LECTURE I

Def (Ring): A ring is a set R with two binary operations
- Addition : $(a,b) \longmapsto a+b$
- multiplication : $(a,b) \longmapsto ab$

Such that

① A is an abelian gp. under addition:
- $a+b = b+a \quad \forall\ a,b \in R$
- $\exists\ 0 \in A \ni a+0 = a \quad \forall\ a \in R$
- $\forall\ a \in A\ \exists\ -a \in A \ni a+(-a) = 0$.

② Multiplication is associative:
- $(ab)c = a(bc)$

③ Multiplication distributes over addition
- $a(b+c) = ab+ac$
- $(a+b)c = ac+bc$.

Example: Let A be an abelian group.

$$R = \mathrm{End}(A)$$
$$= \{ f : A \to A \mid f(a+b) = f(a)+f(b) \}$$

is a ring, when with $(f+g)(a) = f(a)+g(a)$

$$(fg)(a) = f(g(a))$$

In this example the identity map:

$$1 = id_A : A \to A$$

has the property $f \cdot 1 = 1 f = f$

1 is called a unit, R is said to be unital.

Defn (Ring homomorphism)

A ring homomorphism is a function $f: R \to R'$ where R and R' are rings and $f(a+b) = f(a)+f(b)$
$$f(ab) = f(a)f(b).$$

Defn (left R-module)

An R-module is an abelian group M together with a ring homomorphism $R \to \mathrm{End}(M)$

Example: A - abelian group. Then A is a left End(A) - module.

Defn (R-module homomorphism)

An R-module homomorphism is a function $f: M \to M'$ where M and M' are R-modules, f is a homomorphism of abelian groups such that $f(am) = af(m)$ $\forall\, a \in R$ and $m \in M$

$\mathrm{Hom}_R(M, M')$ denotes the space of R-module homs.

Example: Let R be a ring. Fix $a \in R$

Then $f: R \to R$ defined by
$$f(x) = xa$$
is an R-module homomorphism.

Defn (Direct sum)

If $\{M_\alpha\}$ is a collection of R-modules, then an R-module M is said to be a <u>direct</u> <u>sum</u> of the M_α's if $\forall\ \alpha$, $\exists$ an R-module homomorphism $\varphi_\alpha : M_\alpha \to M$ such that whenever $\{\eta_\alpha : M_\alpha \to N\}$ is a collection of R-module homomorphisms, there exits a unique R-module homomorphism $\eta : M \to N$ such that

$$\eta \circ \varphi_\alpha = \eta_\alpha$$

$$\begin{tikzcd} M_\alpha \arrow[r, "\varphi_\alpha"] \arrow[dr, "\eta_\alpha"'] & M \arrow[d, dashed, "\eta"] \arrow[dl, phantom, "\circlearrowright"] \\ & N \end{tikzcd}$$

<u>Theorem</u>: Every collection of R-modules has a direct sum, which is unique up to unique isomorphism <u>which</u> <u>preserves</u> <u>the</u> φ_α's.

<u>Proof</u>: Define

$$M = \{(m_\alpha) \in \prod_\alpha M_\alpha \mid m_\alpha = 0 \text{ for all but finitely many } \alpha\}$$

R-action componentwise

Define $\varphi_\alpha : M_\alpha \to M$ by $m \mapsto (m_\beta)$ where $m_\beta = \begin{cases} 0 & \text{if } \alpha \neq \beta \\ m & \text{if } \alpha = \beta \end{cases}$

(4)

Given $\{\eta_\alpha : M_\alpha \to N\}$ must have

$$\eta : M \to N \text{ by } \eta(m_\alpha) = \sum_{\alpha \in} \eta_\alpha(m_\alpha)$$

If M' is another direct sum, with $\{\varphi'_\alpha : M_\alpha \to M\}$, then

$$\begin{tikzcd}
 & M \arrow[d, "\varphi'"] \arrow[dd, bend left=60, "id_M"] \\
M_\alpha \arrow[ur, "\varphi_\alpha"] \arrow[r, "\varphi'_\alpha"] \arrow[dr, "\varphi_\alpha"'] & M' \arrow[d, "\varphi"] \\
 & M
\end{tikzcd}$$

$$M = \bigoplus_\alpha M_\alpha$$

Corollary $\mathrm{Hom}(\oplus M_\alpha, N) = \prod_\alpha \mathrm{Hom}(M_\alpha, N)$

Example: (free module)

Let S be any set. The free R-module on S is $R^S = \bigoplus_{\alpha \in S} R$

Remark: (projections from a direct sum)

In the defn of direct sum, fix β

Take $N = M_\beta$.

Define $\eta_\alpha = \begin{cases} 0 & \text{if } \alpha \neq \beta \\ id_{M_\alpha} & \text{if } \alpha = \beta \end{cases}$

Then the induced map $p_\beta = \eta : \oplus M \to M_\beta$ satisfies $p_\beta \circ \eta_\alpha = \begin{cases} 0 & \text{if } \alpha \neq \beta \\ id_{M_\alpha} & \text{if } \alpha = \beta \end{cases}$

projection onto M_β

<u>Theorem</u> Suppose S is a finite set. For every collection $\{q_\alpha : N \to M_\alpha\}$ of R-module homomorphisms, there exists a unique $q : N \to M$ such that

$$\begin{tikzcd} M \arrow[r, "p_\alpha"] & M_\alpha \\ & N \arrow[ul, dashed, "q"] \arrow[u, "q_\alpha"'] \arrow[ul, phantom, shift left=3, "G"] \end{tikzcd}$$

<u>Proof</u>: Omitted

<u>Corollary</u>: If S is finite, $Hom(N, \bigoplus_{\alpha \in S} M_\alpha) = \prod_{\alpha \in S} Hom(N, M_\alpha)$

<u>Corollary</u> If S is finite

$$Hom(\bigoplus_\alpha M_\alpha, \bigoplus_{\beta \in S} N_\beta) = \prod_\alpha \prod_{\beta \in S} Hom(M_\alpha, N_\beta)$$

It is customary to think of such a homomorphism as a matrix. Composition is matrix multiplication.

<u>Exercise</u>: If R is unital, then $End_R R = R$

<u>Corollary</u>: $Hom_R(R^n, R^m) \cong M_{m\times n}(R)$

The composition map $Hom(R^m, R^k) \times Hom(R^n, R^m)$

$$\downarrow$$

$$Hom(R^n, R^k)$$

Corresponds to the matrix mult. map.

⑥

Example (where $R \cong R \oplus R$)

Suppose $R \to R \oplus R$ is an iso

It is given by a 2×1 matrix $\begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$ with entries in R

Injectivity means: $e_1 a = e_2 a = 0 \Rightarrow a = 0 \ \forall a \in R$

Surjectivity means: $\exists f_1 \,\&\, f_2 \in R \ni e_i f_j = \delta_{ij} \ \forall i, j$

e.g. (V.S. Sunder)

Let V be a two dimensional Hilbert space with orthonormal bases $\{f_1, f_2\}$

$$R = \mathrm{End}_{\mathbb{C}}(\mathbb{C} \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots)$$

mult $(\vec{x}_1 \otimes \cdots \otimes \vec{x}_k)(\vec{y}_1 \otimes \cdots \otimes \vec{y}_k) = \vec{x}_1 \otimes \cdots \otimes \vec{x}_k \otimes \vec{y}_1 \otimes \cdots \otimes \vec{y}_k$.

Then $f_1 \,\&\, f_2 \in R$ (left mult)

define $e_i(x_1 \otimes \cdots \otimes x_k)$

$$= \langle e_i, x_1 \rangle \, x_2 \otimes \cdots \otimes x_k$$

Theorem: If R is commutative and $R^n \cong R^m$ then $m = n$

Proof: $\underset{e_1, \ldots, e_n}{R^n} \xrightarrow{\varphi} \underset{f_1, \ldots, f_m}{R^m} \xrightarrow{\psi} \underset{e_1, \ldots, e_n}{R^n}$ $\quad \underset{id_{R^n}}{\varphi \circ \psi \,\|}, \ \underset{id_{R^m}}{\psi \circ \varphi \,\|}$

$$\varphi\left(\underset{m \times n}{A}\begin{pmatrix} \vec{e}_1 \\ \vdots \\ \vec{e}_n \end{pmatrix}\right) = \begin{pmatrix} \vec{f}_1 \\ \vdots \\ \vec{f}_m \end{pmatrix} \qquad \psi\left(\underset{n \times m}{B}\begin{pmatrix} \vec{f}_1 \\ \vdots \\ \vec{f}_m \end{pmatrix}\right) = \begin{pmatrix} \vec{e}_1 \\ \vdots \\ \vec{e}_n \end{pmatrix}$$

Then $AB = I_{m\times m}$

Assume $m > n$.

Let $\tilde{A} = \left[A \,/\, 0 \right]_{m\times m}$ $\quad \tilde{B} = \left[\frac{B}{0} \right]_{m\times m}$

$$\tilde{A}\tilde{B} = AB = I$$

$\Rightarrow \tilde{B}\tilde{A} = I$ (why?)

But $\tilde{B}\tilde{A} = \begin{bmatrix} BA & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow \Leftarrow$

LECTURE II

Theorem: If R is a pid, then every submodule of R^n is free of rank $m \le n$.

Pf: Induct on n.

$n = 1$, $M \subset R \Rightarrow M = (f)$ $f \in R \Rightarrow$ $a \mapsto af$
$R \mapsto M$

R^n spanned by $e_1, \dots, e_n$

Consider R^{n-1} spanned by $e_2, \dots, e_n$ $\quad R'$ spanned by e_1

If $M \subset R^{n-1}$ done

Else, $\dfrac{M + R^{n-1}}{R^{n-1}} \subseteq \dfrac{R^n}{R^n} \cong R$ is a free module of rk. 1,

& gen^d by $f_1 + R^{n-1}$, $f_1 \in R^1$

$M \cap R^{n-1}$ is a free module of rk $m-1$, $m \le n$

gen. by $f_2, \dots, f_m$

Suppose $m \in M$. $\exists\, a_1 \in R \ni m - a_1 f_1 \in R^{n-1} \dots$

Defn: (finitely gen. R-module)

M is a finitely generated R-module if $\exists$ surjective R-module hom $R^n \to M$ for some $n \in \mathbb{N}$.

$K = \{x \in R^n \mid x \mapsto 0 \in M\}$.

Relation to matrices: $0 \to K \to R^n \to M \to 0$

K is free. Take a basis $f_1, \dots, f_m$

$$\begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} = \underbrace{A_{m\times n}}_{\text{matrix of relations}} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

Change of basis $\longleftrightarrow$ PAQ

$P \in GL_m(R)$

$Q \in GL_n(R)$.

$\therefore$ A & PAQ give rise to isomorphic R-modules

Defn: $A, B \in M_{m\times n}(R)$ are said to be equivalent if $\exists$ $P \in GL_m(R)$ & $Q \in GL_n(R)$ $\ni$ $B = PAQ$.

Theorem: (Smith canonical form):

Let R be a p.i.d. Then every $A \in M_{m\times n}(R)$ is equivalent to a matrix of the form $\begin{pmatrix} d_1 & & & & 0 \\ & d_2 & 0 & & \\ 0 & & \ddots & & \\ & & & d_r & \\ & & 0 & & 0 \end{pmatrix}$

where $d_1 \mid d_2 \mid \dots \mid d_r$, $d_i \neq 0$. Moreover, d_i's are unique up to multiplication by units.

<u>Proof</u>: We are allowed elementary row & column ops

First assume that R is a <u>Euclidean domain</u>

with norm: $\delta : R \to \mathbb{N}$ $(\delta(0) = \infty)$ Assume $A \neq 0$.

Suppose a_{ij} is such that $\delta(a_{ij})$ is minimal

By interchanging rows and columns, can make sure

that $\delta(a_{11})$ is minimal

For $k > 1$ if $a_{1k} \neq 0$, $a_{1k} = a_{11} b_k + b_{1k}$. If $b_{1k} \neq 0$,

$$C_k \to C_k - b_k C_1.$$

Get a new matrix with $\delta(a_{1k}) < \delta(a_{11})$

Again interchange rows and columns to get

$\delta(a_{11})$ minimal.

This new value is strictly less than the old one

Can do the same thing with the rows

Since $\delta \in \mathbb{N}$, a finite no of steps will result

in a matrix for which $a_{11} | a_{1k}$ & $a_{11} | a_{j1}$ $\forall j, k$.

Then use row & column ops to get

$$\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \qquad A' = \begin{pmatrix} a'_{22} & a'_{23} & \cdots & a'_{2n} \\ a'_{32} & & & \\ \vdots & & & \\ a'_{n2} & & & \end{pmatrix}$$

proceed by induction

(10)

The same method works over a PID with a little modification:

For $a \neq 0$, define $\ell(a) = \#$ prime factors in the decomposition of a

[$\ell(a) = 0$ if a is a unit]

As before, may assume that $\ell(a_{11})$ is minimal.

