \in G} p\sigma_g(c)$ where $p\sigma_g(c) = p(g^{-1} \sigma(gc)) = g^{-1} p\sigma(gc)$ since p is $\mathbb{F}[G]$ -linear.
 $\therefore p\sigma(gc) = gc$, so $p\sigma_g(c) = g^{-1} gc = c \implies p\sigma_g = \text{Id}$. So apply to arbitrary element: $p\hat{s}(c) = |G|c$. If $|G| \neq 0$ in \mathbb{F} , we can invert:
 \therefore Define splitting map $s(c) = \frac{1}{|G|} \hat{s}(c)$ where s is $\mathbb{F}[G]$ linear. Define $\psi: A \oplus C \rightarrow B$ by $\psi(a, c) = i(a) + s(c)$. By basis theorem, ψ is \mathbb{F} -isomorphism and $\mathbb{F}[G]$ -linear. q.e.d.

$(B = A \oplus C)$

Examples that falsify Maschke's Theorem - If $|G| \neq 0$ in \mathbb{F} , then every $\mathbb{F}[G]$ -submodule $U \leq V$ has a complement $W \leq V$ st. $V = U \oplus W$.

1. If G is infinite, Maschke fails. Define $\rho: \mathbb{Z}_{\text{cop}} \rightarrow GL_2(\mathbb{C})$ by $n \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ for $n \neq 0$. This is a representation: $\rho(n+m) = \begin{pmatrix} 0 & n+m \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \rho(n)\rho(m)$.

Take a 1-dimensional $\mathbb{C}[\mathbb{Z}_{\text{cop}}]$ -submodule $U = \text{span}\{e_1\} = \lambda \langle \cdot \rangle$. Then U is $\mathbb{C}[\mathbb{Z}_{\text{cop}}]$ -invariant. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \lambda \end{pmatrix} \in U$ is an eigensubspace.

But U has no complement since matrix is not diagonalisable because $m(x) = (x-1)^2$. $\mathbb{C}^2 \cong U \oplus ?$

28 October 2015
Mr. Ismail NADIM.
Gordon, St (25) D103.

Recap of course thus far:

- ① Representations $\rho: G \rightarrow GL_n(\mathbb{C})$, $g \mapsto A$.
- ② Modules over rings M over R maps, submodules.
- ③ Simple/Semisimple modules $M = \bigoplus_{i \in I} S_i$.
- ④ Group ring $\mathbb{F}[G]$: modules over $\mathbb{F}[G] \xleftrightarrow{1:1} \rho$ representations of G .
- ⑤ Schur's lemma V_1, V_2 (simple modules).
- ⑥ Maschke's theorem using SES.

More examples where Maschke's theorem fails -

2. If $|G| = 0$ in \mathbb{F} i.e. $\text{char}(\mathbb{F}) \mid |G|$. Then $\rho: G_p \rightarrow GL_2(\mathbb{F}_p) \cong \text{Aut}(\mathbb{C}_p \times \mathbb{C}_p)$, $\mathbb{C}_p = \langle x \mid x^p = 1 \rangle$. Then $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$ s.t. $x^j \mapsto \begin{pmatrix} 1 & 0 \\ 0 & \zeta^j \end{pmatrix}$, $j \in \{0, 1, \dots, p-1\}$.

ρ defines a representation since $\rho(x^p) = \rho(x^p) = \rho(1)$. Let $U = \text{span}\{e_1\} \leq V$ be an $\mathbb{F}_p[G_p]$ -submodule of $V = \mathbb{F}_p^2$. Then U is \mathbb{C}_p -invariant.

$\rho(x^j)(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & \zeta^j \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1 \in U$. But $\nexists W \leq V$ s.t. $\mathbb{F}_p^2 \cong U \oplus W$. If there was such a W , then $\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$ would be diagonalisable. However,

$m_{\rho}(x) = (x-1)^2$, so there is only one eigenvalue \Rightarrow no complement for U .

Hint: ρ reducible completely \vee over $\mathbb{F}[G]$ semisimple $\Rightarrow \rho(g)$ diagonalisable $\forall g$. $\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \cong \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$.

3. If $|G| = 0$ in \mathbb{F} , let $\rho: D_8 \rightarrow GL_2(\mathbb{F}_2)$. $|D_8| = 8 = 0$ in \mathbb{F}_2 . $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then let $U = \text{span}\{e_1 + e_2\} = \text{span}\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$. Then

$U \leq V = \mathbb{F}_2^2$ is a D_8 -invariant submodule. $\rho(x) \cdot u = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = u$. $\rho(y) \cdot u = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}u$. Let $V = U \oplus W$, let $W = \text{span}\{\lambda e_1 + \mu e_2\}$. λ, μ not both zero.

If $\lambda = 0, \mu \neq 0 \Rightarrow W = \text{span}\{e_2\}$ and if $\lambda \neq 0, \mu = 0 \Rightarrow W = \text{span}\{e_1\}$. However, both are not D_8 -invariant by x . So $\nexists W$ s.t. $V = \mathbb{F}_2^2 = U \oplus W$.

Thus, $V = \mathbb{F}_2^2$ is not a simple $\mathbb{F}_2[D_8]$ -module.

The point of Maschke's theorem is to give us an algorithm to decompose V as an $\mathbb{F}[G]$ -module into $\bigoplus \mathbb{F}[G]$ -modules: Here we have an example where Maschke works:

Use S.E.S. proof / splitting map $s: A \oplus C \rightarrow B$. Define $\rho: S_3 \rightarrow GL_3(\mathbb{C})$ by $\sigma \cdot e_i = e_{\sigma(i)} \forall \sigma \in S_3$. $\sigma = (1 2 3) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $\tau = (1 2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Let $\rho: B \rightarrow C$ be the projection maps \mathbb{F} -modules: $\begin{matrix} e_1 \mapsto 0 \\ e_2 \mapsto 0 \\ e_3 \mapsto a + e_2 + e_3 \end{matrix}$. By basis theorem, $B \cong A \oplus C$ as \mathbb{F} -modules, and also as $\mathbb{F}[G]$ -modules using splitting map.

Use $s(w) = \frac{1}{|G|} \sum_{g \in S_3} g^{-1} \sigma(g \cdot v)$ to perform an averaging process. Then we get $V = \mathbb{C}^3 = U \oplus W = \text{Im}(s) \oplus \text{Ker}(s) = \text{span}\{e_1 - e_2, e_3 - e_2\}$ [dim 2].

By Maschke, $S_3 \cong D_6$ with $\rho: S_3 \rightarrow GL_3(\mathbb{C})$ is reducible i.e. $V = \mathbb{C}^3$ is a semi-simple $\mathbb{C}[S_3]$ -module = 1 dim submodule (simple) \oplus 2 dim submodule (simple). Even if not, can be further broken down.

Lemma Let V and W be R -modules st. $\text{Hom}_R(V, W) = \text{Hom}_R(W, V) = 0$. Then $\text{End}_R(V \oplus W) \cong \text{End}_R(V) \times \text{End}_R(W)$.

Proof - $\text{Hom}_R(V, W) = \text{ring matrices of the form } \begin{pmatrix} d_{VV} & d_{VW} \\ d_{WV} & d_{WW} \end{pmatrix}$ where $d_{VV}: V \rightarrow V$, $d_{VW}: V \rightarrow W$, $d_{WV}: W \rightarrow V$, $d_{WW}: W \rightarrow W$ are R -linear module homomorphisms.

Since $\text{Hom}_R(V, W) = \text{Hom}_R(W, V) = 0 \therefore \text{End}_R(V \oplus W) \xrightarrow{\cong} \text{End}_R(V) \times \text{End}_R(W)$ defines an isomorphism $\alpha \mapsto (d_{VV}, d_{WW})$, $q \in d$.

Schur's Lemma revisited for $\mathbb{F}[G]$ -modules $\leftrightarrow \rho$ reps of G .

(V1) If M, N are simple non-zero modules, then $\varphi: M \rightarrow N$ is either 0 or homomorphism.

(V2) If M is a simple $\mathbb{F}[G]$ -module, then $\text{End}_{\mathbb{F}[G]}(M)$ is a division ring. i.e. $\varphi \in \text{End}_{\mathbb{F}[G]}(M)$ then $\varphi = \lambda \text{Id}$ for λ a non-zero eigenvalue since \mathbb{F} is algebraically closed.

Note - In (V1) we do not require \mathbb{F} to be algebraically closed.

(V3) [Strong form]. If V is a finitely-generated $\mathbb{F}[G]$ -module, then V is simple $\Leftrightarrow \text{End}_{\mathbb{F}[G]}(V)$ is a division ring.

Proof - (\Rightarrow) (V2). (\Leftarrow) Suppose $V \cong S_1^{n_1} \oplus \dots \oplus S_m^{n_m}$ is semi-simple. Then $\text{End}_{\mathbb{F}[G]}(V) = \text{End}_{\mathbb{F}[G]}(S_1^{n_1} \oplus \dots \oplus S_m^{n_m})$, n_i are dimension of S_i , $S_i \neq S_j$ if $i \neq j$.

$= \text{End}_{\mathbb{F}[G]}(S_1^{n_1}) \oplus \dots \oplus \text{End}_{\mathbb{F}[G]}(S_m^{n_m})$ [commut HW2 or previous lemma]. $= M_{n_1}(\text{End}_{\mathbb{F}[G]}(S_1)) \oplus \dots \oplus M_{n_m}(\text{End}_{\mathbb{F}[G]}(S_m))$.

$= \bigoplus_{i=1}^m M_{n_i}(\text{End}_{\mathbb{F}[G]}(S_i))$. Assume $\text{End}_{\mathbb{F}[G]}(V)$ is a division ring, then $\bigoplus_{i=1}^m M_{n_i}(\text{End}_{\mathbb{F}[G]}(S_i)) \xrightarrow{\text{Schur}} \bigoplus_{i=1}^m M_{n_i}(D_i)$ (division rings).

The RHS is a division ring if \exists unique r s.t. $n_i = 1 \forall i \neq r \Rightarrow V \cong S_r$ simple. $\text{End}_{\mathbb{F}[G]}(V) = M_{n_r}(D_r)$.

Schur's lemma (V3) is a tool for detecting when a representation is irreducible/reducible i.e. when V as an $\mathbb{F}[G]$ -module is simple/semi-simple.

Some elegant examples of Schur (V3) -

1. Let $\rho: D_8 \rightarrow GL_2(\mathbb{C})$. $x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Is ρ irreducible (= simple as a $\mathbb{C}[D_8]$ -module)? Compute $\text{End}_{\mathbb{C}[D_8]}(\rho)$ = all complex 2×2 matrices that commute with all $g \in D_8$.

i.e. $A \in GL_2(\mathbb{C})$ st. $A \rho(g) = \rho(g) A \forall g \in D_8$. Only need to do $A \rho(x) = \rho(x) A$, $A \rho(y) = \rho(y) A$ (conjugates the generators). Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$A \rho(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\rho(x) A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow a=d, c=b$ simply by comparing terms. Then $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Then we observe that

$A \rho(y) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & -b \\ -b & -a \end{pmatrix}$, $\rho(y) A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \Rightarrow a=a, b=-b \Rightarrow 2b=0, b=0 \Rightarrow A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. $\therefore \text{End}_{\mathbb{C}[D_8]}(\rho) = \{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{C} \} \cong \mathbb{C}$.

by $A \mapsto a$, which is a division ring. Therefore, ρ is an irreducible 2-dimensional representation of $D_8 \Rightarrow V = \mathbb{C}^2$ is simple as $\mathbb{C}[D_8]$ -module.

2. Let $\sigma: D_6 \rightarrow GL_3(\mathbb{C})$. $\sigma(x) = (1 2 3) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $\sigma(y) = (1 2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Is σ irreducible? Compute $\text{End}_{\mathbb{C}[D_6]}(\sigma) \Rightarrow$ all $M_3(\mathbb{C})$ that commutes with generators.

$\text{End}_{\mathbb{C}[D_6]}(\sigma) = \{A \in \text{GL}_3(\mathbb{C}) \mid A\sigma(x) = \sigma(x)A, A\sigma(y) = \sigma(y)A\}$. Let $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}$. $A\sigma(x) = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} b & f & a \\ h & k & g \\ a & c & d \end{pmatrix}$, $\sigma(x)A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix} = \begin{pmatrix} d & e & f \\ a & b & c \\ g & h & k \end{pmatrix}$.
Then $a=k=e, b=g=f, c=h=d \Rightarrow A = \begin{pmatrix} a & b & c \\ b & a & c \\ c & b & a \end{pmatrix}$. Then $A\sigma(y) = \begin{pmatrix} a & b & c \\ b & a & c \\ c & b & a \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} b & a & c \\ c & b & a \\ a & c & d \end{pmatrix}$, $\sigma(y)A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix} = \begin{pmatrix} d & e & f \\ a & b & c \\ g & h & k \end{pmatrix}$.
As such, $a=a, b=c \Rightarrow A = \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix}$. $\therefore \text{End}_{\mathbb{C}[D_6]}(\sigma) = \left\{ \begin{pmatrix} a & b & b \\ b & a & b \\ b & b & a \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \cong \mathbb{C}^2$ by $A \mapsto (a, b)$. \mathbb{C}^2 is not a division ring. e.g. $(1, 0)^{-1}$ does not exist.

$\therefore \rho: D_6 \rightarrow \text{GL}_3(\mathbb{C})$ is not irreducible \Rightarrow it is reducible $\Rightarrow V = \mathbb{C}^3$ is a semisimple $\mathbb{C}[D_6]$ -module.

Definition Let $\rho_1: G \rightarrow \text{GL}(U)$ and $\rho_2: G \rightarrow \text{GL}(W)$ be two representations of G . Then define the direct sum of representations $(\rho_1 \oplus \rho_2)(g) = \rho_1(g) \oplus \rho_2(g)$ be the map $\rho_1 \oplus \rho_2$ with representation space $U \oplus W$. Let $\text{span}\{u_1, \dots, u_m\} = U$ and $\text{span}\{w_1, \dots, w_n\} = W$. Then with respect to these bases $\rho_1: G \rightarrow \text{GL}_m(\mathbb{C})$ and $\rho_2: G \rightarrow \text{GL}_n(\mathbb{C})$, $\therefore \rho_1 \oplus \rho_2$ w.r.t. $\{u_1, \dots, u_m, w_1, \dots, w_n\}$ gives a representation. $\rho_1 \oplus \rho_2: G \rightarrow \text{GL}_{m+n}(\mathbb{C})$, $g \mapsto \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ is a block diagonal matrix.

Observe that from our last example, $\sigma: D_6 \rightarrow \text{GL}_3(\mathbb{C})$ in the last example was a direct sum of 2 simple (1-dim & 2-dim) $\mathbb{C}[G]$ -modules.

Example 1. Let $\rho_1: G \rightarrow \text{GL}_1(\mathbb{C})$ and $\rho_2: G \rightarrow \text{GL}_2(\mathbb{C})$ was conjugated, so we could not easily identify A and B.

We now classify all representations of finite abelian groups over \mathbb{C} :

Let G be a finite abelian group, $G_1 \times \dots \times G_n$. Let V be a simple $\mathbb{C}[G]$ -module. Since G is abelian, $g \cdot (xv) = gxv = xg \cdot v \ \forall x, g \in G, \forall v \in V$.

Let $\rho_x \in \text{End}_{\mathbb{C}[G]}(V)$, $\rho_x: V \rightarrow V$, $v \mapsto xv$ for fixed $x \in G$. By Schur (V2), $\text{End}_{\mathbb{C}[G]}(V)$ is a division ring as V is simple, so every map has an inverse. $\therefore \rho_x = \lambda_x \text{Id}$ for $\lambda_x \neq 0, \lambda_x \in \mathbb{C}$. \therefore by substitution, our map is $\lambda_x \text{Id}: V \rightarrow V$, $v \mapsto \lambda_x v \Rightarrow$ scalar multiple of $v \Rightarrow \lambda_x \in \mathbb{C}$.