Suppose $a_{11} \nmid a_{1k}$

By interchanging cols., assume

$$a_{11} \nmid a_{12}$$

Let $d = (a_{11}, a_{12})$

Can write $a_{11}x + a_{12}y = d$

Calculate

$$\begin{pmatrix} a_{11} & a_{12} \\ * & * \end{pmatrix} \begin{pmatrix} x & \frac{a_{12}}{d} \\ y & \frac{-a_{11}}{d} \end{pmatrix} = \begin{pmatrix} d & 0 \\ * & * \end{pmatrix}$$

Moreover $\det \begin{pmatrix} x & \frac{a_{12}}{d} \\ y & -\frac{a_{11}}{d} \end{pmatrix} = -\frac{a_{11}x + a_{12}y}{d} = -1$ (unit)

$$A \begin{pmatrix} x & \frac{a_{12}}{d} & & \\ y & -\frac{a_{11}}{d} & & 0 \\ & & 1 & \\ 0 & & & 1 \end{pmatrix} = \begin{pmatrix} d & 0 & * & \cdots \\ * & * & & \\ & & & * \\ & & & \end{pmatrix}$$

$$\ell(d) < \ell(a_{11})$$

Claim: Can arrange that b_{11} divides all the entries of A'.

For if not, then $\delta(b_{11})$ can be decreased further.

Suppose $b_{11} \nmid a'_{ij}$.

$R_1 \to R_1 + R_i$.

First row: $b_{11} \quad a'_{i2} \ldots a'_{in}$

Repeat the above process.

Get a new matrix of type

$$\begin{pmatrix} b_{11} & 0 \cdots & 0 \\ 0 & & \\ \vdots & A' & \\ 0 & & \end{pmatrix}$$

with $\delta(b_{11})$ strictly less.

For uniqueness we use the following lemma:

<u>Lemma</u>: Suppose A is equivalent to B.

$\Delta_i(A) = \gcd$ of $i \times i$ minors of A

$\Delta_i(B) = \gcd$ of $i \times i$ minors of B.

Then $\Delta_i(A)$ & $\Delta_i(B)$ differ by units.

<u>Pf.</u> Suppose $PAQ = B$.

Then cols. of B are lin. combinations of columns of A.

$\therefore$ $i \times i$ minors of B are linear combos. of $i \times i$ minors of A.

$\therefore$ each $i \times i$ minor of $B \in (\Delta_i(A))$

$\Rightarrow \Delta_i(B) \subseteq (\Delta_i(A))$

If Q is invertible, so $A = BQ^{-1}$

$\Rightarrow \Delta_i(A) \subseteq (\Delta_i(B))$

$\therefore (\Delta_i(A)) = (\Delta_i(B))$

Similarly if $PA = B$, then $(\Delta_i(A)) = (\Delta_i(B))$

Combining: $\Delta_i(PAQ) = \Delta_i(A)$

(12)

Suppose $A \sim \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$

$\Delta_i(A) = d_1 \cdots d_i \cdot u$

$d_1 = \Delta_1(A)u$, $d_i = \dfrac{\Delta_i(A)}{\Delta_{i-1}(A)}u$ for $i = 1, \ldots, r$, $d_i = 0$ $i > r$

$\therefore d_i$'s are determined upto unit by A $\boxed{\text{QED}}$

<u>Defn</u> The ith invariant factor of A is the ideal generated by the $i \times i$ minors of A.

<u>Corollary</u> A and B are equivalent iff they have the same invariant factors.

<u>Back to finitely generated R-modules</u>

We have:

$$0 \to \underset{\langle d_1 e_1, \ldots, d_r e_r \rangle}{K} \longrightarrow \underset{\langle e_1, \ldots, e_n \rangle}{R^n} \xrightarrow{\varphi} M \longrightarrow 0$$

Let $z_i = \varphi(e_i)$.

Then $M = Rz_1 \oplus \cdots \oplus Rz_n$

As an R-module $Rz_i \cong R/\mathrm{Ann}(z_i)$

where $\mathrm{Ann}(z_i) = \{ r \in R \mid \underset{\varphi(re_i)}{rz_i} = 0 \} = (d_i)$.

(put $d_{r+1} = \cdots = d_n = 0$)

Theorem: (Structure of finitely generated modules over a PID)

If $M (\neq 0)$ is a finitely generated module over a PID, then $\exists$ non-zero elements $z_1, z_2, \dots, z_s \in M$ such that $M = Rz_1 \oplus \dots \oplus Rz_s$

with $\text{Ann}(z_1) \supset \text{Ann}(z_2) \supset \dots \supset \text{Ann}(z_s)$

$\therefore M \simeq R/(d_1) \oplus \dots \oplus R/(d_s)$ $(d_1) \supset (d_2) \supset \dots \supset (d_s)$

Lecture III

Defn: (Torsion module)

Let R be any commutative domain & M be an R-module.

$M_{tor} = \{ m \in M \mid rm = 0 \text{ for some } r \in R, r \neq 0 \}$

M_{tor} is a submodule of R, called its torsion module

Defn: M is a torsion R-module if $M = M_{tor}$.

Theorem: Any finitely generated module over a p.i.d. is a ~~torsi~~ direct sum of M_{tor} & a free submodule.

Pf. $M = Rz_1 \oplus \dots \oplus Rz_s$

$\text{Ann}(z_1) \supseteq \dots \supseteq \text{Ann}(z_s)$.

k = largest integer for which $\text{Ann}(z_i) \neq (0)$ $\forall i \geq k$.

$M_{tor} = Rz_k \oplus \dots \oplus Rz_s$

$M_{free} = Rz_1 \oplus \dots \oplus Rz_{k-1}$

Example: (the free part is not canonical)

$$\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}(1,1) \oplus \mathbb{Z}(0,1)$$

Definition: (primary component) Let R be a PID. Let $\mathfrak{p} \subset R$ be a prime ideal. The $\mathfrak{p}$-primary component of an R-module M is

$$M_{\mathfrak{p}} := \{ m \in M \mid p^k m = 0 \text{ for some } k \in \mathbb{N} \}.$$

Here p denotes a generator for $\mathfrak{p}$.

Clearly, ① $M_{\mathfrak{p}} \subset M$ is a submodule

② $M_{\mathfrak{p}} \subset M_{tor}$

Definition (primary module) M is called $\mathfrak{p}$-primary if $M = M_{\mathfrak{p}}$. M is called primary if M is $\mathfrak{p}$-primary.

Theorem: (primary decomposition)
Let R be a PID, and M a finitely generated torsion R-module. Then

① $M_{\mathfrak{p}} = 0$ for all but finitely many prime ideals $\mathfrak{p} \subset R$.

② $M = \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}}$ (direct sum over all prime ideals).

Proof:

Step 1: Suppose $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_h$ are distinct prime ideals in R, then $M_{\mathfrak{p}_1} \cap (M_{\mathfrak{p}_2} + \ldots + M_{\mathfrak{p}_h}) = 0$.

pf of step 1: Suppose $y \in M_{p_1} \cap (M_{p_2} + \cdots + M_{p_k})$

Then $y = y_2 + \cdots + y_k$, where $p_i^{k_i} y_i = 0$ for $i = 2, \ldots, k$

$((p_i) = p_i)$

$\therefore \quad p_2^{k_2} p_3^{k_3} \cdots p_k^{k_k} y = 0$

Moreover $p_1^{k_1} y = 0$

$\therefore \quad (p_1^{k_1}, p_2^{k_2} \cdots p_k^{k_k}) \in \operatorname{ann}(y)$

But $1 \in (p_1^{k_1}, p_2^{k_2} \cdots p_k^{k_k})$.

$\therefore \quad y = 0$

Step 2: If $M = Rx$, where $\operatorname{ann}(x) = (d)$ and $d = gh$, with $(g, h) = 1$, then $M = Ry + Rz$ for some $y, z \in M$ with $\operatorname{ann}(y) = (g)$ and $\operatorname{ann}(z) = h$

pf of Step 2: $rg + sh = 1$

Put $y = hx$, $z = gx$.

Then $x = (rg + sh)x = rz + sy \in Ry + Rz$

$\therefore \quad M = Rx = Ry + Rz$.

Step 3: If $M = Rx$, where $\operatorname{ann}(x) = (d)$ and $d = p_1^{e_1} \cdots p_t^{e_t}$, where the p_i's are distinct primes, then $M = Rx_1 \oplus \cdots \oplus Rx_t$ where $\operatorname{ann}(x_i) = (p_i^{e_i})$ $\therefore M = M_{p_1} + \cdots + M_{p_t}$ (since $M_{p_i} \supset Rx_i$)

pf of Step 3: Step 2 + induction.

(16)

Conclusion of the proof

M finitely gen

$\Rightarrow$ $M = Rx_1 + \cdots + Rx_n$ (not nec. a direct sum)

$$= \sum_p (Rx_1)_p + \cdots + (Rx_n)_p$$

$$= \sum_p M_p$$

The sum must be direct because of Step 1.

Structure of M_p:

By the structure theorem for modules over a PID,

$$M_p = Rz_1 \oplus \cdots \oplus Rz_s$$

$\mathrm{ann}(z_i) = p^k$ for some k

$$\therefore M_p = R/_{p^{\lambda_1}} \oplus \cdots \oplus R/_{p^{\lambda_k}}$$

with $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_k$.

Corollary: Every finitely generated module over a PID is a direct sum of primary cyclic modules.

Invariance theorem: Suppose $M = Dz_1 \oplus \cdots \oplus Dz_s = Dw_1 \oplus \cdots \oplus Dw_r$, with $\mathrm{ann}(z_1) \supset \cdots \supset \mathrm{ann}(z_s)$ & $\mathrm{ann}(w_1) \supset \cdots \supset \mathrm{ann}(w_r)$, and none of the summands is zero. Then $r = s$ and $\mathrm{ann}(z_i) = \mathrm{ann}(w_i)$ $\forall$ $i = 1, \ldots, s$.

Invariance theorem:

Suppose $M = R\mathfrak{z}_1 \oplus \cdots \oplus R\mathfrak{z}_s$

$= Rw_1 \oplus \cdots \oplus Rw_t$

where $\text{ann}\, \mathfrak{z}_1 \supset \cdots \supset \text{ann}\, \mathfrak{z}_s$

$\text{ann}\, w_1 \supset \cdots \supset \text{ann}\, w_t$

and none of the components are 0.

Then $s = t$ and $\text{ann}\, \mathfrak{z}_i = \text{ann}\, w_i \quad \forall\ 1 \le i \le s=t$.

Proof: The ideals $(\mathfrak{z}_i)$, (w_i) are called order ideals.

(1) Reduction to torsion modules:

Suppose u, v are such that

$\text{ann}\, \mathfrak{z}_u \neq 0, \quad \text{ann}\, \mathfrak{z}_{u+1} = 0$

$\text{ann}\, w_v \neq 0, \quad \text{ann}\, w_{v+1} = 0$.

$$\text{Then } M = \underbrace{\boxed{R\mathfrak{z}_1 \oplus \cdots \oplus R\mathfrak{z}_u}}_{M_{tor}} \oplus \underbrace{\boxed{R\mathfrak{z}_{u+1} \oplus \cdots \oplus R\mathfrak{z}_s}}$$
$$= \underbrace{\boxed{Rw_1 \oplus \cdots \oplus Rw_v}}_{\| \atop M_{tor}} \oplus \underbrace{\boxed{Rw_{v+1} \oplus \cdots \oplus Rw_t}}_{\cong M/M_{tor}}$$

$\therefore\ s - u = t - v$ and it suffices to prove the theorem for M_{tor}. So we may assume $M = M_{tor}$.

(2) Reduction to primary modules:

$R\mathfrak{z} = \oplus (R\mathfrak{z})_p$

$\mathfrak{z} = \sum_p \mathfrak{z}_p$

Then $(R\mathfrak{z})_p = R\mathfrak{z}_p$

$\text{ann}(\mathfrak{z}) = \prod_p \text{ann}(\mathfrak{z}_p)$.

$$M = \bigoplus_p M_p = \bigoplus_p \left[R(z_1)_p \oplus \cdots \oplus R(z_s)_p \right]$$

$$= \bigoplus_p \left[R(w_1)_p \oplus \cdots \oplus R(w_s)_p \right]$$

So if the order ideals in the direct sum decompositions of each M_p are the same, then so are the order ideals in the direct sum decomposition of M.

(3) Proof in the primary case:

Assume $M = M_p$.

Then $\operatorname{ann}(z_i) = p^{e_i} \quad e_1 \le \ldots \le e_s$

$\operatorname{ann}(w_i) = p^{f_i}. \quad f_1 \le \ldots \le f_t$.

$p^k M = \{p^k x \mid x \in M\}$ is a submodule.

$M \supset pM \supset p^2 M \supset \ldots$ descending chain.

$M^{(k)} := p^k M / p^{k+1} M$ — an R/p-module
field

$\dim M^{(k)} = \# \{ i \mid e_i > k \}$

$= \# \{ i \mid f_j > k \}$

Draw a Young diagram: $(e_1, e_2, e_3, e_4) = 1, 2, 4, 6$

e_i-boxes in the ith row.

$\# \{ i \mid e_i > k \} = \#$ boxes in the kth column

k any field

$k[t]$ – ring of polynomials with coeffs. in k.

Euclidean domain, hence a P.I.D.

We already understand the isomorphism classes of finitely generated $k[t]$-modules.

Suppose V is a finitely generated torsion $k[t]$-module.

Restricting the $k[t]$-action $\varphi: k[t] \to End(V)$ to k, gives V the structure of a k-vector space.

Get: $\varphi: k[t] \longrightarrow End_k(V)$

A cyclic $k[t]$ module is of the form $k[t]/p(t)$ for some $p(t) \in k[t]$, hence a finite dimensional vector space

Since V is a finite direct sum of such modules, V is a finite dimensional k-vector space

Let $T = \varphi(t) \in End_k(V)$

Then $\varphi(a_0 + a_1 t + \cdots + a_n t^n) = a_0 + a_1 T + \cdots + a_n T^n$

$\therefore$ φ is completely determined by T.

Suppose V' is another such $k[t]$-module. $\psi : k[t] \to \operatorname{End} W$

Let $\mathcal{X} : V \to W$ be a $k[t]$-module isomorphism.

for $\alpha \in k$

$$\mathcal{X}(\alpha \vec{v}) = \mathcal{X}(\varphi(\alpha)\vec{v}) = \psi(\alpha)\,\mathcal{X}(\vec{v}) = \alpha\,\mathcal{X}(\vec{v})$$

$$\therefore \mathcal{X} \in \operatorname{Hom}_k(V, W). \qquad \mathcal{X} \circ T = T' \circ \mathcal{X}$$

$\therefore$ {Isomorphism classes of finitely generated torsion R-modules}

$\updownarrow$ bijective

$$\{(V,T)\} \Big/ \; (V,T) \sim (V',T') \text{ if } \exists\, \mathcal{X} \in \operatorname{Iso}_k(V,V') \ni \mathcal{X}\circ T = T'\circ \mathcal{X}$$

$\updownarrow$ bijective

$$M_{n,n}(k) \Big/ \; A \sim A' \text{ if } \exists\, X \in GL_n(k) \ni XA = A'X$$

$\parallel$

Similarity classes of $n \times n$ matrices over k.

Defn: $A, A' \in M_n(k)$, then A is similar to A' if $\exists$ $X \in GL_n(k) \ni XA = A'X$.

Conclusion: The classification of finitely generated $k[t]$ modules is equivalent to the classification of similarity classes of $n \times n$ matrices with entries in k.

Some examples of the correspondence:

1. $p(t) \in k[t]$ $d = \deg(p(t))$.

   $M = k[t]/p(t)$

   Take as basis of M : $\{1, t, t^2, \dots, t^{d-1}\}$.

   $k[t] \to \mathrm{End}_k(M)$

   $t \mapsto$ multiplication by t.

$$1 \mapsto t$$
$$t \mapsto t^2$$
$$t^{d-2} \mapsto t^{d-1}$$
$$t^{d-1} \mapsto t^d$$

Suppose $p(t) = a_0 + a_1 t + \dots + a_d t^d$, $a_d \neq 0$.

can assume $a_d = 1$, $p(t)$ is monic.

In M, $p(t) = 0$

$$a_0 + a_1 t + \dots + a_{d-1} t^{d-1} + t^d = 0$$

so $t^d = -a_0 - a_1 t - \dots - a_{d-1} t^{d-1}$

So w.r.t. the basis $\{1, t, \dots, t^{d-1}\}$ the matrix of T is:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix} =: C_{p(t)}$$

the companion matrix of $p(t)$

Under the correspondence:

{Finitely gen. torsion $k[t]$-modules} $\longleftrightarrow$ {Similarity classes of matrices}.

$$k[t]/p(t) \longleftrightarrow C_{p(t)}$$

$$\chi_{C_{p(t)}}(t) = p(t) \quad \therefore \; C_{p(t)} \sim C_{q(t)} \Leftrightarrow p(t) = q(t).$$

(2) $M \longleftrightarrow A$

$M' \longleftrightarrow A'$

$M \oplus M' \longleftrightarrow \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}$

__Theorem__ (test for similarity of matrices over a field)

Let k be any field, $A, B \in M_n(k)$.

Then A is similar to B if and only if the matrices $\lambda I - A$ is equivalent $\lambda I - B$ in $M_n(k[\lambda])$.

__Proof:__ $\Rightarrow$ Suppose $A \sim B$. Then $\exists\, X \in M_n(k)$ invertible $\ni AX = XB$.

Then $(\lambda I - A)X = X(\lambda I - B)$

Moreover, $X \in M_n(k[\lambda])$ is invertible.

$\therefore$ $\lambda I - A$ is similar to $\lambda I - B$.

$\Leftarrow$ There is a unique $k[\lambda]$-module homomorphism

$$\eta : k[\lambda]^n \longrightarrow k^n$$

which sends $\lambda e_i \longmapsto A e_i \cdot \; i = 1, \dots, n$

Let $K = \ker(\eta)$ ← free $k[\lambda]$ module of rank $\leq n$.

<u>Lemma</u>: The elements $f_i = \lambda e_i - \sum_{j=1}^{n} a_{ij} e_j \quad 1 \leq i \leq n$

form a base for K.

<u>Proof</u> $\eta(f_i) = Ae_i - \sum_{j=1}^{n} a_{ij} e_j = 0$.

$\therefore f_i \in K$ for $1 \leq i \leq n$

Suppose $\sum_{i=1}^{n} h_i(\lambda) f_i = 0$.

If any of the $h_i(\lambda)$'s is non-zero, then pick the non-zero $h_i(\lambda)$ with highest degree, call the degree d.

Coeff of λ^{d+1} in

$$\sum_{i=1}^{n} h_i(\lambda) f_i = \sum_{i=1}^{n} h_i(\lambda)\left(\lambda e_i - \sum a_{ij} e_j\right)$$

is $\sum_{i=1}^{n} h_i^{(d)} e_i$.

where $h_i^{(d)}$ is the coeff of λ^d in $h_i(\lambda)$.

$\therefore h_i^{(d)} = 0 \quad \forall\, i = 1, \ldots, n$, a contradiction.

$$g_i(\lambda) = \lambda h_i(\lambda) + b_i$$

$$g_i(\lambda) e_i = h_i(\lambda) \lambda e_i + b_i e_i$$

$$= h_i(\lambda)\left(\lambda e_i - \sum_{j=1}^{n} a_{ij} e_j\right) + b_i e_i$$

(22)

$$\therefore \sum_{i=1}^{n} g_i(\lambda) e_i = \sum_{i=1}^{n} \Big[h_i(\lambda) f_i + \underbrace{\Big(b_i - \sum_{j=1}^{n} a_{ij}\Big) e_i}_{b_i' e_i} \Big]$$

If $\sum_{i=1}^{n} g_i(\lambda) e_i \in K$,

then $\sum b_i' e_i \in K$

$$\therefore \sum_{i=1}^{n} g_i(\lambda) e_i = \sum_{i=1}^{n} h_i(\lambda) f_i \qquad \text{QED}.$$

$\therefore$ when k^n is thought of as $\eta(k[\lambda]^n)$, then the matrix of relations is $\lambda I - A$.

If $\lambda I - A$ is equivalent to $\lambda I - B$, then the $k[t]$-modules corresponding to A and B will be isomorphic.

<u>Corollary</u>. $A \sim B$ iff $\Delta_i(\lambda I - A) = \Delta_i(\lambda I - B)$ for all $i = 1, 2, \ldots, n$

[Recall that $\Delta_i(\lambda I - A) \in k[\lambda]$ is the ith invariant factor of $\lambda I - A \in M_n(k[\lambda])$]

We have $k^n = k[\lambda]z_1 \oplus \cdots \oplus k[\lambda] z_n$

where $\operatorname{ann}(z_i) = i$th invariant factor of $\lambda I - A$

The sequence of order ideals is of the form
$\{1, 1, \ldots, 1, d_1, \ldots, d_s\}$ $(1) \supsetneq (d_1) \supset (d_2) \supset \cdots \supset (d_s)$

$$\therefore \quad A \sim \begin{pmatrix} C_{d_1(t)} & & 0 \\ & \ddots & \\ 0 & & C_{d_s(t)} \end{pmatrix} \qquad (*)$$

where $d_i(t)$ is the ith invariant factor of $\lambda I - A$.

Lecture IV

Defn. (minimal polynomial)

The minimal polynomial of $A \in M_n(k)$ is the unique monic polynomial $m_A(x)$ for which

$$(m_A(t)) = \{ p(t) \in k[t] \mid p(A) = 0 \}$$

<u>Computation of the minimal polynomial:</u>

Observe that $p(A_1 \oplus A_2) = p(A_1) \oplus p(A_2)$

$\therefore \; p(A_1 \oplus A_2) = 0 \iff p(A_1) = 0$ and $p(A_2) = 0$.

$\therefore \; (m_{A_1 \oplus A_2}(t)) = (m_{A_1}(t)) \cap (m_{A_2}(t))$

Consequently in $(*)$,

$$m_A(t) = d_s(t) = \Delta_n(\lambda I - A)$$

$$= \frac{\det(\lambda I - A)}{\gcd \text{ of } (n-1)\times(n-1) \text{ minors of } \lambda I - A}$$

<u>Interpretation of primary decomposition:</u>

<u>Recall</u>: $M = \bigoplus_p M_p$

$$M_p \cong R/_{p^{\lambda_1}} \oplus \cdots \oplus R/_{p^{\lambda_\ell}} \qquad \lambda_1 \leq \cdots \leq \lambda_\ell.$$

For matrices, this means:

$$A \sim \bigoplus_p A_p$$

where $A_p \sim J_{\lambda_1}(p) \oplus \dots \oplus J_{\lambda_\ell}(p)$

Here $J_{\lambda_i}(p) = \begin{pmatrix} C_{p(x)} & & & O \\ M & C_{p(x)} & & \\ & M & \ddots & \\ O & & M & C_{p(x)} \end{pmatrix}_{d\lambda \times d\lambda}$ $\quad M = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & O & & \vdots \\ & & & 0 \end{pmatrix}_{d \times d}$

Generalised Jordan canonical form

$d = \text{degree } p$

To see this, take the basis

$e_{0,0}, e_{0,1}, \dots, e_{0,d-1}, e_{1,0}, e_{1,1}$

$1, x, \dots, x^{d-1}, p(x), xp(x), \dots, x^{d-1}p(x), p(x)^2, xp(x)^2, \dots, x^{d-1}p(x)^2,$

$\dots, p(x)^{\lambda-1}, xp(x)^{\lambda-1}, \dots, x^{d-1}p(x)^{\lambda-1}$

$$x^d = x^d - p(x) + p(x)$$
$$= -a_0 e_{0,0} - a_1 e_{0,1} - \dots - a_{d-1} e_{0,d-1} + e_{1,0}$$

Computation of centralisers

Defn (Centraliser of a matrix)

The centraliser of a matrix $T \in M_n(k)$ is the ring

$$Z(T) = \{ A \in M_n(k) \mid AT = TA \}$$

Recall: Can use T to define a $k[t]$-module structure on k^n:

$$t \cdot \vec{v} = T\vec{v}.$$

Fundamental lemma:

For any $A \in Z(T)$, the map $\varphi_A : \vec{x} \mapsto A\vec{x}$, $k^n \to k^n$ is a $k[t]$-module homomorphism.

$$A \mapsto \varphi_A$$

is an isomorphism $Z(T) \to \mathrm{End}_{k[t]}(k^n)$ of rings.

Proof: Suppose $A \in Z(T)$

$$\varphi_A(t\vec{v}) = \varphi_A(T\vec{v}) = AT\vec{v}$$
$$= TA\vec{v} = t\varphi_A(\vec{v})$$

$\therefore \varphi_A \in \mathrm{End}_{k[t]}(k^n)$

Conversely, suppose $\varphi \in \mathrm{End}_{k[t]}(k^n)$, then

$$\varphi(\vec{v}) = A_\varphi \vec{v} \quad \forall \vec{v} \in k^n$$

for some $A_\varphi \in M_n(k)$.

$$\varphi(t\vec{v}) = A_\varphi T\vec{v}$$
$$\| $$
$$t\varphi(\vec{v}) = TA_\varphi \vec{v}.$$

$\therefore A_\varphi \in Z(T)$

The maps $A \mapsto \varphi_A$ and $\varphi \mapsto A_\varphi$ are clearly homomorphism of rings and are mutual inverses.