Then V is simple $\Rightarrow \dim V = 1 \Rightarrow$ every irreducible $\mathbb{C}[G]$ -module is one-dimensional: every irreducible representation of G is 1-dimensional.

Example 1. Let $\rho_1: C_n \rightarrow \text{GL}_1(\mathbb{C})$, $x \mapsto \lambda_1^k$, $\lambda_1^k = e^{\frac{2\pi i k}{n}}$, i.e. $x \mapsto \xi_1^k$, $\mathbb{C}[C_n] \cong \mathbb{C}[x]/(x^n - 1) = \mathbb{C}[x]/(x-1) \times \dots \times \mathbb{C}[x]/(x-\xi_{n-1})$.

2. $\rho: C_2 \times C_2 \rightarrow \text{GL}_4(\mathbb{C})$, $\rho_1: x \mapsto 1, \rho_2: y \mapsto -1, \rho_3: x \mapsto -1, \rho_4: y \mapsto -1$.

Let $G = C_n = \langle x \mid x^n = 1 \rangle$. We can define $|C_n| = n$ irreducible 1D representations by $\rho_\lambda: C_n \rightarrow \text{GL}_1(\mathbb{C})$, $x \mapsto \lambda x \in \mathbb{C}$, $\lambda^n = e^{\frac{2\pi i k}{n}}$. $\mathbb{C}[C_n] \cong \mathbb{C}[x]/(x^n - 1) \cong \mathbb{C}[x]/(x-1) \times \dots \times \mathbb{C}[x]/(x-\xi_{n-1}) \cong \mathbb{C} \times \dots \times \mathbb{C} \Rightarrow \rho_1 \times \dots \times \rho_n$ are representations.

1 November 2013
Mr Jamil NADIM
Maths 500.

Let $G = C_2 \times C_2$. There are $|G| = 4$ irreducible representations of $C_2 \times C_2$. $\rho_1: C_2 \times C_2 \rightarrow \text{GL}_1(\mathbb{C})$ by $x \mapsto 1$ or $y \mapsto -1$ or $x \mapsto -1$ or $y \mapsto 1$. So $\mathbb{C}[C_2 \times C_2] \cong U_1 \oplus U_2 \oplus U_3 \oplus U_4 \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$, where the U_i are all submodules of dimension 1.

3. Example: define $\rho: C_n \rightarrow \text{GL}_n(\mathbb{C})$, $x \mapsto \begin{pmatrix} \lambda_0 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ = direct sum of all the simple representations of dimension 1.

Definition The regular representation corresponds to a module $\mathbb{C}[G]$ as a $\mathbb{C}[G]$ -module (by correspondence theorem). Since $\mathbb{C}[G] \cong \mathbb{C}[G]$ is a \mathbb{C} -algebra with basis $B = \{g \mid g = 1, g_1, \dots, g_n\}$ define the regular representation $\rho_{\text{reg}}: G \rightarrow \text{GL}(\mathbb{C}[G]) = \text{GL}(|G|)$ by $g \mapsto \rho_g$ where ρ_g is a matrix obtained by left g -action on the basis B $\rho_g g_i = g_i \rightarrow$ matrix $\rho_{\text{reg}}(g)$. Point: ρ_{reg} is always reducible.

Examples of regular representations -

1. Let $G = C_3 = \langle x \mid x^3 = 1 \rangle$. Label $g_1 = 1, g_2 = x, g_3 = x^2$. $\rho_{\text{reg}}: G \rightarrow \text{GL}_3(\mathbb{C}) = \text{GL}(\mathbb{C}[G])$. $\rho_{\text{reg}}(g_1) = \rho_{\text{reg}}(1) = x1 = x = g_2$. $\rho_{\text{reg}}(g_2) = \rho_{\text{reg}}(x) = x \cdot x = x^2 = g_3$. $\rho_{\text{reg}}(g_3) = \rho_{\text{reg}}(x^2) = x \cdot x^2 = 1 = g_1$. $\rho: x \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \rho_{\text{reg}}(x)$.
Fact: $\mathbb{C}[G] = \rho_{\text{reg}}$ is reducible = semisimple and we decompose using Wedderburn and Maschke: $\mathbb{C}[G] \cong U_1 \oplus \dots \oplus U_r \cong S_1^{m_1} \oplus \dots \oplus S_r^{m_r}$, where U_i are simple.

$\mathbb{C}[G]$ -submodules of dim $\neq n$. $\cong M_{n_1}(\mathbb{C}) \times \dots \times M_{n_r}(\mathbb{C}) \cong \rho_1 \times \dots \times \rho_r =$ all irreducible reps of G . By an old proposition, any simple $\mathbb{C}[G]$ -submodule is $\cong S_i$ for some i .

2. $C_3 = \langle x \mid x^3 = 1 \rangle$. Decompose $\mathbb{C}[C_3]$: let $U_1 = 1 + x + x^2 \in \mathbb{C}[C_3]$, $U_1 = \text{span}\{u_1\}$ then $x \cdot u_1 = x + x^2 + 1 = 1 \cdot u_1 \Rightarrow U_1 \leq \mathbb{C}[G]$ (as it is $\mathbb{C}[G]$ -invariant), where U_1 is a 1D submodule. (and we said every submodule is giving us a representation). Let $u_2 = 1 + w^2x + wx$, $x \cdot u_2 = w + w^2x + wx^2 \Rightarrow U_2 = \text{span}\{u_2\} \leq \mathbb{C}[G]$. $\therefore U_2$ is a 1D submodule giving us a representation by $x \mapsto w$. Let $u_3 = 1 + wx + w^2x$. Repeat do above. Then $\mathbb{C}[C_3] \cong U_1 \oplus U_2 \oplus U_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

Corollary if all irreducible representations are of dimension 1, then G is abelian.

Proof - By Maschke and Wedderburn, we can decompose $\mathbb{C}[G] \cong U_1 \oplus U_2 \oplus \dots \oplus U_r$ where all the U_i are 1D by assumption. Choose a basis $\{u_1, \dots, u_r\}$ and write matrix action on the basis. $\rho(g) = \begin{pmatrix} \lambda_0 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$, which is diagonal. $G/\text{ker}(\rho) \cong \text{Im}(\rho) \subseteq \{\text{diagonal matrices}\}$. $\therefore G$ is abelian, q.e.d.

Remark - A consequence of this is that if \exists an irreducible/simple representation of dim ≥ 2 , then G is non-commutative i.e. non-abelian i.e. $\exists \rho: G \rightarrow \text{GL}_n(\mathbb{C})$ $n \geq 2$ (e.g. D_6, Q_8 etc).

Theorem $\mathbb{C}[G]$ is a semisimple algebra $\Leftrightarrow \mathbb{C}[G]$ viewed as a $\mathbb{C}[G]$ -module is semisimple.

Proof - Suppose $\mathbb{C}[G]$ is semisimple, where the S_i are non-isomorphic simple submodules of dim n : $\mathbb{C}[G]^{\oplus} = \text{End}_{\mathbb{C}[G]}(\mathbb{C}[G]) = \text{End}(S_1^{m_1} \oplus \dots \oplus S_r^{m_r}) = \text{End}(S_1^{m_1}) \oplus \dots \oplus \text{End}(S_r^{m_r}) = M_{m_1}(\text{End}(S_1)) \oplus \dots \oplus M_{m_r}(\text{End}(S_r))$. Usim: $\text{End}(S_i) \cong \mathbb{C}$. This is because $\text{End}(S_i)$ is a division ring (by Schur's v2 + Burnside's lemma), but the only division ring over \mathbb{C} is \mathbb{C} , so $\text{End}(S_i) \cong \mathbb{C}$. $\therefore M_{m_i}(\mathbb{C}) \oplus \dots \oplus M_{m_r}(\mathbb{C}) = \mathbb{C}[G]^{\oplus}$. Take opposites again: then we get that overall, $\mathbb{C}[G] = (\mathbb{C}[G]^{\oplus})^{\oplus} = (M_{m_1}(\mathbb{C}) \oplus \dots \oplus M_{m_r}(\mathbb{C}))^{\oplus} = M_{m_1}(\mathbb{C})^{\oplus} \oplus \dots \oplus M_{m_r}(\mathbb{C})^{\oplus} = M_{m_1}(\mathbb{C}) \oplus \dots \oplus M_{m_r}(\mathbb{C}) = \rho_1 \oplus \dots \oplus \rho_r$ q.e.d.

Definition The values $\dim_{\mathbb{C}}(S_i) = n_i$ are the degrees of the irreducible representations of G .

Corollary order of group, $|G| = n_1^2 + \dots + n_r^2$.

Proof - $|G| = \dim_{\mathbb{C}}(\mathbb{C}[G]) = \dim_{\mathbb{C}}(\bigoplus_{i=1}^r M_{n_i}(\mathbb{C})) \xrightarrow{\text{Wedderburn}} \sum_{i=1}^r \dim(M_{n_i}(\mathbb{C})) = n_1^2 + \dots + n_r^2$ where $\dim_{\mathbb{C}}(M_{n_i}(\mathbb{C})) = n_i^2$.

thus, we obtain a generalised approach to decomposing $\mathbb{C}[G]$ and classifying representations for G .

Note - This only provides us with information on the type of representations (and their degrees), but not the matrices themselves.

1. Decompose $\mathbb{C}[G]$, then $\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \times \dots \times M_{n_r}(\mathbb{C})$.
2. Note that $|G| = n_1^2 + \dots + n_r^2$.
3. We can always take $n_1 = 1$ as we always have the trivial representation.
4. Each $n_i \mid |G|$ exactly.
5. We stop at $r = \text{number of conjugacy classes of } G = \#\{x \in G\} = \#\{g x g^{-1} : g \in G\}$.

We examine several examples of group rings, as follows.

1. $\mathbb{C}[C_2]$. We begin by finding the conjugacy classes of $C_2 = \{1, x \mid x^2 = 1\}$. These are $\{1\}$ and $\{x\}$, so $r=2$. $|G| = |C_2| = 2 = n_1^2 + n_2^2$ and we may take $n_1=1$, so, $2 = 1 + n_2^2$.

Thus, we must have $n_2=1$. So there are 2 representations: $\mathbb{C}[C_2] = M_1(\mathbb{C}) \times M_1(\mathbb{C}) = \mathbb{C} \times \mathbb{C}$
 $\begin{pmatrix} x \mapsto 1 \\ 1 \mapsto 1 \end{pmatrix} \quad \begin{pmatrix} x \mapsto -1 \\ 1 \mapsto -1 \end{pmatrix}$

2. $\mathbb{C}[C_3]$. The conjugacy classes of $C_3 = \{1, x, x^2 \mid x^3 = 1\}$ are $\{1\}, \{x\}, \{x^2\} \Rightarrow r=3$. Then we have $|G| = |C_3| = 3 = n_1^2 + n_2^2 + n_3^2 = 1^2 + n_2^2 + n_3^2$.

This again forces us to take $n_2 = n_3 = 1$. As such, we have $n_1 = n_2 = n_3 = 1$ and therefore,

$\mathbb{C}[C_3] = M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_1(\mathbb{C}) = \mathbb{C} \times \mathbb{C} \times \mathbb{C}$ which corresponds to $\rho_1 \times \rho_2 \times \rho_3$ where $w = e^{\frac{2\pi i}{3}}$ is the cube root of unity.

$\Rightarrow C_3$ has only 3 irreducible 1D representations.

3. $\mathbb{C}[D_6]$. The conjugacy classes of D_6 are $\{1\}, \{s\}, \{y\} \Rightarrow r=3$. $|G| = |D_6| = 6 = n_1^2 + n_2^2 + n_3^2 = 1 + n_2^2 + n_3^2 \Rightarrow n_1 = n_2 = 1, n_3 = 2$ wlog. Then,

$\mathbb{C}(D_6) = M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_2(\mathbb{C}) \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \cong \rho_1 \times \rho_2 \times \rho_3$
 $\begin{pmatrix} x \mapsto 1 \\ y \mapsto 1 \end{pmatrix} \quad \begin{pmatrix} x \mapsto 1 \\ y \mapsto -1 \end{pmatrix} \quad \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

thus, we see that D_6 has 2 simple 1D representations, and 1 simple (i.e. irreducible) 2D representation only.

Note - The matrix $\begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}$ is irreducible.

We can always bring it to the standard form by finding T s.t. $T \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix} T^{-1}$ = standard model.

4. Wedderburn Decomposition of $\mathbb{C}[Q_8]$. $Q_8 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y \mid x^4 = y^4 = 1, x^2 = y^2, x^i x^j = x^{i+j}, x^i y = y x^i\}$. We have conjugacy classes: $\{x\} = \{x, x^3, x^5, x^7\}$. 11 November 2013.

These are $\{1\}, \{x^2\}, \{x, x^3\}, \{y, x^2y\}, \{xy, x^3y\} \Rightarrow r=5$. Solve $|Q_8| = 8 = n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 1^2 + 1^2 + 1^2 + 1^2 + n_5^2$ is only solution up to order. Mr Jamir NADIM.

$\mathbb{C}[Q_8] = M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_1(\mathbb{C}) \times M_2(\mathbb{C}) \cong \mathbb{C}^{(4)} \times M_2(\mathbb{C}) \Rightarrow$ 4 irreducible 1D reps: $\rho_1, \rho_2, \rho_3, \rho_4: Q_8 \rightarrow \mathbb{C}$
 1 unique 2D rep: $\rho_5: Q_8 \rightarrow GL_2(\mathbb{C})$. Gordon St (25) D103.

5. Take $G = D_{10} = \langle x, y \mid x^5 = y^2 = 1, yx = xy \rangle$. Conjugacy classes are $\{1\}, \{x, x^4\}, \{x^2, x^3\}, \{y, xy, x^2y, x^3y, x^4y\} \Rightarrow r=4$. Solve $|D_{10}| = 10 = n_1^2 + n_2^2 + n_3^2 + n_4^2 = 1^2 + 1^2 + 2^2 + 2^2$.

Then $\mathbb{C}[D_{10}] \cong M_1(\mathbb{C}) \times M_2(\mathbb{C})^{(2)} = \mathbb{C}^{(2)} \times M_2(\mathbb{C})^{(2)} \Rightarrow$ 2 irreducible 1D reps, 2 irreducible 2D reps only.

6. Take $G = A_4 = \{ \sigma \in S_4 : \text{sgn}(\sigma) = +1 \}$ = even permutations on 4 items. $A_4 = \langle (1, 2, 3, 4) \mid s^2 = t^3 = (st)^2 = 1, x^2 = 1, x^2 s = st, x^2 t = ts \rangle$ where we have

$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, st = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. We then compute conjugacy classes: $\{1\}, \{s, t, st\}, \{x, xs, xt, xst\}, \{x^2, x^2s, x^2t, x^2st\} \Rightarrow r=4$. Solve $|A_4| = 12 = n_1^2 + n_2^2 + n_3^2 + n_4^2 = 1^2 + 1^2 + 1^2 + 3^2$ upto order \Rightarrow 3 irreducible 1D reps, 1 irreducible 3D rep only.

Definition An $\mathbb{F}[G]$ -module M is completely reducible when $M = \bigoplus_{i=1}^r M_i = M_1 \oplus \dots \oplus M_r$, where each M_i is a simple $\mathbb{F}[G]$ -submodule.

Lemma (Maschke's Theorem)

If G finite, $|G| \neq 0$ in \mathbb{F} , then every $\mathbb{F}[G]$ -module M is completely reducible (semisimple) into $\mathbb{F}[G]$ -submodules. \therefore each M_i is simple and of any dimension.