<u>Lemma</u>: Suppose R is a p.i.d, and $p, q \in R$ are such that $(p,q)=1$. Then $\mathrm{Hom}_R(R/(p), R/(q))=0$.

<u>Proof</u>: Suppose $\varphi \in \mathrm{Hom}_R(R/(p), R/(q))$

$\varphi(1+(p)) = a_\varphi + (q)$ for some $a_\varphi \in R$.

$0 = \varphi(0) = \varphi(p(1+(p))) = p\varphi(1+(p)) = pa_\varphi + (q)$

$\therefore pa_\varphi \in (q)$

Since $(p,q)=1$ $pa_\varphi \in (q) \Rightarrow a_\varphi \in q \Rightarrow \varphi \equiv 0$. QED.

<u>Corollary</u>: Suppose $M = \bigoplus_p M_p$ (primary decomposition) is a torsion module over a PID R, then

$$\mathrm{End}_R(M) = \bigoplus_p \mathrm{End}_R(M_p).$$

<u>Some notation</u>: $\lambda = (\lambda_1 \geq \dots \geq \lambda_\ell)$ Young diagram.

k some field.

Then $k^\lambda = k[t]/(t^{\lambda_1}) \oplus \cdots \oplus k[t]/(t^{\lambda_\ell})$

a $k[t]$-module.

<u>e.g.</u> $\lambda = (\underbrace{1, \dots, 1}_{n\text{-times}}) =: (1^n)$

$k^{(1^n)} = k^n$

$\lambda = (m, \dots, m) =: (m^n)$

$k^{(m^n)} = (k[t]/(t^m))^n$.

$$G_\lambda(k) := \mathrm{End}_{k[t]} k^\lambda$$

e.g. $G_{(1^n)}(k) = GL_n(k)$

$$G_{(m^n)}(k) = GL_n(k[t]/t^m).$$

Calculation of $\mathrm{End}_{k[t]} M_p$: Let M be a finitely generated torsion $k[t]$-module

Recall that $M = \bigoplus_{p(t)} M^\lambda_{p(t)}$ ($\lambda = \lambda_p$ depends on p)

$$M^\lambda_{p(t)} \cong k[t]/p(t)^{\lambda_1} \oplus \cdots \oplus k[t]/p(t)^{\lambda_\ell}$$

(here $p(t)$ is an irreducible monic polynomial, of degree d).

We wish to calculate $\mathrm{End}_{k[t]} M^\lambda_{p(t)}$.

Lemma: Let $p(t)$ be an irreducible monic polynomial with coefficients in k. Let $E = k[t]/p(t)$. Then the rings $k[t]/(p(t)^r)$ & $E[u]/(u^r)$ are isomorphic (in characteristic 0)

Proof: $E[u]/(u^r) = k[t,u]/(p(t), u^r) \xrightarrow{\text{want}} k[t]/(p(t)^r)$ $\quad t \longmapsto ?$

Lemma (Hensel): $\exists\, q(t) \in k[t]/(p(t)^r)$ such that $q(t) \equiv t \mod p(t)$ and $p(q(t)) = 0$.

(28)

Motivation: This is another case of a type of result that was first discovered by Hensel in the context of Diophantine equations:

Suppose $p(t) \in \mathbb{Z}[t]$, $p(a_1) \equiv 0 \pmod p$, and $p'(a_1) \not\equiv 0 \pmod p$. Then $\exists$ a sequence $\{a_n\}$ of integers such that $a_{n+1} \equiv a_n \pmod{p^n}$ and $p(a_n) \equiv 0 \pmod{p^n}$

Proof: $p(a_1+ph) = p(a_1) + ph\, p'(a_1) + \frac{p^2h^2}{2!} p''(a_1) + \cdots$

$p'(a_1) \not\equiv 0 \pmod p$ so it is possible to solve the congruence

$$p(a_1) + ph\, p'(a_1) \equiv 0 \pmod{p^2}$$

Let $a_2 = a_1 + ph$, where h is a solution.

Can continue in this manner to obtain the sequence $\{a_n\}$, which is called a p-adic solution to the equation $p(t) = 0$.

<u>Defn</u>: Let k be a field of characteristic p. k is said to be <u>perfect</u> if $x \mapsto x^p$ is an automorphism of k.

<u>Example</u> ① $k = \mathbb{F}_{q^n}$

$$k^\times \cong \mathbb{Z}/(q^n-1)\mathbb{Z}$$

Since $(q^n-1, p) = 1$, p is a unit in $\mathbb{Z}/(q^n-1)\mathbb{Z}$, hence $x \mapsto x^p$ is an automorphism

② $k = \mathbb{F}_{q^n}((t))$ [Laurent series in $\mathbb{F}_{q^n}$]

t has no p-th root.

k is not perfect.

<u>Lemma</u>: Let k be a perfect field. Let $\bar{x} \in k[t]/p(t)$ denote the image of $x \in k[t]/p(t)^r$.

$\exists$ a ring homomorphism $s : k[t]/p(t) \to k[t]/p(t)^r$ such that $\overline{s(y)} = y \ \forall\ y \in k[t]/p(t)$.

<u>Proof</u>: Given $y \in k[t]/_{p(t)}$, consider y^{1/p^m}, where m is so large that $p^m > r$.

If $\bar{x}_1 = \bar{x}_2 = y$, then $x_1 - x_2 \equiv 0 \bmod p(t)$

$\therefore x_1^{p^m} - x_2^{p^m} = (x_1 - x_2)^{p^m} \equiv 0 \bmod p(t)^r$

$\therefore x_1^{p^m} = x_2^{p^m}$.

So if s exists, it must have $s(y) = x^{p^m}$, where $x \in k[t]/_{p(t)^r}$ is any element for which

$\bar{x} = y^{1/p^m}$

($s(y)$ will not depend on the choice of x)

$$s(x_1)\, s(x_2) = y_1^{p^m} y_2^{p^m}, \text{ where } \bar{y}_i = x_i^{1/p^m}$$

$$= (y_1 y_2)^{p^m}$$

$$= s(x_1 x_2), \text{ since } \overline{y_1 y_2} = \bar{y}_1 \bar{y}_2 = x_1^{1/p^m} x_2^{1/p^m} = (x_1 x_2)^{1/p^m}.$$

$\therefore s$ is multiplicative,

$$s(x_1) + s(x_2) = y_1^{p^m} + y_2^{p^m}$$

$$= (y_1 + y_2)^{p^m}$$

$$= s(x_1 + x_2), \text{ since } \overline{y_1 + y_2} = \bar{y}_1 + \bar{y}_2$$

and $(\bar{y}_1 + \bar{y}_2)^p = \bar{y}_1^p + \bar{y}_2^p = x_1 + x_2$.

the image of this homomorphism.

As k vector spaces, both rings have dimension rd.

$\therefore$ it is an isomorphism.

Lecture V

Theorem $Z(T)$ is isomorphic to a product of groups of the form $G_\lambda(E)$ where λ is a Young diagram and E is a finite extension of k.

Proof:
$$Z(T) = \mathrm{End}_{k[t]}(k^n)$$
$$= \mathrm{End}_{k[t]}\Big(\bigoplus_{p(t)} (k^n)_{p(t)}\Big)$$
$$= \prod_{p(t)} \mathrm{End}_{k[t]}(k^n)_{p(t)}$$
$$= \prod_{p(t)} \mathrm{End}_{k[t]}\Big(k[t]/(p(t)^{\lambda_1}) \oplus \cdots \oplus k[t]/(p(t)^{\lambda_\ell})\Big)$$

Now:
$$\mathrm{End}_{k[t]}\; k[t]/(p(t)^{\lambda_1}) \oplus \cdots \oplus k[t]/(p(t)^{\lambda_\ell})$$
$$= \mathrm{End}_{k[t]/(p(t)^{\lambda_1})}\; k[t]/(p(t)^{\lambda_1}) \oplus \cdots \oplus k[t]/(p(t)^{\lambda_\ell})$$
$$= \mathrm{End}_{E[u]/(u^{\lambda_1})}\; E[u]/(u^{\lambda_1}) \oplus \cdots \oplus E[u]/(u^{\lambda_\ell})$$

Proof of Hensel's Lemma:

Induct on r.

Suppose $r = 1$.

Can take $q(t) = t$.

Now suppose $q_{r-1}(t) \in k[t]$ is such that

$$q_{r-1}(t) \equiv t \mod p(t)$$

and $p(q_{r-1}(t)) \in (p(t))^{r-1}$.

Then $p(q_{r-1}(t) + p(t)^{r-1} h(t))$

$$= p(q_{r-1}(t)) + p(t)^{r-1} h(t) p'(q_{r-1}(t)) + \text{h.o.t.}$$

$p'(q_{r-1}(t)) \equiv p'(t) \mod p(t)$, [since $q_{r-1}(t) \equiv t \mod p(t)$]

$\therefore$ ~~one~~ the congruence

$$p(q_{r-1}(t)) + p(t)^{r-1} h(t) p'(q_{r-1}(t)) \equiv 0 \mod p(t)^r$$

has a solution $h_0(t)$.

Set $q_r(t) = q_{r-1}(t) + p(t)^{r-1} h_0(t)$.

Define a ring homomorphism

$$k[t,u] / (p(t), u^r) \longrightarrow k[t] / p(t)^r$$

by $t \mapsto q(t)$ and $u \mapsto p(t)$

It is surjective, because $t = q(t) + ?\, p(t)$ lies in

$$= \mathrm{End}_{E[u]} E^{\lambda}$$

$$= G_{\lambda}(E) \qquad \text{QED}$$

Features of modules:

Definition (Irreducibility)

An R-module M is said to be irreducible if M has no non-trivial proper R-stable subgroups

Definition (Indecomposable)

An R-module M is said to be indecomposable if M is not isomorphic to a direct sum of two non-trivial R-modules.

Remark: A matrix $T \in M_n(k)$ will be said to be irreducible, indecomposable, etc, if the corresponding $k[t]$-module structure on k^n is respectively, irreducible, indecomposable, etc.

Example:

- All irreducible matrices are similar to $C_{p(t)}$, where $p(t)$ is an irreducible polynomial
- All indecomposable matrices are similar to $C_{p(t)^r}$ where $p(t)$ is irred., $r \geqslant 2$ is an integer.

These are given by the generalised Jordan canonical form

$$J_r(p) = \begin{pmatrix} C_{p(t)} & & & \mathbb{O} \\ \mathbb{I} & C_{p(t)} & & \\ & \mathbb{I} & \ddots & \\ \mathbb{O} & & \mathbb{I} & C_{p(t)} \end{pmatrix}_{rd \times rd} \qquad \mathbb{I} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & \bigcirc & & \vdots \\ & & & 0 \end{pmatrix}_{d \times d}$$

Invariant subspaces:

$$\langle e_1, \dots, e_d \rangle \longleftrightarrow J_1(p)$$

$$\langle e_1, \dots, e_{2d} \rangle \longleftrightarrow J_2(p)$$

$$\langle e_1, \dots, e_{(r-1)d} \rangle \longleftrightarrow J_{r-1}(p) \text{ maximal invariant subspace}$$

<u>Theorem</u> (Schur's Lemma)

If M is a simple R-module, then $\mathrm{End}_R M$ is a division ring.

<u>Proof</u>: $\varphi: M \to M$ be a non-zero R-module homomorphism.

Then $\mathrm{Im}\,\varphi$ & $\ker\varphi$ are R-stable subgroups of M

$\therefore \mathrm{Im}\,\varphi = M$

$\quad \ker\varphi = 0$

Hence φ is a bijection.

Its set theoretic inverse is also an R-module homomorphism.

<u>Example</u>: T irreducible, then $Z(T) = k[t]/p(t)$ { algebraic field extension.

char. poly of T

Generalised Jordan canonical form:

Let $\theta(t) = t - q(t)$

Then $\theta(t) \in (p(t))$ [$\because \theta(t) \equiv t \pmod{p(t)}$]

But $\theta(t) \notin (p(t)^2)$,

for if it did, then

$$p(t) = p(\theta(t) + q(t)) = p(q(t)) + \theta(t)\, p'(q(t)) + \cdots$$

$$\equiv 0 \pmod{p(t)^2}.$$

$\Rightarrow\Leftarrow$

$\therefore$ $\theta(t) = \alpha\, p(t)$, where α is a unit.

In $\left(k[x]/_{p(x)}\right)[u]/_{(u^r)} \longleftrightarrow k[t]/_{(p(t)^r)}$

$$x \longleftrightarrow q(t)$$

$$\alpha u \longleftrightarrow \theta(t)$$

Some unit

In $\left(k[x] / p(x) \right)[u] / (u^r)$, the set

$$\{ (\alpha u)^j x^i \mid 0 \le j \le r-1, 0 \le i \le d-1 \}$$

is a k-basis.