Proof - If M is simple, nothing to prove. So suppose M is semisimple. Then choose an $\mathbb{F}[G]$ submodule of each possible dimension, say M_1 . Proof by induction.

By induction hypothesis, any $\mathbb{F}[G]$ -module of dimension $< \dim_{\mathbb{F}}(M)$ is completely reducible. Form a SES: $0 \rightarrow M_1 \rightarrow M \xrightarrow{\text{which splits by Maschke}} M/M_1 \rightarrow 0, \mathbb{F}[G] \rightarrow M/M_1$

Since $M_1 \neq \{0\}$, $\dim(M_1) < \dim M \Rightarrow \dim_{\mathbb{F}}(M/M_1) < \dim_{\mathbb{F}}(M) \therefore$ By induction hypothesis, $M/M_1 \cong M_2 \oplus \dots \oplus M_r \hookrightarrow M \cong M_1 \oplus M_2 \oplus \dots \oplus M_r$
 $\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \oplus \dots \oplus M_{n_r}(\mathbb{C})$.

We seek a more rapid approach to test conjugacy classes. The conjugacy classes of x is $\{x^g = gxg^{-1} : g \in G\}$. Also, note that conjugacy classes are disjoint.

Definition The **centre** of a group ring $Z(\mathbb{C}[G]) = \{z \in \mathbb{C}[G] \mid \exists x \in G \forall z \in \mathbb{C}[G] : zx = xz\}$ (i.e. the set of elements that commute with all others).

Lemma $\dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = r$.

Proof - By Wedderburn and Maschke, $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \dots \times M_{n_r}(\mathbb{C})$, so $Z(\mathbb{C}[G]) \cong Z(M_{n_1}(\mathbb{C})) \times \dots \times Z(M_{n_r}(\mathbb{C})) \cong \mathbb{C} \times \mathbb{C} \times \dots \times \mathbb{C}$ (r copies).
since $Z(M_{n_i}(\mathbb{C})) = \{ \begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix} : * \in \mathbb{C} \} \cong \mathbb{C} \Rightarrow \therefore \dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = r$ where $\mathbb{C}[G]$ is a \mathbb{C} -algebra, $Z(\mathbb{C}[G])$ is a \mathbb{C} -subalgebra.

Theorem If G is finite, in $\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \times \dots \times M_{n_r}(\mathbb{C})$, where $r = \text{no. of conjugacy classes}$.

Proof - let $z = \sum_{g \in G} \lambda_g g \in Z(\mathbb{C}[G]) = \{z \in \mathbb{C}[G] \mid zx = zx \forall x \in G\}$ and conjugate $\forall h \in G : hzh^{-1} = z = \sum \lambda_g g$ (since $z \in Z(\mathbb{C}[G])$).

Also by definition, $hzh^{-1} = h(\sum \lambda_g g)h^{-1} = \sum \lambda_g h g h^{-1} = \sum \lambda_{hg^{-1}h} g \Rightarrow$ coefficients are constant on conjugacy classes. $\Rightarrow \therefore r$ in n_r refers to the number of conjugacy classes. Basis for $Z(\mathbb{C}[G])$ consists of linear combinations: $\sum_{g \in K_i} g$ where K_i is a conjugacy class. $\therefore \dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = r$, qed.

Examples of applications -

1. $G = D_6 = \langle x, y \mid x^3 = y^2 = 1, yx = xy^2 \rangle$. Conjugacy classes are $\{1\}, \{x, x^2\}, \{y, xy, xy^2\} \Rightarrow r=3$. $L = 1^2 + 1^2 + 2^2$, $\mathbb{C}[D_6] = \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$, and a basis for $Z(\mathbb{C}[D_6])$ is $\{1, x+x^2, y+xy+xy^2\}$ and $\dim Z(\mathbb{C}[D_6]) = 3$.

We now examine some formulae to compute conjugacy classes. We first recall some definitions - $\textcircled{1}$ the conjugacy classes of $x : x^g = gxg^{-1} : g \in G$. The centraliser of x is $C_G(x) = \{g \in G : gx = xg\}$. Then the size of $K^x = \frac{|G|}{|C_G(x)|}$ by the orbit-stabiliser theorem. $\textcircled{2}$ The class Equation is $G = Z(G) + \sum_{i=1}^r K_i$.

Conjugacy classes are as follows -

- For all cyclic groups, $C_n = \langle x \mid x^n = 1 \rangle$. $\forall x^i \in C_n$, $x^j x^i x^{-j} = x^{i+j-i} = x^i \Rightarrow$ each x^i is its own conjugacy class. $C_n = \{1, x, x^2, \dots, x^{n-1}\}$. $1^{C_n} = \{1\}$, $x^{C_n} = \{x\}$, $(x^2)^{C_n} = \{x^2\}$ etc. $\Rightarrow n$ conjugacy classes $\{1, x, \dots, x^{n-1}\} \Rightarrow n$ 1D representations, $\mathbb{C}[C_n] = \mathbb{C} \times \mathbb{C} \times \dots \times \mathbb{C}$.
 - Finite abelian groups $C_{n_1} \times \dots \times C_{n_r}$ works the same way. $C_2 \times C_2 = \{1, x, y, xy\}$, $x^{C_2 \times C_2} = \{x\}$.
 - Dihedral groups: $D_{2n} = \langle x, y \mid x^n = y^2 = 1, yx = x^{n-1}y \rangle$. If n is odd (e.g. D_6, D_{10}, D_{14}), there are $\frac{n+3}{2}$ conjugacy classes, which are $\{1\}, \{x, x^2, \dots, x^{n-1}\}, \{y, xy, xy^2, \dots, x^{n-1}y\}$. For instance, $D_{14} \Rightarrow 14 = 2 \times 7 \Rightarrow \frac{14+3}{2} = 5$ conjugacy classes, which are $\{1\}, \{x, x^2, \dots, x^6\}, \{x^7, x^8, \dots, x^{13}\}, \{y, xy, xy^2, \dots, x^6y\}$.
 - If n is even (e.g. D_8, D_{12}), then there exist $m+3$ conjugacy classes, where $m = \frac{n}{2}$. These are $\{1\}, \{x, x^2, \dots, x^{m-1}\}$ for $i=1, 2, \dots, m-1$, and $\{x^i y : 0 \leq i \leq m-1\}$, $\{x^i y^2 : 0 \leq i \leq m-1\}$ several sets, possibly. E.g. $D_8 \Rightarrow 8 = 4 \times 2 \Rightarrow m+3 = 5$ conjugacy classes, which are $\{1\}, \{x, x^2\}, \{x, x^3\}, \{y, x^2y\}, \{xy, x^3y\}$.
4. **Permutation** conjugacy classes: # conjugacy classes = # permutation sets of same shape and size. e.g. $S_3 = \{1d, (12), (13), (23), (123), (132)\}$. Then, the conjugacy classes are $\{1d\}, \{(12), (13), (23)\}, \{(123), (132)\} \cong \{1, (12), (13), (23)\}$, which is conjugate to $S_3 \cong D_6$. Likewise, we have the structure of S_4 - for $|S_4| = 24$, we have $\{1, (12), (13), \dots\}$ transpositions, $\{(12)(34), \dots\}$ products of transpositions, $\{(123), (132), \dots\}$ 3-cycles, and $\{(1234), \dots\}$ 4-cycles. This is consistent with the partition of n , $p(n)$. e.g. for 5, $5 = 0+5, 1+4, 2+3, 1+1+3, 1+1+1+2, 1+1+1+1+1 \Rightarrow S_4$ has $p(4) = 5$ conjugacy classes, S_5 has 7. $\mathbb{C}[S_5] = \mathbb{C}^{n_1^2} + \dots + \mathbb{C}^{n_r^2}$.

Tensor Products.

These give us a way to break down structures such as $\mathbb{C}[G \times H]$ to the form $\bigoplus M_{n_i}(\mathbb{C})$. This works as $\mathbb{C}[G \times H] \cong \mathbb{C}[G] \otimes \mathbb{C}[H]$ for a tensor product \otimes .

Beware! These are not like $V \times W$, direct products of vector spaces... nor like direct sums \oplus . We know that $V \times W \cong V \oplus W$ for finite V, W . What about infinite vector spaces? We know that $\bigoplus_{i=1}^{\infty} V_i \subset \prod_{i=1}^{\infty} V_i$ is a proper subset, but $\bigoplus_{i=1}^{\infty} V_i \neq \prod_{i=1}^{\infty} V_i$. For instance, $\bigoplus_{i=1}^{\infty} \mathbb{R} \neq \prod_{i=1}^{\infty} \mathbb{R}$, since $(1, 1, 1, \dots) \notin \bigoplus_{i=1}^{\infty} \mathbb{R}$. Both vectors belong to $\prod_{i=1}^{\infty} \mathbb{R}$.

We care about finite vector spaces: recall $\dim_{\mathbb{F}}(V \oplus W) = \dim_{\mathbb{F}}(V \times W) = \dim(V) + \dim(W)$.

Consider tensor products $V \otimes_{\mathbb{F}} W$ over fields \mathbb{F} . The idea is to construct a vector space $V \otimes_{\mathbb{F}} W$ whose elements look like $\sum_{i,j} v_i \otimes w_j$ where i, j are arbitrary. 13 November 2013. Mr Iqbal MAM Maths 500. To obey: $\forall \lambda \in \mathbb{F}, \forall v, v' \in V, \forall w, w' \in W$.

so for example: $\sum_{i=1}^k v_i \otimes w_i = v_1 \otimes w_1 + v_2 \otimes w_2 + \dots + v_k \otimes w_k$, k arbitrary. Contrast this with $V \oplus W = (v, w) = (v, 0) + (0, w)$. We want \otimes to obey: (1) $v \otimes (w + w') = v \otimes w + v \otimes w'$ (2) $(v + v') \otimes w = v \otimes w + v' \otimes w$ and (3) (Key Rule) $\lambda(v \otimes w) = \lambda v \otimes w = v \otimes \lambda w$.

Generally, if $v = \sum_{i=1}^m \lambda_i v_i$ and $w = \sum_{j=1}^n \mu_j w_j$, then $v \otimes w = \sum_{i,j} \lambda_i \mu_j (v_i \otimes w_j)$. For example - $v = 2v_1 - v_2$, $w = w_1 + 3w_2$. Then $v \otimes w = (2v_1 \otimes w_1) + (2v_1 \otimes 3w_2) + (-v_2 \otimes w_1) - (-v_2 \otimes 3w_2)$.

If given a basis $\{e_i\}_{i=1}^m$ for V , $\{f_j\}_{j=1}^n$ for W , then we want $\{e_i \otimes f_j\}$ to be a basis for $V \otimes_{\mathbb{F}} W$. However, this is not always possible to realize, although it is possible for vector spaces over \mathbb{F} . In this case, $\dim_{\mathbb{F}}(V \otimes W) = \dim_{\mathbb{F}}(V) \times \dim_{\mathbb{F}}(W)$. Example: $\dim_{\mathbb{R}}(\mathbb{R} \otimes \mathbb{R}^m) = \dim_{\mathbb{R}}(\mathbb{R}) \times \dim(\mathbb{R}^m) = 1 \times m = m$. "lots of elements in $V \otimes W$ ".

Can we make such a space exist? Yes. (Used heavily by physicists: for elasticity, electromagnetic fields, stress/strain).

Definition Given vector spaces U, V, W over \mathbb{F} , a bilinear map $f: V \times W \rightarrow U$ satisfies

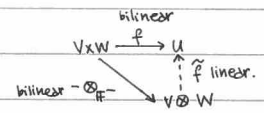
- $f(v_1 + v_2, w) = f(v_1, w) + f(v_2, w)$
- $f(v, w_1 + w_2) = f(v, w_1) + f(v, w_2)$
- $f(\lambda v, w) = f(v, \lambda w) = \lambda f(v, w)$ $\lambda \in \mathbb{F}, v_i \in V, w_j \in W$

Note - f is not linear! since $f(\lambda v, \lambda w) = \lambda f(v, w) = \lambda^2 f(v, w)$.

Examples -

1. The dot product $v \cdot w$
2. The inner product $f = \langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{R}$, $\langle v, w \rangle = v \cdot Aw$, $\forall A \in M_n(\mathbb{R})$. [Note: dot product is just taking $A = I_n$.]
3. Triple product $f: \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $v \times w$.
4. $(\lambda, \mu) \mapsto \lambda \mu$ scalar multiplication on modules is bilinear.
5. $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ multiplication is linear.

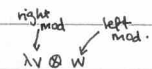
Definition Let V, W be vector spaces over \mathbb{F} . By a tensor product $(V \otimes_{\mathbb{F}} W, - \otimes_{\mathbb{F}} -)$ we mean (i) $V \otimes_{\mathbb{F}} W$ is a vector space, given any bilinear map $f: V \times W \rightarrow U$ \exists a unique linear map $\tilde{f}: V \otimes_{\mathbb{F}} W \rightarrow U$ making the diagram commute [i.e. $\tilde{f} \circ (- \otimes_{\mathbb{F}} -) = f$].



\therefore Every bilinear map f can be factored through $- \otimes -$ (this is called the universal property of \otimes). $\Rightarrow V \otimes W$ turn bilinear maps into linear maps.

Note - 1. To show two spaces are isomorphic using $- \otimes -$, just define linear maps \tilde{f} and show universal property definition works.

2. To calculate, use bilinearity (key rule) $\lambda(v \otimes w) = \lambda v \otimes w = v \otimes \lambda w$, $\lambda \in \mathbb{F}$.



Generalise this to modules over $R =$ commutative rings: $V \otimes_R W$. If rings are non-commutative, we encounter trouble.

Examples of \mathbb{Z} -modules tensored together - Use key rule: $\lambda v \otimes w = v \otimes \lambda w = \lambda(v \otimes w)$.

1. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong 10\mathbb{Z}$ as \mathbb{Z} -modules. Let $\mathbb{Z}/2\mathbb{Z} = \{e, a\}$ s.t. $a+a=2a=e$, $\mathbb{Z}/3\mathbb{Z} = \{e, b, 2b\}$ s.t. $3b=e$. [later let $e=0, a=1, b=1$].

Note that elements of $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ look like $\lambda_1(e \otimes e) + \lambda_2(e \otimes b) + \lambda_3(e \otimes 2b) + \lambda_4(a \otimes e) + \lambda_5(a \otimes b) + \lambda_6(a \otimes 2b)$. So we only have 6 simple tensors to consider $3 \times 3 \mathbb{Z}$, by key rule, shift vectors. cannot be broken.

claim: All these simple tensors collapse to $e \otimes e = 0 \otimes 0 = 0$.
 ① $e \otimes e$ is itself
 ② $e \otimes b = 3e \otimes b = e \otimes 3b = e \otimes e = 0$
 ③ $e \otimes 2b = 3e \otimes 2b = e \otimes 6b = e \otimes e = 0$
 ④ $a \otimes e = a \otimes 2e = 2a \otimes e = e \otimes e = 0$
 ⑤ $a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes e = 0$
 ⑥ $a \otimes 2b = 2a \otimes b = e \otimes b = e \otimes e = 0$. \Rightarrow all 6 products are $e \otimes e$.

$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong \sum 0 \otimes 0 = 10\mathbb{Z}$.

2. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Let $\mathbb{Z}/2\mathbb{Z} = \{e, a\}$, $2a=e$, $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$. claim: we will only obtain 2 elements in tensor space. Our possibilities are as such:
 $e \otimes$ even no. $a \otimes$ even no.
 $e \otimes$ odd no. $a \otimes$ odd no. $\cdot e \otimes$ even = $0 \otimes$ even = $0 \cdot 0 \otimes$ even = $0 \otimes 0$ even = $0 \otimes 0$. $\cdot e \otimes$ odd = $0 \cdot 0 \otimes$ odd = $0 \otimes 0$ odd = $0 \otimes 0$.