$\therefore$ the set

$\{ \theta(t)^j q(t)^i \mid 0 \le j \le r-1, 0 \le i \le d-1 \}$ is a k-basis in $k[t] / p(t)^{r-1}$.

$$t\,\theta(t)^j q(t)^i = \theta(t)^{j+1} + q(t)^{i+1}$$

If $i = d-1$,

$$t\,\theta(t)^j q(t)^i = \theta(t)^{j+1} + q(t)^d$$

$$= \theta(t)^{j+1} - a_0 - a_1 q(t) - \cdots - a_{d-1} q(t)^{d-1}$$

If $j = r-1$,

$$t\,\theta(t)^{r-1} q(t)^i = \underbrace{\theta(t)^r}_{\in p(t)^r} + q(t)^{i+1}$$

$$= 0 + q(t)^{i+1}$$

So the matrix of multiplication by t is given by

$$J_p(\lambda) = \begin{pmatrix} C_p & & & 0 \\ I & C_p & & \\ & I & \ddots & \\ 0 & & I & C_p \end{pmatrix}$$

which will be called a Jordan block.

<u>Theorem:</u> Every matrix over a separable field is similar to a direct sum of Jordan blocks, which are uniquely determined up to a rearrangement.

This is the generalised Jordan canonical form of a matrix.

Defn (Semisimplicity):

An R-module [matrix] is said to be semisimple if it is a direct sum of simple R-modules. [matrices]

Example: $J_r(p) = \begin{pmatrix} C_p(t) & & 0 \\ I & \ddots & \\ 0 & I & C_p(t) \end{pmatrix}$ is not semisimple

Theorem: The following are equivalent for $A \in M_n(k)$

(1) A is semisimple

(2) m_A is square-free

(3) The Jordan canonical form of A consists only of blocks of size 1

(4) $Z(A)$ is a direct sum of matrix rings.

Example: $T = J_r(p) = \begin{pmatrix} C_p & & 0 \\ I & \ddots & \\ 0 & I & C_p \end{pmatrix}$.

Recall that $\exists\ q(t) \in k[t] \ni q(t) \equiv t \mod p(t)$ and $p(q(t)) \equiv 0 \mod p(t)^r$.

$\therefore\ p(q(T)) = 0 \Rightarrow m_{q(T)}(t) \mid p(t)$

Since $p(t)$ is irreducible $m_{q(T)}(t) = p(t)$

$\therefore\ q(T)$ is semisimple

Remark: Matrix of $q(t)$ is $C_p \oplus C_p \oplus \cdots \oplus C_p$.

34

<u>Defn</u> (nilpotent):
A matrix A (resp linear transfmn) is <u>nilpotent</u> if $A^n = 0$ for some $n \in \mathbb{N}$.

<u>Lemma</u>: Suppose A is semisimple and $f \in k[t]$ is such that $f(A)$ is nilpotent, then $f(A) = 0$.

<u>Proof</u>: $f(A)^n = 0$

$\Longrightarrow m_A(t) \mid f(t)^n$

$\Longrightarrow m_A(t) \mid f(t)$

$\Longrightarrow f(A) = 0$

<u>Theorem:</u> The following are equivalent:

1. A is cyclic
2. $m_A = \chi_A$
3. $Z(A) = k[A]$

<u>Pf.</u> Consider the rational canonical form:

$$k^n \cong k[t]/p_1(t) \oplus \cdots \oplus k[t]/p_r(t).$$

$$p_1(t) \mid p_2(t) \mid \cdots \mid p_r(t).$$

A is cyclic iff $r = 1$ (Invariance theorem)

<u>① ⟺ ②</u> : Note that $m_A \mid \chi_A$.

$$\therefore \ m_A = \chi_A \iff \underset{\substack{\| \\ \deg p_r(t)}}{\deg m_A} = \underset{\substack{\| \\ n}}{\deg \chi_A}.$$

But $\deg p_r(t) = n$ iff $r = 1$

① ⟹ ③ Suppose A is cyclic

$$Z(A) \cong \mathrm{End}_{k[t]} k^n \cong k[t]/p(t)$$

$\therefore$ every element of $Z(A)$ is a poly. in t.

③ ⟹ ① Suppose A is not cyclic. Then $r > 1$.

Suppose $q(t) \in k[t]$.

Then $q(t)\big|_{k[t]/p_i(t)} = 0 \Rightarrow q(t) \in (p_i(t))$.

$\therefore q(t)\big|_{k[t]/p_r(t)} \equiv 0 \Rightarrow q(t)\big|_{k[t]/p_{r-1}(t)} \equiv 0 \Rightarrow \cdots$

Let E be the projection onto $k[t]/p_{r-1}(t)$.

Then $E\big|_{k[t]/p_{r-1}(t)} \not\equiv 0$ but $E\big|_{k[t]/p_r(t)} \equiv 0$

$\therefore E \neq q(t)$ for any $q(t) \in k[t]$.

However, $E \in \mathrm{End}_{k[t]} k^n = Z(A)$.

<u>Application to the Jordan Canonical form:</u>

<u>Theorem:</u> Suppose $A = S + N$, where S is s.s., N is nilpotent, and $SN = NS$.

Then $S, N \in k[A]$.

<u>Proof:</u> <u>Cyclic case:</u> theorem is true because $S, N \in Z(A)$

<u>Primary case:</u> $A = A_p$

$$A \sim J_{\lambda_1}(p) \oplus \cdots \oplus J_{\lambda_\ell}(p)$$

$$\lambda_1 \leq \cdots \leq \lambda_\ell.$$

<u>Proposition</u> (Invariance of semisimplicity & nilpotence under field extension)

Let k be a perfect field, and $E/_k$ be a finite extension. An identification $E = k^d$ as k-vector spaces gives an embedding

$$M_{\frac{n}{d}}(E) \hookrightarrow M_n(k) \quad \forall\, n \ni d \mid n.$$

Let $X \in M_{\frac{n}{d}}(E)$.

Then X is semisimple (resp. nilpotent) in $M_n(k)$ iff X is semisimple (resp. nilpotent) in $M_{\frac{n}{d}}(E)$.

<u>Proof</u>:

<u>Lemma</u>: ~~Let~~ If $p(t) \in k[t]$ square-free then $p(t)$ is square-free in $E[t]$.

<u>Pf</u>: $p_0(t)$ irr., then $(p_0(t), p_0'(t)) = 1$ in $k[t]$, hence in $E[t]$. $\therefore p_0(t)$ sq. free in $E[t]$

$p(t) = p_1(t) \dots p_k(t)$, then each is sq. free, and they the distinct irreducibles have no common factors.

Lemma: $a \in E$, $S \in M_n(E)$

S is semisimple iff $S - aI$ is semisimple

Proposition: Suppose $A = A_p$, then the Jordan decomposition of A is unique.

Proof: $A = J_{\underline{\lambda}}(p)$ $\qquad \underline{\lambda} = (\lambda_1 \leq \dots \leq \lambda_\ell)$.

$$J_{\underline{\lambda}}(p) = \begin{pmatrix} J_{\lambda_1}(p) & 0 \\ 0 & J_{\lambda_\ell}(p) \end{pmatrix}$$

$A = S + N \qquad S, N \in Z(A)$

Then $S, N \in GL_{\underline{\lambda}}(E) = Z(J_{\underline{\lambda}}(0)) \subset M_n(E)$

$$A = q(t) I + J_{\underline{\lambda}}(0)$$

$$A = S + N$$

$$\therefore \underbrace{q(t) I - S}_{\text{s.s.}} = \underbrace{N - J_\lambda(0)}_{\text{nilpotent}}.$$

$$\therefore q(t) I - S = N - J_\lambda(0) = 0.$$

36 3

Claim: If $q(J_r(p)) = C_p^{\oplus r}$ and $s \leq r$, then

$$q(J_s(p)) = C_p^{\oplus s}$$

Pf: $J_s(p)$ is the matrix by which $J_r(p)$ acts on the subspace spanned by $e_1, \dots, e_{sd}$.

General case: $A = \bigoplus A_p$

suppose $q_p(A_p)$ is the semisimple part S_p of A_p

The minimal polynomial of A_p is $p(t)^{r_p}$ for some $r_p \in \mathbb{N}$.

Let $q \in k[t]$ be such that

$$q(t) \equiv q_p(t) \mod p(t)^{r_p} \quad \forall p$$

(this exists by the Chinese Remainder theorem)

$$q(A) = \bigoplus q(A_p) = \bigoplus q_p(A_p) + \cancel{(p(A)^{r_p}) \cdot \text{stg}}$$

$$= \bigoplus S_p = S \quad \text{QED}$$

$S = q(A) \quad N = A - q(A)$.

38

<u>Theorem</u> (Jordan Decomposition Theorem) k perfect.

For every $A \in M_n(k)$, $\exists!$ $S, N \in M_n(k)$ such that S is semisimple, N is nilpotent, $SN = NS$ and $A = S + N$.

S and N determined by the above conditions are polynomials in A.

<u>Proof</u>: Only need to prove the uniqueness.

Suppose $A = S + N = S' + N'$, S, S' s.s., N, N' nilp., ~~S,N~~ $SN = NS$ and $S'N' = N'S'$.

Then S, N, S', N' are all polynomials in A, hence they all commute.

$\therefore \quad S' = S + (N - N')$

Since N, N' commute, and are nilpotent

$(N - N)'$ is nilpotent,

(because $(N-N')^n = N^n - \binom{n}{1} N^{n-1}N' + \cdots + (-1)^{n-1}\binom{n}{n-1} N N'^{n-1} + (-1)^n N'^n$

In this expansion at least one of N & N' has power $\geq \frac{n}{2}$.]

$\therefore (N - N') = q(S')$ by Lemma.

$\Rightarrow \quad N - N' = 0$

$\therefore S = S'$ and $N = N'$.

<u>Theorem</u>: Suppose $A \in M_n(k)$ is semisimple & $f(t) \in k[t]$, then $f(A)$ is also semisimple.

<u>Proof</u>: Suppose $f(A) = S + N$ (Jordan decompo.)

$N = g(f(A))$ for some $g(t) \in k[t]$

$\Rightarrow N = 0$.

R any ring (possibly non-unital)

<u>Defn</u> (Noetherian module)

An R-module M is called <u>Noetherian</u> if it satisfies the descending chain condition:

For every family $M \supset M_1 \supset M_2 \supset \cdots$ of submodules,

$\exists\, N \in \mathbb{N} \ni M_n = M_{n+1} \ \forall\, n > N$

<u>Defn</u> (Artinian module)

An R-module M is called <u>Artinian</u> if it satisfies the ascending chain condition:

For every family $0 \subset M_1 \subset M_2 \subset \cdots$ of submodules

$\exists\, N \in \mathbb{N} \ni M_n = M_{n+1} \ \forall\, n > N$

Suppose $u \in \operatorname{End}_R M$, M Noetherian.

$$\operatorname{Im} u \supset \operatorname{Im} u^2 \supset \cdots$$

must stabilize. Let $\operatorname{Im} u^\infty := \bigcap_{i=1}^{\infty} \operatorname{Im} u^i$.

Then $\exists\, n \in \mathbb{N} \ni \operatorname{Im} u^\infty = \operatorname{Im} u^n$.

Suppose $u \in \operatorname{End}_R M$, M Artinian

$$\ker u \subset \ker u^2 \subset \cdots$$

must stabilize. Let $\ker u^\infty := \bigcup_{i=1}^{\infty} \ker u^i$

$\exists\, n \in \mathbb{N} \ni \ker u^\infty = \ker u^n$

Theorem (Fitting)

Suppose an R-module M is both Noetherian and Artinian. Then

$$M = \operatorname{Im} u^{\infty} \oplus \ker u^{\infty}.$$

Proof: Let $n \in \mathbb{N}$ be such that $\operatorname{Im} u^{\infty} = \operatorname{Im} u^{n}$ and $\ker u^{\infty} = \ker u^{n}$.

- If $x \in \operatorname{Im} u^{\infty} \cap \ker u^{\infty}$,

  then $x = u^{n}(y)$ for some $y \in M$

  $u^{2n}(y) = 0 \Rightarrow y \in \ker u^{2n} = \ker u^{n}$

  $\therefore x = u^{n}(y) = 0$

- Suppose $x \in M$.

  $u^{n}(x) = u^{2n}(y)$ for some $y \in M$

  $$x = \underbrace{x - u^{n}(y)}_{\in \ker u^{\infty}} + \underbrace{u^{n}(y)}_{\in \operatorname{Im} u^{\infty}}$$

Defn (local ring)

A ring R is said to be local if its set of non-units forms a two-sided ideal.

* Proposition: If M is an indecomposable Noetherian and Artinian R-module, then

① every element of $\mathrm{End}_R M$ is either an automorphism or is nilpotent.