$\cdot a \otimes$ even e.g. $a \otimes 2n = 2a \otimes n = e \otimes n = 0 \otimes n = 0 \otimes 0$ from above. $\cdot a \otimes$ odd e.g. $a \otimes 1 = a \otimes 3 = 3a \otimes 1 = a \otimes 3 = a \otimes 1$, cannot simplify. $= 3a \otimes 1 = a \otimes 1$

Thus we get two elements, $\{0 \otimes 0, a \otimes 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

3. $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^2 \cong \mathbb{Z}^4$ [to be seen later].

Formal properties of tensor products, using universal property -

1. $R \otimes V \cong V$
 $\lambda \otimes v \mapsto \lambda v$
2. $V \otimes W \cong W \otimes V$
 $(v \otimes w) \mapsto (w \otimes v)$
3. $U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$
 $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$
4. $U \otimes (V \oplus W) \cong U \otimes V \oplus U \otimes W$
 $u \otimes (v, w) \mapsto (u \otimes v, u \otimes w)$

Refined definition of Tensor Product: Let U, V, W be R -modules. Then a tensor product $(V \otimes W, - \otimes -)$ (i) is an R -module, $V \otimes W$, with a bilinear map $- \otimes -: V \times W \rightarrow V \otimes W$ s.t. (ii) \forall bilinear map $f: V \times W \rightarrow U$, \exists unique linear map $\tilde{f}: V \otimes W \rightarrow U$ making the diagram commute (as above).

Idea: consider the following diagram:
 $V \times W \xrightarrow{\text{bilinear } f} U$
 $\downarrow - \otimes - \quad \uparrow \tilde{f}$
 $V \otimes W \xrightarrow{\tilde{f}} U$
 This is beautiful, as instead of constructing bilinear maps $f: V \times W \rightarrow U$, we can equivalently construct linear maps $\tilde{f}: V \otimes W \rightarrow U$ from our constructed space $V \otimes W$.

last time, we showed that $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} \cong 10\mathbb{Z}$ as \mathbb{Z} -modules. We calculated using spanning sets e.g. $\{e, a\}$, but we did not use universal property.

Question: What does it mean to say $V \otimes W \cong 10\mathbb{Z}$? \Rightarrow every bilinear map out of $V \times W$ is a zero map \Leftrightarrow every linear map out of $V \otimes W$ is a zero map

\Rightarrow every simple tensor $v \otimes w = 0$ is zero in the image of $f(v, w)$. $V \otimes W = \sum \lambda_i (v_i \otimes w_i) = 10\mathbb{Z}$.

We now examine proofs that tensor spaces are isomorphic: from above. 1: $f: \lambda \otimes v \mapsto \lambda v$. Why do we need universal property? Ponger - the map $\sum \lambda_i v_i \mapsto \sum \lambda_i v_i$ is not well-defined.

This is because the symbols $\lambda_i \otimes v_i$ do not form a basis. They are however a generating/spanning set (not li). let $- \otimes -: R \times V \rightarrow R \otimes V$ $(\lambda, v) \mapsto \lambda \otimes v$ be a bilinear map. let the function $f: R \times V \rightarrow V$ $(\lambda, v) \mapsto \lambda v$ be bilinear. let $\tilde{f}: R \otimes V \rightarrow V$ be linear, given by $\lambda \otimes v \mapsto \lambda v$. [check commutativity: $\tilde{f} \circ (- \otimes -) = f$].

To show isomorphism, we need an inverse $\tilde{f}^{-1}: V \rightarrow R \otimes V$, $v \mapsto 1 \otimes v$. Then $\tilde{f} \circ \tilde{f}^{-1}(v) = \tilde{f}(1 \otimes v) = 1 \otimes v = v$. $\tilde{f}^{-1} \circ \tilde{f}(\lambda \otimes v) = \tilde{f}^{-1}(\lambda v) = 1 \otimes \lambda v = \lambda \otimes v = 1 \otimes (\lambda v)$. $\Rightarrow \tilde{f}$ is an isomorphism, q.e.d.

Theorem Let \mathbb{F} be a field, then $M_n(\mathbb{F}) \otimes M_m(\mathbb{F}) \cong M_{nm}(\mathbb{F})$.

Proof - let $f: M_n(\mathbb{F}) \times M_m(\mathbb{F}) \rightarrow M_{nm}(\mathbb{F})$ be the "secret" bilinear map given by $(A, B) \mapsto \begin{pmatrix} a_{11}b & \dots & a_{1m}b \\ \vdots & \ddots & \vdots \\ a_{n1}b & \dots & a_{nm}b \end{pmatrix}$. then take $- \otimes -: M_n(\mathbb{F}) \times M_m(\mathbb{F}) \rightarrow M_n(\mathbb{F}) \otimes M_m(\mathbb{F})$ $(A, B) \mapsto A \otimes B$.

We work around this indirectly. NTS: $\exists \tilde{f}$ linear which is an isomorphism. let U, V be finite dimensional \mathbb{F} -vector spaces. let $S: U \rightarrow U$, $T: V \rightarrow V$ be \mathbb{F} -linear maps (endomorphisms). then, define $S \otimes T: U \otimes V \rightarrow U \otimes V$ $End(U) \otimes End(V) \rightarrow End(U \otimes V)$ $u \otimes v \mapsto S(u) \otimes T(v)$, which is linear. then we have $S \otimes T \mapsto S \otimes T$ which gives the isomorphism: let $\dim(U) = m$, $\dim(V) = n$.

Therefore bases, $End(U) \cong M_n(\mathbb{F})$, $End(V) \cong M_m(\mathbb{F})$, and $End(U \otimes V) \cong M_{nm}(\mathbb{F})$ q.e.d.

Examples - 1. $\mathbb{I}_m \otimes \mathbb{I}_n \cong \mathbb{I}_{mn}$, 2. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \mathbb{I}_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix} \cong M_2(\mathbb{F}) \times M_2(\mathbb{F}) \rightarrow M_{2 \times 2}(\mathbb{F}) = M_4(\mathbb{F})$

Tensor Products of algebras.

Let A, B be algebras over \mathbb{F} . Then $A \otimes_{\mathbb{F}} B$ becomes an \mathbb{F} -algebra by defining $\sum (a \otimes b) \cdot (a' \otimes b') = \sum a a' \otimes b b'$ with unit $1 \otimes 1$.

Example - \mathbb{C} is a \mathbb{C} -algebra, so $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ is a \mathbb{C} -algebra. Likewise, group ring $\mathbb{C}[G]$ is a \mathbb{C} -algebra, so let V, W be $\mathbb{C}[G]$ modules, then $V \otimes_{\mathbb{C}} W$ is an algebra by defining $g(v \otimes w) = gv \otimes gw$.

Further Wedderburn Decomposition.

By Wedderburn and Maschke, we know that $\mathbb{C}[G] \cong \prod_{i=1}^r M_{n_i}(\mathbb{C})$. We want $\mathbb{C}[G \times H] \cong \mathbb{C}[G] \otimes_{\mathbb{C}} \mathbb{C}[H]$, with isomorphism $(g, h) \mapsto g \otimes h$.

Examples -

1. We know that $\mathbb{C}[D_6 \times D_6]$ breaks down... $\mathbb{C}[D_6] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \because 6 = 1^2 + 1^2 + 2^2$. We use the theorem $M_m(\mathbb{F}) \times M_n(\mathbb{F}) \cong M_{mn}(\mathbb{F})$. Think of \mathbb{C} as $M_1(\mathbb{C})$.

then by isomorphism, $\mathbb{C}[D_6 \times D_6] \cong \mathbb{C}[D_6] \otimes_{\mathbb{C}} \mathbb{C}[D_6] \cong (\mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})) \otimes (\mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})) \cong (\mathbb{C} \otimes \mathbb{C}) \times (\mathbb{C} \otimes \mathbb{C}) \times (\mathbb{C} \otimes M_2(\mathbb{C})) \times (\mathbb{C} \otimes M_2(\mathbb{C})) \times (\mathbb{C} \otimes M_2(\mathbb{C})) \times (\mathbb{C} \otimes M_2(\mathbb{C}))$
 $\cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}) \times M_2(\mathbb{C}) \times M_2(\mathbb{C}) \times M_2(\mathbb{C}) \times M_2(\mathbb{C}) \times M_2(\mathbb{C})$

$\Rightarrow D_6 \times D_6$ has 4 distinct 1D representations, 4 distinct 2D representations and 1 irreducible 4D representation.

We verify that both sides have the same \mathbb{C} -dimension: $\mathbb{C}[D_6 \times D_6] \cong \mathbb{C}[D_6] \times \mathbb{C}[D_6] \cong \mathbb{C}^{(4)} \times M_2(\mathbb{C})^{(4)} \times M_4(\mathbb{C}) \Rightarrow 6 \times 6 = 4 + 4(2 \times 2) + 4 \times 4 = 36$.

2. $D_6^* = \langle x, y \mid x^2 = y^4 = 1, yx = xy^3 \rangle \cong C_2 \times C_8$ has 12 elements $\{1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2, y^3, xy^3, x^2y^3\}$. We then seek $\mathbb{C}[D_6^*]$. We need $r = \text{no. of classes} = 6$.

these are $\{1\}, \{x, x^2\}, \{y, xy, x^2y\}, \{y^2\}, \{y^3, xy^3, x^2y^3\}$. Then $|D_6^*| = 12 = n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 + 2^2$.

i.e. $\mathbb{C}[D_6^*] \cong \mathbb{C}^{(4)} \times M_2(\mathbb{C})^{(2)}$, isotypic decomposition. Then $\mathbb{C}[D_6^* \times D_6^*] \cong \mathbb{C}[D_6^*] \otimes_{\mathbb{C}} \mathbb{C}[D_6^*]$, $(g, h) \mapsto g \otimes h \cong (\mathbb{C}^{(4)} \times M_2(\mathbb{C})^{(2)}) \otimes (\mathbb{C}^{(4)} \times M_2(\mathbb{C})^{(2)})$

$\cong \mathbb{C}^{(16)} \times M_2(\mathbb{C})^{(16)} \times M_4(\mathbb{C})^{(4)}$. Again we verify, $12 \times 12 = 144$. $16 + 4 \cdot 16 + 16 \cdot 4 = 16 + 64 + 64 = 144$.

$\therefore D_6^* \times D_6^*$ has 16 distinct 1D representations, 16 distinct simple 2D representations and 4 distinct simple 4-dim reps.

Thus, we always know for any G how many representations $\rho: G \rightarrow GL_n(\mathbb{C})$ there are. Now, we attempt to actually construct these matrices.

Induced representations = constructing $\rho: G \rightarrow GL_n(\mathbb{C})$
 $g \mapsto ?$

Idea: To construct all \mathbb{C} -representations of G , starting from cyclic group representations (since we know these).

Construction: let G be a finite group, $H \leq G$ a subgroup. Let V be a $\mathbb{C}[H]$ -module (G representation of H). Then define the $\mathbb{C}[G]$ -module (targeted representation of G that we want) by $\text{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$, where we will think of V as a $\mathbb{C}[G]$ -module, where G acts trivially, i.e. $g \cdot v = v$.

Then consider submodule $Y = \{ \sum_{g \in G} g \otimes v \mid v \in V \}$ so we get a \mathbb{C} -vector space $\mathbb{C}[G] \otimes_{\mathbb{C}} V / Y \cong \mathbb{C}[G/H] \otimes_{\mathbb{C}} V \cong \text{Ind}_H^G(V)$. Then thinking of elements as scalars.

1. Define the set of left cosets $G/H = \{gH \mid g \in G\}$ where $g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H$.
2. Let $\{g_1, \dots, g_n\}$ be a complete set of coset representatives, $G = \bigcup_{i=1}^n g_iH$.
3. Define the quotient space $\mathbb{C}[G/H]$, which is a \mathbb{C} -vector space with basis $\{g_1, \dots, g_n\}$ = set of coset representatives.
4. Choose a basis for $\mathbb{C}[G/H] \otimes_{\mathbb{C}} V$ and we need to define how g acts on the tensors $g \cdot (g_i \otimes v) = ?$. We use group relations of G and key rule of \otimes . Thinking of elements as in $\mathbb{C}[H]$.

Examples -

1. Let us find a representation of $D_6 = \langle x, y \mid x^2 = y^4 = 1, yx = xy^3 \rangle$. Let $H = C_2 = \{1, x\}$ be the subgroup. V is a $\mathbb{C}[C_2]$ -module, on which x acts as $w = e^{2\pi i/2}$, i.e. $x \cdot v = -v$.
 $\rho: C_2 \rightarrow GL_1(\mathbb{C})$
 $x \mapsto w$. $\because |C_2| = |D_6|/|C_2| = 2 \Rightarrow \text{index } 2 = \text{normal}$. i.e. $D_6 = C_2 \cdot 1 \cup C_2 \cdot y$

3. Define quotient module $\mathbb{C}[D_6/C_2] \cong \mathbb{C}[G]$ with basis $\{1, y\}$. 4. Let $\{1 \otimes 1, y \otimes 1\}$ be a basis for $\mathbb{C}[G] \otimes V$. V is a 1D rep, so $V \cong \mathbb{C}$ as modules. i.e. $\{1\}$ is a basis for V .

Now find x and y actions on the basis: use relations for D_6 . x -action - $x(1 \otimes 1) = x \cdot 1 \otimes 1 = 1 \cdot x \cdot 1 \otimes 1 = 1 \otimes w \cdot 1 = (1 \otimes 1) \cdot w$. Then we have $x(y \otimes 1) = xy \otimes 1 = yx^2 \otimes 1 = y \otimes x^2 \cdot 1 = y \otimes w^2 \cdot 1 = (y \otimes 1) \cdot w^2$. Therefore, $\text{Ind}_{C_2}^{D_6}(V) = \rho: D_6 \rightarrow GL_2(\mathbb{C})$ sends $x \mapsto \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}$. Likewise, we evaluate y -action: $y(1 \otimes 1) = y \otimes 1$, $y(y \otimes 1) = y^2 \otimes 1 = 1 \otimes 1$, so $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
 first element of basis, second element of basis.

Note - we said earlier that in \mathbb{Z} -modules, $\lambda v \otimes w = v \otimes \lambda w$, but this applies only in commutative group rings! i.e. $xy \otimes 1 \neq y \otimes x!$ 22 November 2013, Mr Jamil NADIM, Maths 500.

Using Wedderburn Decomposition theorem, $\mathbb{C}[D_6] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. $6 = 1^2 + 1^2 + 2^2 \Rightarrow r=3$ conjugacy classes. We have just induced a 2D representation of D_6 , but is it irreducible rep $\Leftrightarrow M_2(\mathbb{C})$, or direct sum $\rho = \rho' \oplus \rho''$ of 1dim representations?

To figure this out, use Schur's lemma vs. compute $\text{End}_{\mathbb{C}[G]}(\text{Ind}_{C_2}^{D_6}(V)) = \{A \in GL_2(\mathbb{C}) : A \cdot \rho(g) = \rho(g) \cdot A \forall g \in D_6\}$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, find $A \rho(x) = \rho(x) A$, $A \rho(y) = \rho(y) A$
 $A \rho(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix} = \begin{pmatrix} aw & bw^2 \\ cw & dw^2 \end{pmatrix}$, $\rho(x) A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix} = \begin{pmatrix} aw & bw^2 \\ cw & dw^2 \end{pmatrix}$, $\rho(y) A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$, $A \rho(y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$
 $\Rightarrow a = a, bw^2 - bw = 0 \Rightarrow b = 0$ since $w^2 - w \neq 0$. $\Rightarrow A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Rightarrow \text{End}_{\mathbb{C}[G]}(\text{Ind}_{C_2}^{D_6}(V)) \cong \mathbb{C}$, a division ring \Rightarrow representation is simple \Rightarrow we have that i.e. irreducible.