② $\mathrm{End}_R M$ is local

Proof: Let $u \in \mathrm{End}_R M$.

By Fitting's lemma: $M = \mathrm{Im}\, u^\infty \oplus \ker u^\infty$

M indecomposable $\Rightarrow$ either ① $\mathrm{Im}\, u^\infty = M \Rightarrow u$ automorphism
② $\ker u^\infty = M \Rightarrow u$ nilpotent.

Suppose u is not a unit, so u is nilpotent.

$\therefore$ u is not surjective $\Rightarrow uv$ is not surj. $\forall v \in \mathrm{End}_R M$
$\Rightarrow uv$ is nilpotent

u is not injective $\Rightarrow vu$ is not injective $\forall v \in \mathrm{End}_R M$
$\Rightarrow vu$ is nilpotent

Suppose u_1 & u_2 are not units, but $u_1 + u_2$ is a unit.

Let $v_1 = u_1(u_1+u_2)^{-1}$ $\quad v_2 = u_2(u_1+u_2)^{-1}$.

Then $v_1 + v_2 = 1$, so $v_2 = 1 - v_1$

v_1 is nilpotent so $1 - v_1$ is a unit.

$\Rightarrow v_2$ is a unit $\Rightarrow\Leftarrow$.

rephrase:

* Proposition: Let M be a Noetherian and Artinian R-module. Then the following are equivalent: ① M is indecomposable
② every element of $\mathrm{End}_R M$ is either an automorphism or is nilpotent
③ $\mathrm{End}_R M$ is local.

<u>Theorem</u> (Krull-Remak-Schmidt)

Let $M \neq 0$ be an R-module which is Noetherian and Artinian. Then E is a finite direct sum of indecomposable R-modules. Up to permutation the indecomposable direct summands are uniquely determined.

<u>Proof:</u> The existence of a direct sum decomposition into indecomposables follows from the Artinian cond.

For uniqueness, suppose

$$M = E_1 \oplus \cdots \oplus E_r = F_1 \oplus \cdots \oplus F_s$$

are two such decompositions.

$id_M : M \to M$ can be represented by a matrix

$$A = (a_{ij})_{s \times r} \qquad a_{ij} : E_j \to F_i$$

& $$B = (b_{ij})_{r \times s} \qquad b_{ij} : F_j \to E_i$$

$$AB = \begin{pmatrix} id_{F_1} & & 0 \\ & \ddots & \\ 0 & & id_{F_s} \end{pmatrix}$$

$\forall i$, $id_{F_i} = a_{i1}b_{1i} + \cdots + a_{ir}b_{ri}$

$\therefore$ $a_{ij}b_{ji}$ is an automorphism for some j

Let $e_{ij} = b_{ji}(a_{ij}b_{ji})^{-1}a_{ij} : E_j \to E_j$.

Then $e_{ij}^2 = e_{ij}$ $\qquad E_j = e_{ij}E_j \oplus (1-e_{ij})E_j$

$\therefore$ $e_{ij} = id_{E_j}$ or $e_{ij} = 0$.

but $a_{ij} e_{ij} b_{ji} = a_{ij} b_{ji}$ is an automorphism

So must have $e_{ij} = id_{E_j}$

$\therefore$ a_{ij} is injective and b_{ji} is surjective.

On the other hand, since $a_{ij} b_{ji}$ is an automorphism,

a_{ij} is surjective & b_{ji} is injective

$$\therefore \left.\begin{array}{l} a_{ij} : E_j \to F_i \\ b_{ji} : F_i \to E_j \end{array}\right\} \text{ are isomorphisms.}$$

By permuting the E_i's & F_j's can assume A is of the form:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{sr} \end{pmatrix}$$

where $a_{11} : E_1 \longrightarrow F_1$ is an isomorphism.

Composing on the right with the automorphism

$$\begin{pmatrix} 1 & -a_{11}^{-1} \circ a_{12} & 0 & \cdots & 0 \\ & 1 & 0 & \cdots & 0 \\ & & 1 & & \\ & 0 & & & \end{pmatrix}$$

gives an iso $\begin{pmatrix} a_{11} & 0 & a_{13} & \cdots & a_{1r} \\ \vdots & & & & \\ a_{s1} & & & & \end{pmatrix}^{1}$

Continuing in this manner, can construct an iso

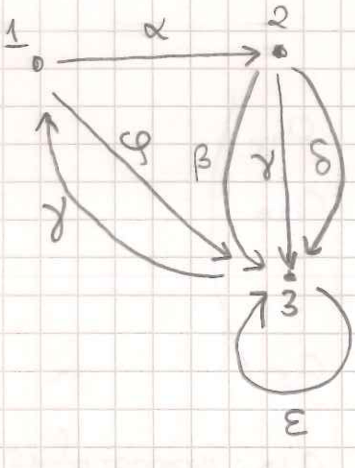
$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{s2} & \cdots & a_{sr} \end{pmatrix} : E_1 \oplus \cdots \oplus E_r \to F_1 \oplus \cdots \oplus F_s$$

Restriction to $E_2 \oplus \cdots \oplus E_r$ gives an iso to $F_2 \oplus \cdots \oplus F_s$

so can proceed by induction on $\min\{r, s\}$.

(If $\min\{r,s\} = 1$, then the statement is clear)

Quivers and path algebras:



A QUIVER

A graph — edges are directed
— multiple edges between nodes are allowed

Defn (Quiver)

A quiver is a quadruple $Q = (Q_0, Q_1, s, t)$ where

Q_0 — set of vertices

Q_1 — set of edges

$s : Q_1 \to Q_0$ starting vertex fn $t : Q_1 \to Q_0$ terminating vertex fn

Defn (Representation of a quiver)

A representation (π, V) of a quiver $Q = (Q_0, Q_1, s, t)$ over a field k consists of a collection $\{V_i \mid i \in Q_0\}$ of k-vector spaces and a collection $\{\pi_\alpha \mid \alpha \in Q_1, \ \pi_\alpha : V_{s(\alpha)} \to V_{t(\alpha)}\}$ of k-linear transformations.

Example: $Q : \overset{1}{\circ} \circlearrowright \alpha$

A representation of Q over k consists of a pair (V, T), where V is a k-vector space and $T \in \mathrm{End}_k(V)$.

Defn: (Morphism of representations)

If (π_1, V_1) & (π_2, V_2) are two representations of a quiver Q, a morphism $\varphi : (\pi, V) \to (\pi', V')$ consists of a collection of k-linear maps

$$\varphi_i : V_i \longrightarrow V_i'$$

such that $\forall\, \alpha \in Q_1$, the diagram

$$\begin{tikzcd} V_{s(\alpha)} \arrow[r, "\varphi_{s(\alpha)}"] \arrow[d, "\pi_\alpha"'] \arrow[dr, phantom, "\circlearrowright"] & V'_{s(\alpha)} \arrow[d, "\pi'_\alpha"] \\ V_{t(\alpha)} \arrow[r, "\varphi_{t(\alpha)}"'] & V'_{t(\alpha)} \end{tikzcd}$$

commutes

Example: $Q : \overset{1}{\circ} \circlearrowright \alpha$

$\varphi : (V, T) \longrightarrow (V', T')$ consists of a linear map

$\varphi : V \longrightarrow V'$ Iso. classes $\longleftrightarrow$ similarity classes of matrices

$\ni \quad \varphi \circ T = T' \circ \varphi$

Example: $Q : \overset{1}{\circ} \xrightarrow{\alpha} \overset{2}{\circ}$

Reps: $V_1 \xrightarrow{\varphi_\alpha} V_2$

Iso. classes: Equivalence classes of linear transfmns. given by $(\dim(V_1), \dim(V_2), \operatorname{rank} \varphi_\alpha)$

Defn (dimension vector)

A dimension vector for a quiver $Q = (Q_0, Q_1, s, t)$ is a function $d : Q_0 \longrightarrow \mathbb{N} \cup \{0\}$

Each rep. (π, V) of Q has a dimension vector $d(\pi, V)$

$$d(\pi, V)(i) = \dim_k(V_i)$$

Relation to ring theory:

$$Q = (Q_0, Q_1, s, t)$$

Let $i, j \in Q_0$.

A path from i to j is a possibly empty finite sequence of

$$(\alpha_1, \dots, \alpha_n)$$

where $\alpha_1, \dots, \alpha_n \in Q_1$ are such that

$s(\alpha_1) = i$,

$t(\alpha_{i-1}) = s(\alpha_i)$ for $i = 2, \dots, n$

$t(\alpha_n) = j$. $\qquad Q(j,i) = \{\text{paths } i \text{ to } j\}$

n is called the length of the path.

For $i, j, l \in Q_0$, there is a composition of paths

$$Q(l, j) \times Q(j, i) \longrightarrow Q(l, i)$$

given by

$\in Q(i,i)$ $((\alpha_1, \dots, \alpha_n) g (\beta_1, \dots, \beta_m)) \mapsto (\beta_1, \beta_2, \dots, \beta_m, \alpha_1, \dots, \alpha_n)$

$$(x, y) \longmapsto xy$$

ply
n

The path algebra of Q is the vectorspace

m i to i

$$k[Q] = \bigoplus_{i,j \in Q_0} kQ(i,j) = \{\text{Paths}(Q) \to k\}$$

where $kQ(i,j)$ denotes the space of k-valued function on $Q(i,j)$.

Multiplication is given by

$$(f_1 * f_2)(u) = \sum_{xy=u} f_1(x) f_2(y)$$

(why is it associative)

for any path u in Q.

$k[Q]$ has unit $\sum_{i \in Q_0} e_i$.

Given a representation (π, V) of a quiver Q

Let $M = \bigoplus_i V_i$

Define $\pi(u)M$ for a path $(\alpha_1, \dots, \alpha_n)$ as follows:

$$\pi(u)\big|_{V_{s(\alpha_1)}} = \pi_{\alpha_n} \circ \dots \circ \pi_{\alpha_1} \quad (V_{s(\alpha_1)} \to V_{t(\alpha_n)})$$

and $\pi(u)\big|_{V_i} \equiv 0$ if $i \neq s(\alpha_1)$.

For $f \in k[Q]$ define $\pi(f)m = \sum_{\text{paths } u} f(u)\pi(u)m$

48

We have:

$$\pi(f_1)(\pi(f_2)m) = \sum_u f_1(u)\pi(u) \sum_v f_2(v)\pi(v)m$$

$$= \sum_u \sum_v f_1(u) f_2(v) \pi(u)(\pi(v)m)$$

Now: $\pi(u)\circ\pi(v) = \pi(u)\circ \pi_{\beta_m} \circ \cdots \circ \pi_{\beta_1}$

$u = (\alpha_1, \dots, \alpha_n)$

$v = (\beta_1, \dots, \beta_m)$

$$= \pi_{\alpha_n} \circ \cdots \circ \pi_{\alpha_1} \circ \pi_{\beta_m} \circ \cdots \circ \pi_{\beta_1}$$

$$= \pi(uv)$$

$$= \sum_u \sum_v f_1(u) f_2(v) \pi(uv) m$$

$$= \sum_x \sum_{uv=x} f_1(u) f_2(v) \pi(uv) m$$

$$= \sum_x f_1 * f_2(x) \pi(x) m$$

$$= \pi(f_1 * f_2) m$$

Hence, a representation of a quiver gives rise to a k-finite dimens. module for the path algebra.

Conversely, given a k-finite dimensional $k[Q]$-module M, such that $k\sum_i e_i$ acts by scalars, define:

$V_i = e_i M$ $\qquad V_i$ is a k-vector space

Each $e_i^2 = e_i$, so e_i is a projection in M

$e_i e_j = e_j e_i = 0$

$\sum_{i \in Q_0} e_i$ is the identity endomorphism of M

It follows that

$$M = \bigoplus_i V_i$$

$\forall\ \alpha \in Q_1,\quad e_{t(\alpha)}\, \alpha\, e_{s(\alpha)} = \alpha$

$\therefore$ α gives rise to a linear transformation $V_{s(\alpha)} \to V_{t(\alpha)}$.

Get a representation (π, V) of the quiver Q.

It can be shown that:

{Morphisms of representations of quivers}

$\Updownarrow$

{$k[Q]$-module homomorphisms}

Can talk about direct sums of reps of quivers.