$\rho: D_6 \rightarrow GL_2(\mathbb{C})$ is simple, where ρ is our constructed induced representation.

Note - We can induce from any subgroup. In particular, if we induce from $\{1\} \leq G$, we get the regular representation of $G: \text{Ind}_{\{1\}}^G(V) = \text{reg}: G \rightarrow GL_{|G|}(\mathbb{C})$. This is always reducible!

2: let $G = D_6 = \langle x, y \mid x^2 = y^2 = 1, yx = xy^2 \rangle$. let $H = G = \langle y \mid y^2 = 1 \rangle \leq D_6$ be a subgroup. However, $C_2 \nmid D_6$ since $gC_2 \neq C_2g \forall g \in D_6$. let V be the 1-dimensional \mathbb{C} -module \mathbb{C} with $y \mapsto -1$. $\rho: C_2 \rightarrow \mathbb{C}$ by $y \mapsto -1$. $|D_6/C_2| = 3 \Rightarrow$ take \mathcal{Q} (cosets) = $\{1, x, x^2\}$ to be coset representatives. Construct $\text{Ind}_{C_2}^{D_6}(\rho) = \mathbb{C}[D_6] \otimes_{\mathbb{C}[C_2]} V \cong \mathbb{C}[Q] \otimes_{\mathbb{C}} V$; which as a basis, we take $\{1 \otimes 1, x \otimes 1, x^2 \otimes 1\}$. then x -action: $x(1 \otimes 1) = x \cdot 1 \otimes 1 = x \otimes 1$. $x(x \otimes 1) = x^2 \otimes 1$. $x(x^2 \otimes 1) = x^3 \otimes 1 = 1 \otimes 1 \Rightarrow x \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, y acts trivially on right factor. y -action: $y(1 \otimes 1) = y \cdot 1 \otimes 1 = 1 \cdot y \otimes 1 = 1 \otimes y \cdot 1 = 1 \otimes (-1) = -1 \otimes 1$. $y(x \otimes 1) = yx \otimes 1 = xy^2 \otimes 1 = x^2 \otimes y \cdot 1 = x^2 \otimes (-1) = -x^2 \otimes 1$. $y(x^2 \otimes 1) = yx^2 \otimes 1 = xy \otimes 1 = x \otimes y \cdot 1 = x \otimes (-1) = -x \otimes 1$. then $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This representation $\rho: D_6 \rightarrow GL_3(\mathbb{C})$ is reducible for two reasons: ① $\mathbb{C}[D_6] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$, ② $\text{End}_{\mathbb{C}[D_6]}(\rho) = \left\{ \begin{pmatrix} a & b & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \right\} \cong \mathbb{C}^2$ not division ring \Rightarrow not simple representation.

3: let $G = Q_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, xy = yx^3 \rangle$. Take $H = C_4 = \langle x \mid x^4 = 1 \rangle \triangleleft Q_8$ (\because every subgroup of Q_8 is normal). let V be the $\mathbb{C}[G]$ -module where x acts as i : $\rho: C_4 \rightarrow \mathbb{C}$ $x \mapsto i$. $\therefore V \cong \mathbb{C} \Rightarrow$ basis $\{1\}$ for V . $|Q_8/C_4| = \frac{8}{4} = 2$, so take $\mathcal{Q} = \{1, y\}$ to be coset reps. Construct $\mathbb{C}[Q_8]$ -module, $\text{Ind}_{C_4}^{Q_8}(V) = \mathbb{C}[Q_8] \otimes_{\mathbb{C}[C_4]} V \cong \mathbb{C}[Q] \otimes_{\mathbb{C}} V$. This has basis $\{1 \otimes 1, y \otimes 1\}$. x -action: $x(1 \otimes 1) = x \cdot 1 \otimes 1 = 1 \cdot x \otimes 1 = 1 \otimes x \cdot 1 = 1 \otimes i = (1 \otimes i) \cdot 1$. $x(y \otimes 1) = xy \otimes 1 = yx^3 \otimes 1 = y \otimes x^3 \cdot 1 = y \otimes (-i) = (y \otimes 1) \cdot (-i)$. $x \sim \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. y -action: $y(1 \otimes 1) = y \otimes 1$, $y(y \otimes 1) = y^2 \otimes 1 = x^2 \otimes 1 = 1 \cdot x^2 \otimes 1 = 1 \otimes x^2 \cdot 1 = 1 \otimes (-1) = (1 \otimes 1) \cdot (-1)$, so $y \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. check: $\text{End}_{\mathbb{C}[Q_8]}(\rho)$. Recall $r=5$ for $\mathbb{C}[Q_8]$, and we have just constructed a $M_2(\mathbb{C})$ -representation. Is it the simple one, or the direct sum of 2 1D-reps? Find $A \in GL_2(\mathbb{C})$ st. $A\rho(x) = \rho(x)A$, $A\rho(y) = \rho(y)A$: let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $A\rho(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} ai & -bi \\ ci & -di \end{pmatrix}$, $\rho(x)A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ai & bi \\ -ci & -di \end{pmatrix} \Rightarrow b=0, c=0$. then $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. $A\rho(y) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix}$, $\rho(y)A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & d \\ a & 0 \end{pmatrix} \Rightarrow a=d$, so $\text{End}_{\mathbb{C}[Q_8]}(\rho) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \right\} \cong \mathbb{C}$, division ring $\Rightarrow \rho$ is a (the) simple representation. And we can write a full list of all representations of Q_8 . $\mathbb{C}[Q_8] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Note - In \otimes key rule, we said $\lambda(x \otimes y) = \lambda x \otimes y = x \otimes \lambda y$ $\lambda \in \mathbb{R}$. However, $\mathbb{N} \otimes \mathbb{N}$ were both left modules. However, in the induced reps "definition": $\text{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$. 25 November 2013.
Mr. Ismail NADIM.
Garden St (25) D103.

Theorem let V be a $\mathbb{C}[H]$ -module, and let $|G/H| = n$ so that $\{g_1, \dots, g_n\}$ is a complete set of coset representatives for coset list g_1H, \dots, g_nH . then $\text{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \cong \bigoplus_{i=1}^n g_i \otimes V$ as \mathbb{C} -modules, where $g_i \otimes V = \{g_i \otimes v \mid v \in V\} \subseteq \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$, and each $g_i \otimes V \cong V$ as \mathbb{C} -modules. Moreover, if V is free (i.e. has a basis), then $\dim \text{Ind}_H^G(V) = |G/H| \times \dim_{\mathbb{C}}(V)$. If $x \in G$, then $x(g_i \otimes V) = g_j \otimes V$ where $xg_i = g_jh$ for some $h \in H$. \therefore the submodules $g_i \otimes V$ are permuted by the action of G . Proof - $\mathbb{C}[H] \otimes_{\mathbb{C}[H]} \mathbb{C}[G] \cong \mathbb{C}[G]$, and H has a permutation action on the basis of $\mathbb{C}[G]$ with n orbits g_1H, \dots, g_nH . Each orbit spans a left $\mathbb{C}[H]$ -module $\mathbb{C}[g_iH]$ of $\mathbb{C}[G]$. $\therefore \text{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V = \bigoplus_{i=1}^n g_i \otimes_{\mathbb{C}[H]} V = \bigoplus_{i=1}^n (\mathbb{C}[g_iH] \otimes_{\mathbb{C}[H]} V) = \bigoplus_{i=1}^n g_i \otimes_{\mathbb{C}[H]} V$ and as \mathbb{C} -modules, $g_i \otimes_{\mathbb{C}[H]} V \cong \mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \cong V$. Next, g -action permutes the basis. let $x \in G$ st. $xg_i = g_jh$ for some $h \in H$. then $x(g_i \otimes V) = xg_i \otimes V = g_jh \otimes V = g_j \otimes hV \in g_j \otimes V$ and equality follows from $x^{-1}: x^{-1}g_j \otimes V = g_i \otimes V$ q.e.d.

CHARACTER THEORY.

Thus far, the theory is sound for \mathbb{C} -reps, but consider the following Wedderburn decomposition: $\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \cong \mathbb{C}[C_3]$, but $S_3 \not\cong C_3$. so we need some kind of invariant to distinguish between group rings. We use character tables (denoted χ -tables).

Theorem if 2 γ -tables are isomorphic, then $\mathbb{C}[G] \cong \mathbb{C}[H]$, but $\mathbb{C}[G] \cong \mathbb{C}[H] \nRightarrow \chi$ -tables are the same. Remark - (beyond scope of course) if $\mathbb{Z}[G] \cong \mathbb{Z}[H]$ then $G \cong H$.

Definition let $A = (a_{ij})$ be an $n \times n$ matrix over F , then the trace of A , $\text{Tr}(A) = \sum_{i=1}^n a_{ii}$. Recall - Property: $\text{Tr}(A) = \text{Tr}(A^T)$.

Proposition let $A, B \in M_n(F)$. then $\text{Tr}(AB) = \text{Tr}(BA)$. [Although $AB \neq BA$ in general]. Proof $(AB)_{ii} = \sum_{j=1}^n a_{ij}b_{ji}$, so $\text{Tr}(AB) = \sum_{i=1}^n \sum_{j=1}^n a_{ij}b_{ji} = \sum_{j=1}^n \sum_{i=1}^n b_{ji}a_{ij} = \sum_{j=1}^n (BA)_{jj} = \text{Tr}(BA)$, q.e.d.

Corollary If A, B are conjugate, then $\text{Tr}(A) = \text{Tr}(B)$. Proof - suppose $\exists T \in GL_n(F)$ st. $B = TAT^{-1}$, then $\text{Tr}(B) = \text{Tr}(TAT^{-1}) = \text{Tr}(AT^{-1}T) = \text{Tr}(A)$, q.e.d.

Definition let G be a finite group, $F = \mathbb{C}$. let V be a finite-dimensional $\mathbb{C}[G]$ -module corresponding to $\rho: G \rightarrow GL_n(\mathbb{C})$. Then the character afforded by ρ is the mapping $\chi_\rho: G \rightarrow \mathbb{C}$ defined by $\chi_\rho(g) = \text{Tr}(\rho(g))$, $\forall g \in G$. Every rep ρ has a character χ_ρ .

Examples - 1. let $G = C_3 = \langle x \mid x^3 = 1 \rangle$. G has 3 conjugacy classes $\langle 1 \rangle, \langle x \rangle, \langle x^2 \rangle$. $\therefore r=3$, $\mathbb{C}[C_3] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C}$. $\rho_1: C_3 \rightarrow \mathbb{C}$ $x \mapsto 1$, $\rho_2: C_3 \rightarrow \mathbb{C}$ $x \mapsto \omega$, $\rho_3: C_3 \rightarrow \mathbb{C}$ $x \mapsto \omega^2$.

$\langle 1 \rangle$	$\langle x \rangle$	$\langle x^2 \rangle$
χ_1	1	1
χ_2	1	ω
χ_3	1	ω^2

 Then we get the following χ -tables as shown on right - Note: $\chi_{\text{reg}} = \chi_1 + \chi_2 + \chi_3 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ is still a function.

Definition if ρ is irreducible, then $\chi_\rho: G \rightarrow \mathbb{C}$ is called an irreducible character. If ρ is a 1-dim rep $\rho: G \rightarrow GL_1(\mathbb{C})$, then $\chi_\rho: G \rightarrow \mathbb{C}$ is called a linear character.

The degree of a representation $\rho: G \rightarrow GL_n(\mathbb{C})$ is also the degree of the character $\chi_\rho: G \rightarrow \mathbb{C}$, $\deg(\chi_\rho) = [V: \mathbb{C}] = n$. To find degree of χ_ρ , compute $\text{Tr}(\rho(1))$.
 Note that χ_ρ is not a homomorphism in general, $\chi_\rho(g) \neq \chi_\rho(g)\chi_\rho(h)$. It is a homomorphism if $\rho: G \rightarrow GL_1(\mathbb{C}) = \mathbb{C}$ is a 1-dim rep.
 since $\chi_\rho(g) = \text{Tr}(\rho(g)) = \text{Tr}(\rho(g)\rho(h)) = \text{Tr}(\rho(g))\text{Tr}(\rho(h)) = \chi_\rho(g)\chi_\rho(h)$.
 $G \rightarrow GL_n(\mathbb{C}) \rightarrow GL_n(\mathbb{C})$
 Recall the definition: two representations ρ and σ were equivalent/conjugate if $\exists T \in GL_n(\mathbb{C})$ s.t. $\sigma(g) = T^{-1}\rho(g)T \forall g \in G$ i.e. \exists a change of basis matrix for $V = \mathbb{C}^n$.

Proposition If ρ and σ are equivalent, then $\chi_\rho = \chi_\sigma$.
 Proof - let $\sigma(g) = T^{-1}\rho(g)T \forall g \in G$. So $\chi_\sigma(g) = \text{Tr}(\sigma(g)) = \text{Tr}(T^{-1}\rho(g)T) = \text{Tr}(\rho(g)T \cdot T^{-1}) = \text{Tr}(\rho(g)) = \chi_\rho(g)$, q.e.d.
 Thus, characters are also independent of changes in basis. \Rightarrow Practical point: If $\chi_\rho \neq \chi_\sigma$, then ρ and σ are not equivalent.

Proposition Characters are constant on conjugacy classes. (i.e. χ_ρ is constant on $(g)^G = \{xgx^{-1} : x \in G\}$).
 Proof - suppose $g = xhx^{-1}$ for some $x \in G$. then $g \in (h)^G$. then $\rho(g) = \rho(xhx^{-1}) = \rho(x)\rho(h)\rho(x^{-1})$. then $\chi_\rho(g) = \text{Tr}(\rho(g)) = \text{Tr}(\rho(x)\rho(h)\rho(x^{-1})) = \text{Tr}(\rho(h)\rho(x)\rho(x^{-1})) = \text{Tr}(\rho(h)) = \chi_\rho(h)$. [Hint: We don't need to find the matrices for all elements in a conjugacy class and then trace them to find χ_ρ .]
 Example -

1. $D_6 = \langle x, y \mid x^2 = y^2 = 1, yx = x^2y \rangle = \langle 1 \rangle \cup \langle x, x^2 \rangle \cup \langle y, xy, x^2y \rangle$ as conjugacy classes. $[D_6] = \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Try a 2-dim rep.
 let $\rho: D_6 \rightarrow GL_2(\mathbb{C})$, $x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $\chi_\rho(1) = \text{Tr}(\rho(1)) = \text{Tr} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2 \Rightarrow$ degree of character is 2. check $\chi_\rho(x) = \chi_\rho(x^2)$
 $\chi_\rho(x) = \text{Tr}(\rho(x)) = \text{Tr} \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} = \omega + \omega^2$, $\chi_\rho(x^2) = \text{Tr}(\rho(x^2)) = \text{Tr} \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} = \omega^2 + \omega = \omega + \omega^2$. (indeed these are the same, and $= -1$).
 likewise, $\langle y, xy, x^2y \rangle$ will share a value of χ . $\chi_\rho(y) = \text{Tr}(\rho(y)) = \text{Tr} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 0$, $\chi_\rho(xy) = \text{Tr}(\rho(xy)) = \text{Tr} \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} = \omega + \omega^2 = -1$ etc.

Theorem let G be finite of order m , $|G| = m$. let $\rho: G \rightarrow GL_n(\mathbb{C})$ be a rep of $G \iff V$ be a finite dimensional $[G]$ -module. let $\chi_\rho: G \rightarrow \mathbb{C}$ be the character afforded by ρ .
 then $\forall g \in G$, we have:

- (1) $\rho(g)$ is diagonalisable,
 - (2) $\chi_\rho(g)$ is a sum of roots of unity,
 - (3) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$. (conjugated)
 - (4) $|\chi_\rho(g)| \leq n$.
- Example - $\sigma: D_6 \rightarrow GL_2(\mathbb{C})$, $D_6 = 6$. $x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ not diagonal. then (1): \exists new basis and $T \in GL_n(\mathbb{C})$ s.t. $x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$ is diagonal. likewise we can modify y .
 It is clear that $\chi_\rho(x) = \omega + \omega^2$ is a sum of roots of unity. (2) $\chi_\rho(x^2) = \overline{\chi_\rho(x)} = \omega^2 + \omega = \omega + \omega^2$. (4): $|\chi_\rho(x)| = |\omega + \omega^2| \leq |\omega| + |\omega^2| = 1 + 1 = 2$.
 Since $|D_6| = 6$, $\forall g, g^6 = 1 \Rightarrow g^6 - 1 = 0$. Look at minimal polynomial for matrix $\rho(g)$, since $\rho(g)^6 - I = 0 \Rightarrow x^6 - 1 = 0 \Rightarrow (x^3 - 1)(x^3 + 1) = 0$
 \therefore either $x^3 - 1 = 0$ or $x^3 + 1 = 0 \Rightarrow x = 1, \omega, \omega^2$

Proof - Since $|G| = m$, $\forall g \in G$, $g^m = 1 \therefore$ minimal polynomial div $x^m - 1 = 0 \iff \rho(g)^m - I_n = 0$. \therefore diagonalisable over $\mathbb{C} \iff \exists$ a basis for $V = \mathbb{C}^n$ and minimal polynomial is a product of roots of unity. $\chi_\rho(g) = \text{Tr} \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix} = \omega_1 + \dots + \omega_n$. then $\chi_\rho(g^{-1}) = \text{Tr} \begin{pmatrix} \overline{\omega_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\omega_n} \end{pmatrix} = \overline{\omega_1 + \dots + \omega_n} = \overline{\chi_\rho(g)}$. then (4):
 $|\chi_\rho(g)| = |\omega_1 + \dots + \omega_n| \leq |\omega_1| + \dots + |\omega_n| = 1 + \dots + 1 = n$, q.e.d.

29 November 2013
Mr Jamil NADIM
Maths 500

If g and g^{-1} are in the same conjugacy class, then $\chi_\rho(g) \in \mathbb{R}$. Reason: if $g^{-1} \in (g)^G$, then $g = xg^{-1}x^{-1}$ for some $x \in G$. $\therefore \chi_\rho(g) = \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)} \Rightarrow \chi_\rho(g) \in \mathbb{R}$. Example: We cannot try cyclic groups as each element is its own conjugacy class: $G = \langle 1 \rangle \cup \langle x \rangle \cup \langle x^2 \rangle$. We try $D_6 = \langle x, y \mid x^2 = y^2 = 1, yx = x^2y \rangle$.
 let $\rho: D_6 \rightarrow GL_2(\mathbb{C})$, $x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $\chi_\rho(x) = \omega + \omega^2 = \cos(\frac{2\pi}{3}) \in \mathbb{R}$, $\chi_\rho(x) = \chi_\rho(x^2)$. Another example - take $G = S_n$. then permutations in same conjugacy class have same shape i.e. inverses $\in (g)^G$. $\chi_\rho(g) \in \mathbb{R} \forall g \in S_n$. Beware that this does not hold for A_n .

Proposition let $\rho: G \rightarrow GL_n(\mathbb{C})$, $\chi_\rho: G \rightarrow \mathbb{C}$ its character. $|G| = m$. then if $\forall g, |\chi_\rho(g)| = \chi_\rho(1) = \text{Tr}(I_n) = n \iff \rho(g) = \omega I_n$ for some root of unity.
 Proof - suppose $\rho(g) = \omega I_n$ for some root ω of $g^m - 1 = 0$. $\chi_\rho(g) = \text{Tr}(\rho(g)) = \text{Tr} \begin{pmatrix} \omega & & 0 \\ & \ddots & \\ 0 & & \omega \end{pmatrix} = n\omega$. Now $|\chi_\rho(g)| = |n\omega| = |n||\omega| = n = \chi_\rho(1)$, $|\omega| = 1$.
 \Rightarrow suppose $|\chi_\rho(g)| = \chi_\rho(1) = n$. Then w.r.t. some basis, $\rho(g) = \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_s \end{pmatrix}$ for some roots of unity. $\chi_\rho(g) = \text{Tr} \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_s \end{pmatrix} = \omega_1 + \dots + \omega_s$.
 $n = |\chi_\rho(g)| = |\omega_1 + \dots + \omega_s| \leq |\omega_1| + \dots + |\omega_s|$ with equality if all roots lie on a straight line $\Rightarrow \omega_1 = \dots = \omega_s = \omega$ for some $\omega \Rightarrow \rho(g) = \begin{pmatrix} \omega & & 0 \\ & \ddots & \\ 0 & & \omega \end{pmatrix}$, q.e.d.

Definition let $\rho: G \rightarrow GL_n(\mathbb{C})$. let $\chi_\rho: G \rightarrow \mathbb{C}$ be character. then the kernel of the character is the set $\text{Ker}(\chi_\rho) = \{g \in G : \chi_\rho(g) = \chi_\rho(1) = n\}$.

Proposition $\text{Ker}(\chi_\rho) = \text{Ker}(\rho)$, where $\text{Ker}(\rho) = \{g \in G : \rho(g) = I_n\}$.

Proof - $\text{Ker}(\rho) \subseteq \text{Ker}(\chi_\rho)$. let $g \in \text{Ker}(\rho) \Rightarrow \chi_\rho(g) = \chi_\rho(1) = n$. By previous propn, $|\chi_\rho(g)| = \chi_\rho(1) = n \Rightarrow \rho(g) = \begin{pmatrix} \omega & & 0 \\ & \ddots & \\ 0 & & \omega \end{pmatrix} = \omega I_n$. $\therefore g \in \text{Ker}(\rho)$, q.e.d.

Definition If $\text{Ker}(\chi_\rho) = \{1\}$, then χ_ρ is called a faithful character. (analogous - "injective").

Examples -
 $\rho_1: x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $\rho_2: x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $\rho_3: x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $\rho_4: x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$
 1. $D_6 = \langle x, y \mid x^2 = y^2 = 1, yx = x^2y \rangle = \langle 1 \rangle \cup \langle x, x^2 \rangle \cup \langle y, xy, x^2y \rangle$. $[D_6] = \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$
 $\text{Ker}(\chi_1) = D_6$, $\text{Ker}(\chi_2) = \langle x \mid x^2 = 1 \rangle = C_2$, $\text{Ker}(\chi_3) = \langle y \mid y^2 = 1 \rangle = C_2$, $\text{Ker}(\chi_4) = \langle 1 \rangle$. [sum of dimensions x characters] clearly then, χ_{reg} is faithful.
 Now define another 2-dim rep of D_6 :
 $\sigma: D_6 \rightarrow GL_2(\mathbb{C})$, $x \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $\chi_\sigma(1) = 2$, $\chi_\sigma(x) = \chi_\sigma(x^2) = -1$, $\chi_\sigma(y) = \chi_\sigma(xy) = \chi_\sigma(x^2y) = 0 \Rightarrow \chi_\sigma = \chi_3$ equivalent

⇒ we can find $T \in GL_2(\mathbb{C})$ s.t. $\sigma(g) = T \rho_3(g) T^{-1}$.

The regular character

Recall the regular representation $\rho_{reg}: G \rightarrow GL(\mathbb{C}[G]) = GL(|G|, \mathbb{C})$ given by $g \mapsto P_g$ matrix. We obtained P_g by treating $\mathbb{C}[G]$ as a \mathbb{C} -vector space with basis $\{1=g_1, \dots, g_n\}$ and g acts on \mathbb{C}^n like $g \cdot g_i = g_j$, then write matrix P_g w.r.t. basis. $P_{g_i} = \begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{pmatrix} \forall g_i \neq 1, P_{g_1} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$. All elements of G except for $1=g_1$ go to permutation matrices, with zeroes on diagonal since if $g \cdot g_i = g_i \Rightarrow g=1 \Rightarrow g_j=1$. $\therefore \chi_{reg}$ is faithful and decomposable. $\Rightarrow \chi_{reg}(g) = \begin{cases} |G| & g=1 \\ 0 & g \neq 1 \end{cases}$. Also, $\mathbb{C}[G]$ as a $\mathbb{C}[G]$ -module gives $\mathbb{C}[G] = S_1^{n_1} \oplus \dots \oplus S_r^{n_r}$.

Example - $\rho_{reg}: D_6 \rightarrow GL_6(\mathbb{C})$
 $\rho_{reg}(1) \mapsto I_6, \rho_{reg}(x) = ?$ $\mathbb{C}[D_6] = \text{span}\{1, x, x^2, y, xy, x^2y\}$. $xg_1 = x \cdot 1 = x = g_2, xg_2 = x \cdot x = x^2 = g_3, xg_3 = x \cdot x^2 = 1 = g_1, xg_4 = xy = g_5, xg_5 = g_6, xg_6 = x^2y = g_4$. Then $\rho(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \rho_{reg}(x)$. Then $\chi_{reg}(x) = \text{Tr}(\rho_{reg}(x)) = 0$.

2 December 2013
Mr Samir NADIM
Gordon St (25) D183.

We use χ to avoid computing $\text{End}_{\mathbb{C}[D_6]}(\rho)$. Exercise: find $\rho_{reg}(x^2), \rho_{reg}(y)$ in above example.

Proposition Recall that $\mathbb{C}[G] \cong \bigoplus_{i=1}^r M_{n_i}(\mathbb{C}) \cong S_1^{n_1} \oplus \dots \oplus S_r^{n_r}$ where S_i are pairwise nonisomorphic $\mathbb{C}[G]$ -simple modules corresponding to representations $\rho_1, \dots, \rho_r: G \rightarrow GL_{n_i}(\mathbb{C})$. $\dim_{\mathbb{C}}(S_i) = n_i$. \therefore Each $M_{n_i}(\mathbb{C}) \cong S_i^{n_i}$ as $\mathbb{C}[G]$ -modules. so the regular $\mathbb{C}[G]$ -module $\mathbb{C}[G] \xrightarrow{\cong} \bigoplus_{i=1}^r n_i \rho_i$.

Take trace, we can rewrite $\chi_{reg} = \sum_{i=1}^r n_i \chi_i$, and applied to a group element g , then $\chi_{reg}(g) = n_1 \chi_1(g) + \dots + n_r \chi_r(g)$.

Example - Take $G = D_6$. Then $\mathbb{C}[D_6] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Then we get the following table:

	χ_1	χ_2	χ_3	χ_4
conjugacy classes	1	1	1	1
dim	1	1	1	1
applied to g	1	-1	0	0
	2	-1	0	0
	6	0	0	0

$\chi_{reg}(1) = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 = 6, \chi_{reg}(x) = 1 \cdot 1 + 1 \cdot (-1) + 2 \cdot 0 = 0, \chi_{reg}(y) = 1 \cdot 1 + 1 \cdot (-1) + 2 \cdot 0 = 0$.

Proposition Two irreducible representations of G are equivalent \Leftrightarrow their characters are equal.

Proof - (\Rightarrow) Suppose $\rho, \sigma: G \rightarrow GL_n(\mathbb{C})$ are equivalent, $\exists T \in GL_n(\mathbb{C})$ s.t. $\sigma(g) = T \rho(g) T^{-1} \forall g$. $\therefore \chi_{\sigma}(g) = \text{Tr}(\sigma(g)) = \text{Tr}(T \rho(g) T^{-1}) = \text{Tr}(\rho(g) T^{-1} T) = \text{Tr}(\rho(g)) = \chi_{\rho}(g)$ q.e.d.

(\Leftarrow) MP: if $\chi_u = \chi_v$, then $U \cong V$ as $\mathbb{C}[G]$ -modules. let $U = S_1^{a_1} \oplus \dots \oplus S_r^{a_r}$ and $V = S_1^{b_1} \oplus \dots \oplus S_r^{b_r}$ be two semisimple $\mathbb{C}[G]$ -modules. Take trace of corresponding representation: $\chi_u = a_1 \chi_1 + \dots + a_r \chi_r, \chi_v = b_1 \chi_1 + \dots + b_r \chi_r$. since χ_i are unique irreducible characters, $\chi_u = \chi_v \Rightarrow a_i = b_i \forall i \Rightarrow U \cong V$ as $\mathbb{C}[G]$ -modules, q.e.d.

Tool - the inner product of χ_i is used to detect when representations are equivalent / not equivalent.

Example - Take $Q_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$, with representations $\rho_1: Q_8 \rightarrow GL_2(\mathbb{C}), \rho_2: Q_8 \rightarrow GL_2(\mathbb{C}), \rho_3: Q_8 \rightarrow GL_2(\mathbb{C})$
 $x \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad x \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad x \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

We know that $\mathbb{C}[Q_8] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$ with conjugacy classes $\langle 1, x^2, x^4, x^2y, xy, x^2y^3, xy^3, xy^5 \rangle$. We plot our character table:

	$\langle 1 \rangle$	$\langle x^2 \rangle$	$\langle x^4 \rangle$	$\langle xy \rangle$	$\langle xy^3 \rangle$
χ_1	2	-2	0	0	0
χ_2	2	-2	0	0	0
χ_3	2	2	0	0	-2

$\rho_1(x^2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \rho_2(x^2) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \dots$ etc. then from character table, $\chi_1 = \chi_2 \Rightarrow \rho_1 \cong \rho_2$, hence $\exists T$ s.t. $\rho_2 = T \rho_1 T^{-1}$ (equivalent representation). However, $\chi_1 \neq \chi_3 \Rightarrow \rho_1 \not\cong \rho_3$, so ρ_3 is different. We can compute $\text{End}_{\mathbb{C}[Q_8]}(\rho_3) \cong \mathbb{C}$ irreducible.

However ρ_3 is reducible (semisimple as a $\mathbb{C}[G]$ -module) - let $B = \{e_1, e_2\}$ be a basis for \mathbb{C} . $\rho_3(x) \cdot e_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} i \\ 0 \end{pmatrix} = i \cdot e_1$. this is stable by ρ_3 . Then $\rho_3(y) \cdot e_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1$. this is stable too, so $\rho_3 \cong \rho^1 \oplus \rho^2$ where $\rho^1: Q_8 \rightarrow \mathbb{C}, \rho^2: Q_8 \rightarrow \mathbb{C}$
 $x \mapsto i, y \mapsto 1$ and $x \mapsto -i, y \mapsto -1$. this gives our representation.

Nilpotency and Idempotency

Definition An element $a \in R$ is called nilpotent if $\exists n \in \mathbb{N}$ s.t. $a^n = 0$.

Proposition If R is an integral domain (i.e. $ab=0 \Rightarrow a=0$ or $b=0$), then the only nilpotent element is trivial (which is 0).

Proof - Suppose a nilpotent, then $a^n = 0 \Rightarrow a(a^{n-1}) = 0$. if $a \neq 0$, then $a^{n-1} \neq 0 \Rightarrow a$ is a zero divisor \Rightarrow contradicts integral domain, q.e.d.

Example - 1. Any \mathbb{F}_p is an integral domain: $\mathbb{F}_3 = \{0, 1, 2\}$. 0 is only nilpotent. However 2. \mathbb{Z}_9 is not an integral domain because $3 \cdot 3 = 9 = 0$. But 3 is nilpotent: $3^2 = 0$.
 3. if $R = M_2(\mathbb{F})$, $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent: $a^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. since $a^2 = 0$ but $a \neq 0$, $M_2(\mathbb{F})$ is not an integral domain.

We want to find another decomposition of $\mathbb{C}[G] \cong \bigoplus_{i=1}^r \mathbb{C}[G] e_i$.