Example: $Q = \cdot\circlearrowleft$

$$k[Q] = k[t]$$

Example: $Q = \overset{1}{\circ} \xrightarrow{\alpha} \overset{2}{\circ}$

$$k[Q] = k\cdot e_1 \oplus k\,\alpha \oplus k\cdot e_2$$

$$e_1 \alpha = \alpha \quad \alpha e_2 = \alpha, \quad e_i^2 = e_i, \quad e_1 e_2 = e_2 e_1 = 0.$$

Example: $Q = {}^{\alpha}\circlearrowleft \overset{1}{\cdot} \circlearrowright^{\beta}$

$k[Q] = k\langle \alpha, \beta \rangle$ = the free k-algebra on two generators

basis: $\{\alpha^{m_1}\beta^{n_1}\alpha^{m_2}\beta^{n_2}\cdots\alpha^{m_i}\beta^{n_i} \mid i \in \mathbb{N}\cup\{0\},\ m_i, n_i \in \mathbb{N}\}$

50 Lets calculate the isomorphism classes of reps. of this quiver:

A rep. consists of a vector space V and two linear endomorphisms: $T_1, T_2 \in \mathrm{End}_k V$

$$(T_1, T_2, V) \sim (T_1', T_2', V')$$

iff $\exists$ iso $\varphi: V \to V'$ $\ni$

$$T_1' \circ \varphi = \varphi \circ T_1$$
$$T_2' \circ \varphi = \varphi \circ T_2 .$$

In matrix language, this is the problem of classification of pairs of matrices upto simultaneous similarity, a.k.a., the <u>matrix pair problem</u>.

$$A, B \in M_n(k)$$

$(A, B) \sim (A', B')$ iff $\exists X \in GL_n(k)$ such that

$$\begin{matrix} A'X = XA \\ B'X = XB \end{matrix} \quad \left(\text{or} \quad \begin{matrix} A' = XAX^{-1} \\ B' = XBX^{-1} \end{matrix} \right).$$

Conclusion: Representations of quivers are Noetherian and Artinian $k[Q]$-modules, hence the Krull-Remak-Schmidt theorem applies.

The classification problem: Fix a field k.

Given a quiver $Q = (Q_0, Q_1, t, s)$, determine all the indecomposable representations over k.

Given any two indecomposable reps. over k, describe all the morphisms between them.

Example 1 The linear quiver:

$$Q : \underset{1}{\bullet} \xrightarrow{\alpha_1} \underset{2}{\bullet} \xrightarrow{\alpha_2} \underset{3}{\bullet} \longrightarrow \underset{4}{\bullet} \quad \cdots \quad \underset{n-1}{\bullet} \xrightarrow{\alpha_{n-1}} \underset{n}{\bullet}$$

Let (π, V) be an indecomposable rep. of Q

Step 1: If $\pi(\alpha_i)$ is not injective then $V_j = 0 \ \forall j > i$.

Suppose $\pi(\alpha_1), \dots, \pi(\alpha_{i-1})$ are all injective and $\pi(\alpha_i)$ is not injective.

Let $W_i = \ker(\pi(\alpha_i))$, $W_{i-1} = \pi(\alpha_{i-1})^{-1}(W_i)$, $W_{i-2} = \pi(\alpha_{i-2})^{-1}(W_{i-1})$

$$\begin{array}{ccccccccccc} V_1 & \xrightarrow{\pi(\alpha_1)} & V_2 & \xrightarrow{\pi(\alpha_2)} & \cdots & \longrightarrow & V_{i-1} & \xrightarrow{\pi(\alpha_{i-1})} & V_i & \xrightarrow{\pi(\alpha_i)} & V_{i+1} \to \cdots \\ & & & & & & & & \cup\!| & & \\ W_1 & \xrightarrow{\sim} & W_2 & \xrightarrow{\sim} & \cdots & \xrightarrow{\sim} & W_{i-1} & \xrightarrow{\sim} & W_i & & \end{array}$$

52

Let $S_1 \subset V_1$ be such that $W_1 \oplus S_1 = V_1$.

Inductively define S_{j+1} such that

① $W_{j+1} \oplus S_{j+1} = V_{j+1}$

② $\pi(\alpha_j)(S_j) \subseteq S_{j+1}$ $\quad j=1,\dots,i-1$

$$\begin{tikzcd} V_j \arrow[r, "\pi(\alpha_j)"] \arrow[d, phantom, "\shortparallel"] & V_{j+1} \\ W_j \oplus S_j \arrow[r] & W_{j+1} \oplus S_{j+1} \end{tikzcd}$$

this is done by enlarging $\pi(\alpha_j)(S_j)$ to a supplement.

Then $V = W \oplus S$ where

$W = W_1 \to \cdots \to W_i \to 0 \to \cdots \to 0$

$S = S_1 \to \cdots \to S_i \to V_{i+1} \to \cdots \to V_n$

Since V is indecomposable, and $W_i \neq 0$, must have $S=0$

$\therefore V_{i+1} = \cdots = V_n = 0$.

<u>Step 2</u>: If $\pi(\alpha_j)$ is not surjective, then $V_h = 0$ for all $h \leq j$

<u>Proof</u>: is similar to that of Step 1

<u>Step 3</u>: V is isomorphic to

$[j, i]: 0 \to 0 \to \cdots \to 0 \to \underset{\substack{\uparrow \\ V_j}}{K} \xrightarrow{id} \cdots \xrightarrow{id} \underset{\substack{\uparrow \\ V_i}}{K} \to 0 \to \cdots \to 0$.

$1 \leq j \leq i \leq n$

If all the $\pi(\alpha_i)$'s are injective, then let $i=n$ else, let i be the first instance where $\pi(\alpha_i)$ is not injective.

If all the $\pi(\alpha_i)$'s are surjective, then let $j=1$ else let j be the last instance where $\pi(\alpha_j)$ is not surj.

By Steps 1 & 2, we have that V is of the form

$$0 \to 0 \to \cdots \to 0 \to V_j \xrightarrow{\pi(\alpha_j)} V_{j+1} \xrightarrow{\pi(\alpha_{j+1})} \cdots \xrightarrow{\pi(\alpha_{i-1})} V_i \to 0 \to \cdots \to 0.$$

and $\pi(\alpha_j), \ldots, \pi(\alpha_{i-1})$ are all isomorphisms.

$\therefore$ V is iso to

$$0 \to \cdots \to 0 \to K^d \xrightarrow{id} \cdots \xrightarrow{id} K^d \to 0 \to \cdots \to 0$$

this is indecomposable $\Rightarrow d = 1$

Step 4: $[j, i]$'s are indecomposable and pairwise non-isomorphic

Pf: Suppose $[j, i] = W \oplus W'$, $W \neq 0$, $W' \neq 0$.

Then $\dim_k V = \dim_k \bigoplus V_i \geq 2$

Hence $j < i$.

Assume wlog that $W_j \neq 0$, so $W_j \cong K$.

Let $h > j$ be minimal $\ni$ $W_h = 0$.

Since $W' \neq 0$, must have $h < i$, $W'_h \cong k$

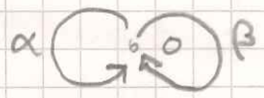
$\therefore$ $\pi \oplus \pi'(\alpha_{h-1}) = 0$ contradicting that $\alpha_{h-1} = id$.

Finite rep type

Example 2: $Q = \alpha \circlearrowleft \circ 1 =: \mathcal{L}_1$ (1-loop).

Indecomposables $\longleftrightarrow$ $\{p(t)^r \mid p(t) \in k[t]$ is an irred monic polynomial & $r \in \mathbb{N}\}$.

Infinite rep type

Example 3 : $\mathcal{L}_2$ 

Claim: the classification problem for $\mathcal{L}_2$ includes the classification problem for any quiver.

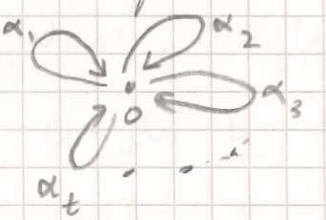
More precisely, for every quiver Q & any rep (π, V) of Q, we will construct a rep $(\tilde\pi, \tilde V)$ of $\mathcal{L}_2$ such that $(\pi, V) \cong (\sigma, W)$ iff $(\tilde\pi, \tilde V) \cong (\tilde\sigma, \tilde W)$,

$(\tilde\pi, \tilde V)$ is indecomposable iff (π, V) is, and

$\mathrm{Hom}_Q(V, W) \hookrightarrow \mathrm{Hom}_{\mathcal{L}_2}(\tilde V, \tilde W)$

This will be done in two steps:

Step 1: the classification problem for $\mathcal{L}_2$ includes the classification problem for $\mathcal{L}_t$ $\forall\, t \geq 2$

$\mathcal{L}_t$ 

Proof: Given a rep (π, V) of $\mathcal{L}_t$ define $(\tilde\pi, \tilde V)$, a rep of $\mathcal{L}_2$ as follows:

$$\tilde V_0 = V_0^{\oplus(t+1)}$$

$$\tilde\pi(\alpha) = \begin{pmatrix} 0 & 1_{V_0} & & 0 \\ & & \ddots & \\ & & & 1_{V_0} \\ 0 & & & 0 \end{pmatrix} \qquad \tilde\pi(\beta) = \begin{pmatrix} 0 & \pi(\alpha_1) & & 0 \\ & & \ddots & \\ & & & \pi(\alpha_t) \\ 0 & & & 0 \end{pmatrix}$$

Suppose $\varphi \in \mathrm{Hom}_{\mathcal{L}_t}(V, W)$.

i.e., $\varphi : V_0 \longrightarrow W_0$ satisfies $\varphi \circ \pi(\alpha_i) = \sigma(\alpha_i) \circ \varphi \ \forall i = 1, \ldots, t$.

Then $\varphi^{\oplus(t+1)}$ satisfies

$$\varphi \circ \tilde{\pi}(\alpha) = \begin{pmatrix} 0 & \varphi & & 0 \\ & & \ddots & \\ & & & \varphi \\ 0 & & & 0 \end{pmatrix} = \tilde{\sigma}(\alpha) \circ \varphi$$

$$\varphi \circ \tilde{\pi}(\beta) = \begin{pmatrix} 0 & \varphi \circ \pi(\alpha_1) & & \\ & & \ddots & \\ & & & \varphi \circ \pi(\alpha_t) \\ & & & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sigma(\alpha_1) \circ \varphi & & 0 \\ & & \ddots & \\ & & & \sigma(\alpha_t) \circ \varphi \\ 0 & & & 0 \end{pmatrix}$$

$$= \tilde{\sigma}(\beta) \circ \varphi.$$

$\therefore \varphi^{\oplus(t+1)} \in \mathrm{Hom}_{\mathcal{L}_2}(\tilde{V}, \tilde{W})$.

Conversely, suppose $\psi \in \mathrm{Hom}_{\mathcal{L}_2}(V, W)$

Then $\psi : V_0^{\oplus t+1} \longrightarrow W_0^{\oplus t+1}$ can be represented by

a matrix $\psi = (\psi_{ij})_{(t+1)\times(t+1)}$, where $\psi_{ij} : V_0 \to W_0$.

$\psi \circ \tilde{\pi}(\alpha) = \tilde{\sigma}(\alpha) \circ \psi$ implies that ψ is of the form

$$\begin{pmatrix} \psi_0 & \psi_1 & \cdots & \psi_t \\ & \psi_0 & \ddots & \\ & & \ddots & \psi_1 \\ & & & \psi_0 \end{pmatrix}$$

$\psi \circ \tilde{\pi}(\beta) = \tilde{\sigma}(\beta) \circ \psi$ implies, among other things, that

$\psi_0 \circ \pi(\alpha_i) = \sigma(\alpha_i) \circ \psi_0$, i.e., $\psi_0 \in \mathrm{Hom}_{\mathcal{L}_t}(V, W)$.

Moreover ψ is an iso. iff ψ_0 is.

Suppose $\varphi: V \to W$ is an iso, then

$$\varphi^{\oplus(t+1)}: \tilde{V} \to \tilde{W} \text{ is also an iso}$$

If $\psi: \tilde{V} \to \tilde{W}$ is an iso, then $\psi_0: V \to W$ is also an iso.

$\therefore V \cong W$ iff $\tilde{V} \cong \tilde{W}$.

Suppose $\psi \in \mathrm{End}_{L_2}(\tilde{V})$. Then ψ is an automorphism (resp nilpotent) iff ψ_0 is.

Suppose V is indecomposable.

Consider $\psi \in \mathrm{End}_{L_2}(\tilde{V})$.

If ψ is not a unit, then $\psi_0 \in \mathrm{End}_{L_t}(V)$ is not a unit, so ψ_0 is nilpotent and hence $\tilde{V}$ is indecomposable.

Conversely, if $\tilde{V}$ is indecomposable, & $\varphi \in \mathrm{End}_{L_t}(V)$ is not a unit, then $\varphi^{\oplus(t+1)} \in \mathrm{End}_{L_2}(\tilde{V})$ is not a unit, hence it is nilpotent. $\therefore \varphi$ is nilpotent.

<u>Step 2</u>: The classification problems for all L_t, $t \geq 2$ include the classification problem for any quiver.

Let Q be any quiver. $Q_0 = \{1, \ldots, n\}$, $Q = \{\beta_1, \ldots, \beta_r\}$

$\beta_j : s_j \to t_j$

$t = n + r$

Let (π, V) be a rep of Q.