Definition An element $e \in R$ is called idempotent if $e^2 = e$.

Examples -

- let $R = \mathbb{Z}_6$, then $3^2 = 9 = 3$, so 3 is idempotent.
- if $R = M_2(\mathbb{F})$, then $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are idempotent.

Proposition If R is an integral domain, then the only idempotent elements are trivial.

Proof - let $e^2 = e$ be idempotent, $e^2 - e = 0, e(e-1) = 0 \Rightarrow e-1 = 0 \Rightarrow e=1$, q.e.d.

Convention: We do not consider 0 to be idempotent, although $0^2 = 0$.

Definition The centre of ring R is $Z(R) = \{z \in R \mid rz = zr \forall r \in R\}$.

Definition An element $e \in R$ is called a central idempotent if $e^2 = e$ and $ee \in Z(R)$.

Definition A set of idempotents $\{e_1, \dots, e_r\}$ are called orthogonal where $\forall i \neq j, e_i e_j = 0$.

The point is, we want to write the unit generator $1 \in R$ as a sum of idempotents.

Example - let $R = R_1 \times R_2 \times R_3$ be a product of 3 subrings. Then we can decompose $1 = (1,1,1)$ into a sum of orthogonal idempotents: $1 = (1,0,0) + (0,1,0) + (0,0,1) = e_1 + e_2 + e_3$

Theorem A ring R can be written as a product of subrings $R = R_1 \times \dots \times R_r \iff 1 \in R$ is a sum of orthogonal central idempotents. In this case, each $R_i \cong Re_i = \{ \sum e_i r_i \in R \}$.

Theorem A ring R is semisimple \iff every left ideal $I \triangleleft R$ is of the form $I = Re_i$ where e_i is an idempotent element. [$1 = \sum e_i \implies e_i = 1 - \sum_{j \neq i} e_j \dots$]

Proof - omitted, not relevant.

Apply to $\mathbb{C}[G]$: We know that $\mathbb{C}[G] \cong \bigoplus_{i=1}^r M_{n_i}(\mathbb{C}) \cong \bigoplus_{i=1}^r \mathbb{C}[G] e_i$ with $(0, \dots, 0, 1, 0, \dots, 0) \mapsto e_i$ where $\{e_1, \dots, e_r\}$ are a set of orthogonal idempotents.

Key point - let $\rho_1, \dots, \rho_r: \mathbb{C}[G] \rightarrow GL_{n_i}(\mathbb{C})$ be the representations of the group ring (irreducible). $\rho_i(\sum a_g g) = \sum a_g \rho_i(g) \forall g \in G$. Then $\rho_i(e_i) = I_{n_i}$ and $\rho_i(e_j) = 0$ if $i \neq j$.

$\implies \chi_i(e_i) = \text{Tr}(\rho_i(e_i)) = \text{Tr}(I_{n_i}) = \text{Tr}(\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}) = n_i = \text{deg}(\rho_i)$. $\chi_i(e_j) = \text{Tr}(0) = 0$.

(Idempotent Formula)

Theorem Let G be finite, $|G| \neq 0$ in \mathbb{F} . Let $\rho_1, \dots, \rho_r: G \rightarrow GL_{n_i}(\mathbb{C})$ be a set of irreducible unique representations of G with corresponding irreducible characters χ_1, \dots, χ_r where

$\chi_i(g) = \text{Tr}(\rho_i(g))$. Then $\{e_1, \dots, e_r\}$ is a set of central orthogonal idempotents $e_i^2 = e_i$ given by the formula $e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g$ where each e_i is associated with a

factor of $\mathbb{C}[G]$ s.t. $\mathbb{C}[G] = \bigoplus_{i=1}^r \mathbb{C}[G] e_i$.

Proof - let $e_i \in \mathbb{C}[G]$, $\therefore e_i = \sum_{g \in G} a_g g \in \mathbb{C}[G]$, $e_i h^i = \sum_{g \in G} a_g g h^i$. Apply both definitions of χ to $e_i h^i$. First, recall $\chi_{\text{reg}}(g) = 1$ if $g=1$ and 0 if $g \neq 1$. Then we get

$$\chi_{\text{reg}}(e_i h^i) = \text{Tr}[\rho_i(e_i h^i)] = \text{Tr}[\rho_i(\sum_{g \in G} a_g g h^i)] = \text{Tr}[\rho_i(a_n h h^i + 0)] = \text{Tr}[\rho_i(a_n h h^i)] = a_n |G|$$

where χ_j are irreducible characters. $\chi_{\text{reg}}(e_i h^i) = \sum_{j=1}^r n_j \chi_j(e_i h^i)$. Recall key point: $\chi_j(e_i) = 0$ if $i \neq j$, $\chi_j(e_j) = \text{Tr}(\rho_j(I_{n_j})) = n_j \implies$ we get that

$$\chi_{\text{reg}}(e_i h^i) = n_i \chi_i(h^i) + 0 \implies a_n |G| = n_i \chi_i(h^i) \implies a_n = \frac{n_i}{|G|} \chi_i(h^i) \implies$$

Example - D_6 , we use the character table from before with same ρ_1, ρ_2, ρ_3 . We can find $\mathbb{C}[D_6] \cong \mathbb{C}[G] (e_1 \oplus e_2 \oplus e_3)$ with $e_i^2 = e_i$, $e_i e_j = 0$

$$\forall i \neq j, \text{ then } 1 \mapsto e_1 + e_2 + e_3. \quad e_1 = \frac{n_1}{|G|} \sum_{g \in D_6} \chi_1(g^{-1}) g = \frac{1}{6} [\chi_1(1^{-1}) 1 + \chi_1(x^{-1}) x + \chi_1(x^2) x^2 + \chi_1(y^{-1}) y + \chi_1(xy) xy + \chi_1(xy^2) xy^2]$$

$$\implies e_1 = \frac{1}{6} [\chi_1(1) 1 + \chi_1(x) x + \chi_1(x^2) x^2 + \chi_1(y) y + \chi_1(xy) xy + \chi_1(xy^2) xy^2] = \frac{1}{6} (1 + x + x^2 + y + xy + xy^2)$$

Check $e_1^2 = e_1$:

$$\text{Repeat for } e_2, e_3. \text{ We get } e_2 = \frac{1}{6} (1 + x + x^2 - y - xy - xy^2), \quad e_3 = \frac{2}{6} (2 - x - x^2) = \frac{1}{3} (2 - x - x^2)$$

Then $1 = e_1 + e_2 + e_3$.

6 December 2013.
Mr. Jamil NAJIM.
Maths 500.

A beautiful application of this is decomposing $\mathbb{C}[G]$ -modules into $\mathbb{C}[G]$ -submodules using e_i where we need to know irreducible χ_i .

Recipe to find submodules -

1. choose basis for $V \subseteq \mathbb{C}^n$, say $\{v_1, \dots, v_n\}$.
2. compute the set $e_i \cdot V = \{ \sum_{j=1}^n a_j v_j : 1 \leq i \leq n \} = \sum_{j=1}^n \chi_j(v_i^{-1}) v_j$. Ignore coefficients.
3. let $V_i = \text{span}_{\mathbb{C}} \{ e_i \cdot V \}$, then $V = \bigoplus V_i$ \therefore we have decomposed $\mathbb{C}[G]$ -module V into submodules.

Example - $D_6 \cong S_3 = \{ (1) \} \cup \{ (1 2), (1 3), (2 3) \} \cup \{ (1 2 3), (1 3 2) \}$. We take $V = \mathbb{C}^3$ to be the $\mathbb{C}[S_3]$ -module (permutation module) given by $\sigma \cdot v_i = v_{\sigma(i)}$

$\forall \sigma \in S_3, \forall v_i \in V$. $\rho: S_3 \rightarrow GL_3(\mathbb{C})$, $(1 2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $(1 3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Let $\{v_1, v_2, v_3\}$ be a standard basis for $V = \mathbb{C}^3$. Compute $e_1 \cdot V \implies$

$$e_1 \cdot v_1 = \frac{1}{6} (v_{(1)}(1) + v_{(1 2 3)}(1) + v_{(1 3 2)}(1) + v_{(1 2)}(1) + v_{(1 3)}(1) + v_{(2 3)}(1)) = \frac{1}{6} (v_1 + v_2 + v_3 + v_2 + v_1 + v_3) = \frac{1}{3} (v_1 + v_2 + v_3)$$

$$e_1 \cdot v_2 = \frac{1}{6} (v_1 + v_3 + v_1 + v_1 + v_2 + v_2) = \frac{1}{3} (v_1 + v_2 + v_3), \quad e_1 \cdot v_3 = \frac{1}{6} (v_1 + v_2 + v_3), \text{ so } V_1 = \text{span}_{\mathbb{C}} \{ e_1 \cdot V \} = \text{span}_{\mathbb{C}} \{ v_1 + v_2 + v_3 \} \subseteq V$$

$$\text{realise } e_2 \cdot v_1 = e_2 \cdot v_2 = 0, \text{ so } V_2 = \text{span}_{\mathbb{C}} \{ e_2 \cdot V \} = 0. \quad e_3 \cdot v_1 = \frac{1}{3} (2v_1 - (1 2 3) - (1 3 2)) = \frac{1}{3} (2v_1 - v_2 - v_3)$$

$$e_3 \cdot v_2 = \frac{1}{3} (2v_1 - v_2 - v_3) = \frac{1}{3} (2v_1 - v_2 - v_3), \quad e_3 \cdot v_3 = \frac{1}{3} (2v_1 - v_2 - v_3) = \frac{1}{3} (2v_1 - v_2 - v_3)$$

$V_3 = \text{span}_{\mathbb{C}} \{ e_3 \cdot V \} = \text{span}_{\mathbb{C}} \{ 2v_1 - v_2 - v_3 \}$. If we ignore coefficients and label $f_i = e_i \cdot v_i$, then $f_1, f_2, f_3 \neq 0 \implies$ not LI. Then $V_3 = \text{span}_{\mathbb{C}} \{ e_3 \cdot V \} = \text{span}_{\mathbb{C}} \{ 2v_1 - v_2 - v_3, 2v_2 - v_1 - v_3 \}$. Then we have

$$V = V_1 \oplus V_3 = \text{span}_{\mathbb{C}} \{ v_1 + v_2 + v_3 \} \oplus \text{span}_{\mathbb{C}} \{ 2v_1 - v_2 - v_3, 2v_2 - v_1 - v_3 \}$$

Class Functions

Recall that characters are $\chi: G \rightarrow \mathbb{C}$ are functions which are constant on conjugacy classes of G . So if $g = xhx^{-1}$, $h \in G$, then $\chi(g) = \chi(h)$.

Definition A class function $\varphi: G \rightarrow \mathbb{C}$ is a function that is constant on conjugacy classes of G . (i.e. $\varphi(g) = \varphi(h)$ if g, h in same conjugacy class).

Examples - clearly, characters of representations.

Let $\mathcal{F} = \{ \varphi: G \rightarrow \mathbb{C} \text{ where } \varphi \text{ is a class function} \}$. This is a \mathbb{C} -vector space of dimension $r = \text{number of conjugacy classes}$. Then χ_1, \dots, χ_r (irreducible characters of G)

form a basis for \mathcal{F} .

Moment let G be finite, then $\mathcal{F} = \text{span}_{\mathbb{C}} \{ \chi_1, \dots, \chi_r \}$ is a basis for the space of class functions, s.t. any $\varphi \in \mathcal{F}$ can be uniquely expressed as $\varphi = \sum_{i=1}^r \lambda_i \chi_i$, $\lambda_i \in \mathbb{C}$

and χ_i are irreducible characters of G .

Proof - we know $\mathbb{C}[G] = \bigoplus_{i=1}^r M_{n_i}(\mathbb{C}) \iff \{ \chi_1, \dots, \chi_r \}$ irreducible characters and r is number of conjugacy classes. Let $\{K_1, \dots, K_r\}$ be conjugacy classes of G .

Define the class functions $\chi_i: G \rightarrow \mathbb{C}$, $\chi_i(g) = \begin{cases} 1 & \text{if } g \in K_i \\ 0 & \text{if } g \notin K_i \end{cases}$. Then $\{ \chi_1, \dots, \chi_r \}$ form a basis if we establish LI. Let $0 = \sum_{j=1}^r \lambda_j \chi_j \in \mathcal{F}$, must show $\lambda_j = 0 \forall j$.

Use idempotents $E_i \rightarrow \chi_i$. $0 = \sum_{j=1}^r \lambda_j \chi_j(E_i)$ where $\chi_j(E_i) = \deg(\chi_j|_{H_i}) = \deg(\chi_j)$ if $i=j$, $\chi_j(E_i) = 0$ if $i \neq j$. Then $0 = \sum_{j=1}^r \lambda_j \chi_j(E_i) = \lambda_i \deg(\chi_i)$. Since $\lambda_i = 0 \forall i \neq i$ q.e.d.

Positive Definite Hermitian Forms

A positive definite Hermitian form is provided by the complex inner product space $(V, \langle \cdot, \cdot \rangle)$, $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{C}$ satisfying:

- (1) $\langle v, w \rangle = \overline{\langle w, v \rangle}$ (conjugate symmetry)
- (2) $\langle \lambda_1 v_1 + \lambda_2 v_2, w \rangle = \lambda_1 \langle v_1, w \rangle + \lambda_2 \langle v_2, w \rangle$ (linearity in first argument - beware, not second! $\langle v_1, \lambda w_1 + \lambda w_2 \rangle = \overline{\lambda} \langle v_1, w_1 \rangle + \overline{\lambda} \langle v_1, w_2 \rangle$)
- (3) $\langle v, v \rangle \geq 0$ and $\langle v, v \rangle = 0 \iff v = 0$.

Example of complex inner product -

$\langle \cdot, \cdot \rangle: \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$
let $V = \mathbb{C}^n$, $\langle v, w \rangle = \overline{v}^T A w$ where A is any positive Hermitian matrix $a_{ij} = \overline{a_{ji}}$ e.g. $A = \begin{pmatrix} 1 & 2-3i \\ 2+3i & 4 \end{pmatrix}$, $\overline{A}^T = A$.

Definition Let φ, ψ be two class functions (characters), then their inner product is the complex number $\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}$ for $\varphi, \psi: G \rightarrow \mathbb{C}$, $\varphi, \psi: G \rightarrow \mathbb{C}$. [$\therefore \varphi, \psi$ as complex vectors].

Example - The set $\{\chi_1, \dots, \chi_r\}$ of irreducible characters $\leftrightarrow \{g_1, \dots, g_r\}$ form an orthonormal basis for the space \mathcal{L} of class functions, if we choose r conjugacy class representatives $\{g_1, \dots, g_r\}$ for G . $\therefore \langle \chi_i, \chi_j \rangle = \delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

Properties (1), (2) are easy to check, so we just check (3) positive definiteness - $\langle \varphi, \varphi \rangle = \frac{1}{|G|} \sum_{g \in G} |\varphi(g)|^2 \geq 0$, with equality iff $\varphi(g) = 0 \forall g$.

Example of inner product of class functions: let $G = S_3$, φ, ψ be class functions $S_3 \rightarrow \mathbb{C}$. character table is given on right. Then, by definition, $\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)} = \frac{1}{6} (\varphi(1)\overline{\psi(1)} + \varphi(x)\overline{\psi(x)} + \varphi(x^2)\overline{\psi(x^2)}) = \frac{1}{6} (1 \cdot \overline{2} + 1 \cdot \overline{1} + 1 \cdot \overline{1}) = \frac{1}{6} (1 - 2 + 1 + 1) = \frac{1}{6} (1 - 1) = 0$. then $\langle \varphi, \psi \rangle = \langle \psi, \varphi \rangle = \frac{1}{6} (1 + 1) = \frac{1}{3} (1 + 1) = \frac{2}{3}$.

$\langle \varphi, \varphi \rangle = \frac{1}{6} (\varphi(1)\overline{\varphi(1)} + \varphi(x)\overline{\varphi(x)} + \varphi(x^2)\overline{\varphi(x^2)}) = \frac{1}{6} (1 + 1 + 1) = 1 \Rightarrow \varphi$ is a basis element and an irreducible character. $\langle \psi, \psi \rangle = \frac{1}{6} (2 \cdot \overline{2} + 1 \cdot \overline{1} + (-1)\overline{(-1)}) = \frac{1}{6} (4 + 1 + 1) = 1 \Rightarrow \psi$ is a reducible character $\therefore \psi = \sum n_i \chi_i$.

We can use this to check if $\rho: G \rightarrow \mathbb{C}$ is simple, without computing $\text{End}_{\mathbb{C}[G]}(\rho)$.

Proposition Let G have conjugacy classes $\{g_1, \dots, g_r\}$. let χ and ψ be two characters of G . then we have:

- (1) $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)}$ and (2) $\langle \chi, \psi \rangle = \sum_{g_i \in G} \frac{\chi(g_i) \overline{\psi(g_i)}}{|C_G(g_i)|}$ where $C_G(g_i) = 1 \times G_i, \chi g_i = g_i \chi$ (3) $\langle \chi, \chi \rangle \in \mathbb{R}$
- Proof - since $\chi(g^{-1}) = \overline{\chi(g)}$ if $g^{-1} \in (g)$, then $\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g^{-1})} = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) \psi(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \psi(g) = \langle \psi, \chi \rangle$ q.e.d.
(2) consider $\sum_{g_i \in G} \chi(g_i) \overline{\psi(g_i)} = \sum_{g_i \in G} (|g_i|)^{-1} \chi(g_i) \overline{\psi(g_i)}$ where g_i are conjugacy class reps. $\therefore \frac{1}{|G|} \sum_{g_i \in G} \chi(g_i) \overline{\psi(g_i)} = \langle \chi, \psi \rangle = \sum_{g_i \in G} \frac{|g_i|^{-1} \chi(g_i) \overline{\psi(g_i)}}{|C_G(g_i)|} = \sum_{g_i \in G} \frac{\chi(g_i) \overline{\psi(g_i)}}{|C_G(g_i)|}$
(3) $\langle \chi, \chi \rangle = \langle \overline{\chi}, \chi \rangle$ (conjugate symmetric) = $\langle \chi, \chi \rangle$ (by definition) $\Rightarrow \langle \chi, \chi \rangle \in \mathbb{R}$ q.e.d.

Example - let $G = A_4 = \{ \sigma \in S_4 : \text{sgn}(\sigma) = 1 \}$. $|G| = 12$. $C \cong C_2 \times C_2 \times C_3 \cong M_3(\mathbb{C})$, $r=4$ conjugacy classes. Define $g_1 = (1)$, $g_2 = (12)(34)$, $g_3 = (123)$, $g_4 = (132)$.
Define two characters $\chi, \psi: A_4 \rightarrow \mathbb{C}$. then we have $\langle \chi, \psi \rangle = \frac{1}{12} \left(\frac{4}{12} + \frac{1 \cdot 0}{4} + \frac{\omega \cdot \overline{\omega^2}}{3} + \frac{\omega^2 \cdot \overline{\omega}}{3} \right) = \frac{1}{12} + \frac{\omega}{3} + \frac{\omega^2}{3} = \frac{1}{12} + \frac{\omega}{3} + \frac{\omega^2}{3} = 1 \Rightarrow \psi$ is irreducible, corresponds to a simple character. $\langle \psi, \psi \rangle = \frac{4 \cdot 4}{12} + \frac{\omega^2 \cdot \overline{\omega^2}}{3} + \frac{\omega \cdot \overline{\omega}}{3} = \frac{16}{12} + \frac{1}{3} + \frac{1}{3} = 2 \Rightarrow$ reducible.

represented by g_1, \dots, g_r
Motivation: We know characters are constant on conjugacy classes and they form a basis for $\mathcal{L} = \text{span} \{ \chi_1, \dots, \chi_r \}$, so we can arrange our characters into an $r \times r$ matrix with entries $\chi_i(g_j)$ where $1 \leq i, j \leq r$.

Definition the character table of G is the $r \times r$ invertible matrix (for basis χ_i) given with the (i,j) -entry $\chi_i(g_j)$:

Example - if $G = D_8$, we have the following table

	g_1	\dots	g_3	\dots	g_r
χ_1	$\chi_1(g_1)$	\dots	$\chi_1(g_3)$	\dots	$\chi_1(g_r)$
χ_2	$\chi_2(g_1)$	\dots	$\chi_2(g_3)$	\dots	$\chi_2(g_r)$
\vdots	\vdots	\dots	\vdots	\dots	\vdots
χ_r	$\chi_r(g_1)$	\dots	$\chi_r(g_3)$	\dots	$\chi_r(g_r)$

Row and Column Orthogonality Relations

Used to reconstruct $(\chi_i(g_j))_{i,j}$ character table, find $|G|, |C_G(g_i)|, |C_G(g_j)|$. used to induce characters etc -

(1) Row orthogonality relation - for two fixed characters, run through the row of conjugacy classes. Since χ_1, \dots, χ_r form an orthonormal basis for \mathcal{L} by irreducibility theorem, $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ so for conjugacy class representatives $\{g_1 = (1), \dots, g_r\}$, we have $\sum_{k=1}^r \frac{\chi_k(g_i) \overline{\chi_k(g_j)}}{|C_G(g_k)|} = \delta_{ij} = \langle \chi_i, \chi_j \rangle$.

(2) Column orthogonality relation (more useful). fix two conjugacy classes, run through all characters on table. $\sum_{k=1}^r \chi_k(g_i) \overline{\chi_k(g_j)} = \delta_{ij} |C_G(g_i)| = \begin{cases} |C_G(g_i)| & \text{if } g_i \text{ is conjugate to } g_j \\ 0 & \text{otherwise (different columns)} \end{cases}$

Proof - Define the class function $\chi_k(g_i) = \delta_{ij}$. then since $\{\chi_1, \dots, \chi_r\}$ form basis for \mathcal{L} , $\chi_k \in \mathcal{L} \Rightarrow \chi_k = \sum_{i=1}^r \lambda_k \chi_i$, $\lambda_k \in \mathbb{C}$. Using Irreducibility Theorem, $\langle \chi_i, \chi_k \rangle = \delta_{ik}$. then $\lambda_k = \langle \chi_i, \chi_k \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_k(g)}$ but yet running through $(g_i)^{G_i}$. Now $\chi_i(g) = 1$ if g is conjugate to g_i , $\chi_i(g) = 0$ otherwise. We also have $|C_G(g_i)|$ elements which are conjugate to g_i . Thus, $\lambda_k = \frac{1}{|G|} \cdot |C_G(g_i)| \overline{\chi_k(g_i)} = \frac{\overline{\chi_k(g_i)}}{|C_G(g_i)|}$. $\therefore \delta_{ij} = \chi_k(g_i) = \sum_{k=1}^r \lambda_k \chi_k(g_i) = \sum_{k=1}^r \frac{\overline{\chi_k(g_i)}}{|C_G(g_i)|} \cdot \chi_k(g_i) \Rightarrow \sum_{k=1}^r \chi_k(g_i) \overline{\chi_k(g_j)} = \delta_{ij} |C_G(g_i)|$ q.e.d.

Example - $G = D_8 = \langle \sigma \rangle \cup \langle \sigma \rangle \cup \langle \sigma \rangle$. $|G| = 8$, $|C_G(g_1)| = 8$, $|C_G(g_2)| = 4$, $|C_G(g_3)| = 2$. then $\sum_{k=1}^4 \chi_k(g_1) \overline{\chi_k(g_1)} = \delta_{11} |C_G(g_1)| = 8$. how can we fill in the bottom row?
By orthogonality, examine first column: $i=1, j=1$. $\sum_{k=1}^4 \chi_k(g_1) \overline{\chi_k(g_1)} = \delta_{11} |C_G(g_1)| = 8$. fix i, j , here $g_i = g_j = 1 \Rightarrow \sum_{k=1}^4 \chi_k(1) \overline{\chi_k(1)} = \delta_{11} |C_G(1)| = 1 \cdot 6 = 6$.
 \Rightarrow by table: $\chi_1(1) \cdot \overline{\chi_1(1)} + \chi_2(1) \cdot \overline{\chi_2(1)} + \chi_3(1) \cdot \overline{\chi_3(1)} + \chi_4(1) \cdot \overline{\chi_4(1)} = 6 \Rightarrow 1 \cdot \overline{1} + 1 \cdot \overline{1} + a \cdot \overline{a} = 6 \Rightarrow 2 + a^2 = 6 \Rightarrow a = 2$. (we reject -2 , because first column is a trace of Id).

Then, we see that $a=2$. Since this is identity column, this produces a 2D representation. Likewise for column 2, fix $i=j$, $g_2=x$ s.t. $1\bar{1} + 1\bar{1} + b\bar{b} = 1c$, $b = \pm 1$? This is ambiguous, so we try another method - first and second column. $i=1, j=2 \Rightarrow S_{ij} = 0$, so we can ignore centralizer s.t. $\sum_{k=1}^3 \chi_k(1) \cdot \overline{\chi_k(x)} = 0 \Rightarrow 1\bar{1} + 1\bar{1} + 2\bar{b} = 0 \Rightarrow 2\bar{b} = -2 \Rightarrow \bar{b} = -1 \Rightarrow b = -1$. For third column, $1\bar{1} + 1\bar{(-1)} + 2\bar{c} = 0 \Rightarrow |C_G(x)| \Rightarrow 2\bar{c} = 0 \Rightarrow c = 0$.

2. A group of order 12 with 4 conjugacy classes $\{g_1, g_2, g_3, g_4\}$ and centralizers $|C_G(g_1)|=12, |C_G(g_2)|=4, |C_G(g_3)|=3, |C_G(g_4)|=3$.

It has partial χ -table as on right: We seek final row of table. First column with itself gives $S_{ii} |C_G(g_i)| = 12 \Rightarrow i\bar{i} + 1\bar{1} + 1\bar{1} + \chi_4(g_i) \cdot \overline{\chi_4(g_i)} = 12$

	g_1	g_2	g_3	g_4
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	?	?	?	?

$\Rightarrow |\chi_4(g_1)|^2 = 9 \Rightarrow \chi_4(g_1) = 3 \Rightarrow$ (reject -3) 3-dimensional rep. Then $i=1, j=2 \Rightarrow 3 + 3\overline{\chi_4(g_2)} = 0 \Rightarrow \chi_4(g_2) = -1$. Then $i=1, j=3 \Rightarrow 3 + 3\overline{\chi_4(g_3)} = 0 \Rightarrow \chi_4(g_3) = -1$. Then $i=1, j=4 \Rightarrow 3 + 3\overline{\chi_4(g_4)} = 0 \Rightarrow \chi_4(g_4) = -1$.

$\Rightarrow 1\bar{1} + 1\bar{\omega} + 1\bar{\omega^2} + 3\overline{\chi_4(g_2)} = 1 + \omega^2 + \omega + 3\overline{\chi_4(g_2)} = 0 \Rightarrow 3\overline{\chi_4(g_2)} = 0 \Rightarrow \chi_4(g_2) = 0$. $i=1, j=4 \Rightarrow 1\bar{1} + 1\bar{\omega} + 1\bar{\omega^2} + 3\overline{\chi_4(g_4)} = 0 \Rightarrow \chi_4(g_4) = 0$.

Last row is $\{3, -1, 0, 0\}$.

Summary on characters.

13 December 2013.
Mr. Jamil NAPIIM.
Next is 500.

We know that $\mathbb{C}[G] \cong S_1^{n_1} \oplus \dots \oplus S_r^{n_r}$ where each S_i is a simple $\mathbb{C}[G]$ -submodule of dimension n_i . For each S_i we have irreducible characters $\{\chi_1, \dots, \chi_r\}$ where $r = \#$ conjugacy classes of G . Then ① $\langle \chi_i, \chi_j \rangle = S_{ij}$ and ② if ψ is any character of G , then $\psi = d_1\chi_1 + \dots + d_r\chi_r$ for some non-negative integers d_i where $d_i = \langle \psi, \chi_i \rangle$. $\langle \psi, \psi \rangle = \sum_{i=1}^r d_i^2$.

Example - $D_6 \cong S_3 = \langle 1 \rangle \cup \langle (123) \rangle \cup \langle (12) \rangle$. Then the character table is as on right:

	(1)	(123)	(12)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	0	-1

$|C_G(1)|=1, |C_G(123)|=2, |C_G(12)|=3$.

$|C_{D_6}(g_i)| = \frac{|G|}{|g_i|}, C_{S_3}(1) = \frac{6}{1} = 6, C_{S_3}((123)) = \frac{6}{2} = 3, C_{S_3}((12)) = \frac{6}{2} = 3$. Let $\rho: S_3 \rightarrow GL_3(\mathbb{C})$ be the permutation representation $(123) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, (12) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. $\chi_\rho(1) = 3, \chi_\rho((123)) = 0, \chi_\rho((12)) = 1$. By ②, ψ is a linear combination of irreducibles.

characters: $\chi_\rho = d_1\chi_1 + d_2\chi_2 + d_3\chi_3$. $\langle \chi_\rho, \chi_1 \rangle = d_1 = \sum_{i=1}^3 \chi_\rho(g_i) \overline{\chi_1(g_i)} \cdot \frac{1}{|C_G(g_i)|} = \frac{3\bar{1} + 0\bar{1} + 1\bar{1}}{3} = 1$. $\langle \chi_\rho, \chi_2 \rangle = d_2 = 0$. $\langle \chi_\rho, \chi_3 \rangle = d_3 = 1$.

$\therefore \chi_\rho = 1\chi_1 + 1\chi_3$.

Theorem (Frobenius Reciprocity Theorem).

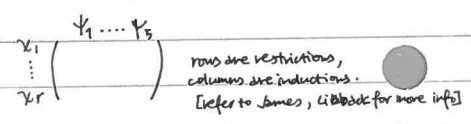
Let $H \leq G$, then if $\chi: G \rightarrow \mathbb{C}$ is a character of G , then $\chi \downarrow H$ is called the restricted character of H , $\chi \downarrow H: H \rightarrow \mathbb{C} \quad \forall h \in H$
 $h \mapsto \chi(h)$ i.e. we ignore elements of G that are not in H [for example, $\rho: G_6 \rightarrow GL_2(\mathbb{C}), \chi: D_6 \rightarrow \mathbb{C}$. Let $H = G_3$, $\chi(1) = 2, \chi(x) = -1, \chi(x^2) = -1$ [fake]
 $\chi(y) = 0, \chi(y^2) = 0$ [ignore].]

If ψ_1, \dots, ψ_s are irreducible characters of H , then $(\chi \downarrow H) = d_1\psi_1 + \dots + d_s\psi_s$ s.t. $\sum_{i=1}^s d_i^2 \leq [G:H]$. For each $\mathbb{C}[H]$ -module V , the induced $\mathbb{C}[G]$ -module $\text{Ind}_H^G(V)$ has character defined using the character ψ of H written as $(\psi \uparrow G)(g) = \frac{1}{|H|} \sum_{y \in G} \psi(y^{-1}gy)$ where $\psi(g) = \begin{cases} \psi(g) & g \in H \\ 0 & g \notin H \end{cases}$

Then $\langle \psi \uparrow G, \chi \rangle_G = \langle \psi, \chi \downarrow H \rangle_H$ where ψ is a character of H and χ is a character of G .

END OF SYLLABUS.

The Frobenius Reciprocity theorem is important as it allows us to write characters for G and H .



END OF COURSE.

A problem class will be convened on Friday, 25 April 2014.