Define a rep $(\tilde{\pi}, \tilde{V})$ of L_t as follows

$$\tilde{V}_0 = V_1 \oplus \cdots \oplus V_n.$$

$\tilde{\pi}(\beta_i)$ is the block matrix whose only non-zero block is 1_{V_i} at pos (i,i) for $i=1,\dots,n$.

For $n<i\leq n+r$, let $\tilde{\pi}(\alpha_i)$ be the block matrix whose only non-zero block is $\pi(\beta_{i-n})$ at pos. (t_{i-n}, s_{i-n}).

Suppose $\varphi \in \mathrm{Hom}_Q(V,W)$

Let $\tilde{\varphi}: \tilde{V}_0 \to \tilde{V}_0$ be $\tilde{\varphi} = \varphi(1) \oplus \cdots \oplus \varphi(n)$.

Clearly, $\tilde{\varphi} \circ \tilde{\pi}(\alpha_i) = \tilde{\sigma}(\alpha_i) \circ \tilde{\varphi}$ for $i=1,\dots,n$

$\tilde{\varphi} \circ \tilde{\pi}(\alpha_i)$ is a block with $\varphi(i) \circ \pi(\beta_i)$ at (i,i)th place & zeros everywhere else

$\tilde{\sigma}(\alpha_i) \circ \tilde{\varphi}$ is a block matrix with $\sigma(\beta_i) \circ \varphi(i)$ at (i,i)th place & zeros elsewhere.

$\therefore$ $\tilde{\varphi} \in \mathrm{Hom}_{\Lambda_t}(\tilde{V}, \tilde{W})$ $\tilde{\varphi}$ is an iso iff $\varphi(1),\dots,\varphi(n)$ are

Conversely suppose $\psi \in \mathrm{Hom}_{\Lambda_t}(\tilde{V}, \tilde{W})$

Then $\psi \circ \tilde{\pi}(\alpha_i) = \tilde{\sigma}(\alpha_i) \circ \psi$ means:

$$\begin{pmatrix} \psi_{11} & \cdots & \psi_{1n} \\ \vdots & & \\ \psi_{n1} & & \psi_{nn} \end{pmatrix} \begin{pmatrix} 0 & & & 0 \\ & \ddots & & \\ & & \pi(\beta_i) & \\ 0 & & & \ddots \\ & & & 0 \end{pmatrix} = \begin{pmatrix} & \psi_{1i}\circ\pi(\beta_i) & \\ 0 & \vdots & 0 \\ & \psi_{ni}\circ\pi(\beta_i) & \end{pmatrix}$$

$$\|$$

$$\begin{pmatrix} 0 & & \\ & \pi(\beta_i) & \\ & & \ddots \\ & & & 0 \end{pmatrix} \begin{pmatrix} \psi_{11} & & \psi_{1n} \\ & & \\ \psi_{n1} & & \psi_{nn} \end{pmatrix} = \begin{pmatrix} & & \\ \pi(\beta_i)\circ\psi_{i1} & \cdots & \pi(\beta_i)\circ\psi_{ni} \\ & & \end{pmatrix}$$

(58) Over $i=1,\dots,n$, these identities mean

$$\psi = \psi(1) \oplus \cdots \oplus \psi(n)$$

for some $\psi(i) : V_i \to V_i$

Moreover, $\psi \circ \tilde{\pi}(\alpha_{n+i}) = \tilde{\sigma}(\alpha_{n+i}) \circ \psi$ means that

$$\begin{pmatrix} \psi(1) & & \\ & \ddots & \\ & & \psi(n) \end{pmatrix} \begin{array}{c} \begin{pmatrix} & & \\ & \pi(\beta_i) & \\ & & \end{pmatrix} \leftarrow t_i \\ \uparrow \\ s_i \end{array} = \begin{pmatrix} & & \\ & \psi(t_i) \circ \pi(\beta_i) & \\ & & \end{pmatrix}$$

$$\begin{pmatrix} & & \\ & \pi(\beta_i) & \\ & & \end{pmatrix} \begin{pmatrix} \psi(1) & & \\ & \ddots & \\ & & \psi(n) \end{pmatrix} = \begin{pmatrix} & & \\ & \sigma(\beta_i) \circ \psi(s_i) & \\ & & \end{pmatrix}$$

$$\therefore \psi(t_i) \circ \pi(\beta_i) = \sigma(\beta_i) \circ \psi(s_i)$$

in other words, $\psi \in \mathrm{Hom}_Q(V, W)$

Clearly, ψ is an iso iff $\psi(1), \dots, \psi(n)$ are

Have: $V \cong W \iff \tilde{V} \cong \tilde{W}$.

V is indecomposable iff $\tilde{V}$ is.

$$\mathrm{Hom}_Q(V, W) = \mathrm{Hom}_{\mathcal{L}_b}(\tilde{V}, \tilde{W}).$$

Ideals:

R any ring. ~~M as~~

R can be thought of as a left R-module ${}_R R$.

A left ideal of R is a submodule of ${}_R R$.

~~Let $M \subset {}_R R$ be a left module. Then it has the following properties~~

Left ideals are characterised by the properties:

(1) they are closed under multi

(2) closed under left mult. in R

Quotients:

~~M is a de~~ Let M be a left R-module, $M' \subset M$ be a submodule

The quotient group M/M' has the structure of a left R-module, given by

$$r \cdot (m + M') = rm + M'.$$

Indeed, this does not depend on the choice of ~~m~~ m in its coset.

~~If $m' \in$ ~~ M',

~~then~~ $\cancel{r(m + m' + M') = (rm + \underset{\in}{rm'}^{M'} + M')}$

$\cancel{= r(m+M')} \qquad \cancel{= rm + M'}$

The same definitions of ideals, quotients work when left is replaced by right. But then we write $M' \backslash M$

Can talk about <u>two-sided</u> <u>ideals</u>, in which case the quotient, denoted $\frac{M}{M'}$ is an (R,R)-bimodule.

Defn (Simple, Irreducible)
An R-module is called simple or irreducible if it is non-trivial and has no non-trivial proper submodules.

Proposition: Let R be any unital ring. Any simple R-module is a quotient of ${}_R R$ by a left ideal.

Proof: Let M be a simple R-module. Take $m \neq 0, m \in M$.
The map $x \longmapsto xm$ is a homomorphism of R-modules
$R \longrightarrow M$
Its image is a non trivial submodule of M, hence it must be surjective. Its kernel K is a left ideal
$\therefore M \cong R/K$ as a left R-modules.

Remark: If K is a left ideal of R, then R/K is simple iff K is a maximal left ideal

Defn (Filtration):
[increasing]
An filtration of an R-module M is a finite strictly increasing sequence of submodules
$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0 \quad (*)$$
Defn (Composition series):
A composition series is a filtration of the form (*) where every quotient ~~of succ~~ $\frac{M_i}{M_{i+1}}$ of successive submodules is simple.

Theorem: Let M be a Noetherian and Artinian R-module. Then M has a composition series.

Pf. Note, firstly, that every Noetherian module has a maximal proper submodule:

Let M_1 be any proper submodule of M (possibly (0)).

If M_1 is maximal, done.

Else, $\exists M \supsetneq M_2 \supsetneq M_1$ proper submodule of M

If M_2 is maximal then done, else take M_3 ...

This process must yield a maximal proper submodule after a finite no. of steps, or else we would have constructed an ascending chain without a maximal element.

Note that submodules of M/M' are in bijective correspondence with submodules of M containing M'.

$\therefore$ M' is maximal in M iff M/M' is simple.

To complete the proof of the theorem:

If M is simple, there is nothing to prove.

Else $\exists$ $M \supsetneq M_1 \supsetneq 0$ maximal proper submodule

M/M_1 is simple. If M_1 is simple, then done.

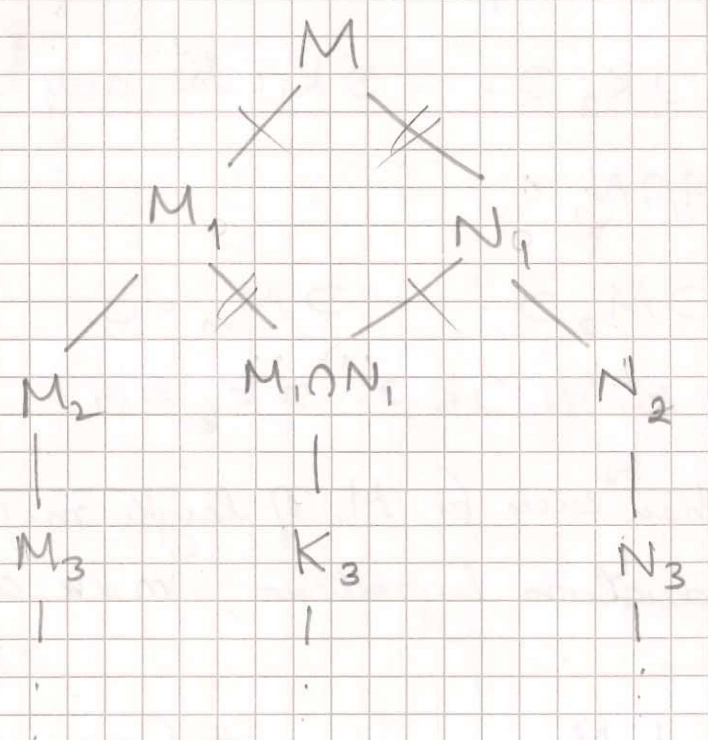
Else $\exists$ $M_1 \supsetneq M_2 \supsetneq 0$, M_2 maximal proper submodule of M_1. Repeating this process, will, by the d.c.c give rise to a composition series in finitely many steps.

<u>Theorem</u> (Jordan-Hölder)

Suppose M is a Noetherian and Artinian R-module and $M = M_0 \supset \cdots \supset M_m = 0$ is a composition series. If $M = N_0 \supset \cdots \supset N_n = 0$ is another, then for $m = n$, and for every simple R-module D, we have:

$$\#\left\{1 \le i \le m \,/\, \frac{M_{i-1}}{M_i} \cong D\right\} = \#\left\{1 \le i \le n \,/\, \frac{N_{i-1}}{N_i} \cong D\right\} \quad (**)$$

<u>Proof</u>



Induct on m.

If $m = 1$, then M is simple, ok.

(62) If $M_1 = N_1$, then $M_1 \supset M_2 \supset \dots \supset M_m$
$M_1 \supset N_2 \supset \dots \supset N_n$
are composition series for M_1 and the result follows from the induction hypothesis.

Else consider $M_1 \cap N_1 \subsetneqq M_1$
$\subsetneqq N_1$.

The natl. inclusion $M_1/M_1 \cap N_1 \hookrightarrow M/N_1 =: D_N$

is an isomorphism, since $M = M_1 + N_1$

Similarly, $N_1/M_1 \cap N_1 \xrightarrow{\sim} M/M_1 =: D_M$

Let $M_1 \cap N_1 \supset K_3 \supset \dots \supset K_k$ be any composition series for $M_1 \cap N_1$.

Now: $M_1 \supset M_2 \supset \dots \supset M_m = 0$
and $\underset{K_1}{M_1} \supset \underset{K_2}{M_1 \cap N_1} \supset K_3 \supset \dots \supset K_k = 0$
are composition series for M_1 of length $m-1$.
By the induction hypothesis, $m = k$ and $\forall$ simple R-module D,
$\#\{2 \leq i \leq m \mid \frac{M_{i-1}}{M_i} \cong D\} = \#\{2 \leq i \leq k \mid \frac{K_{i-1}}{K_i} \cong D\}$
Applying the induction hypothesis again, we see $k = n$ and
$= \#\{2 \leq i \leq k \mid \frac{N_{i-1}}{N_i} \cong D\}$. Since $M/N_1 \cong M_1/M_2$
& $M/M_1 \cong N_1/N_2$
(**) follows

<u>Example:</u> $R = \mathbb{Z}/_2[\mathbb{Z}/2]$, as a left R-module.

Basis $1_0, 1_1$.

Non-zero proper invariant subspaces should be 1-dimensional.

Now, $a1_0 + b1_1$, $a, b \in \mathbb{Z}/_2$ spans an invariant subsp.

iff $1_1(a1_0 + b1_1) = 0$ or $a1_0 + b1_1$.

$$\begin{array}{c} 1_1(a1_0+b1_1) \\ \parallel \\ b1_0 + a1_1 \end{array}$$

If at least one of a & b is non-zero, then must have $a = b = 1$.

$\therefore$ R has a unique non-trivial proper submodule D.

Since it is the only submodule, it can not have a complement.

Clearly D is simple. $\therefore$ $D \cong R/_M$ for some submodule M. The only possibility is $M = D$.

$\therefore$ $D \cong R/_D$ (Exercise: check this explicitly).

<u>Example:</u> $R = \mathbb{Z}/_3[\mathbb{Z}/2]$ as a left R-module.

Basis $1_0, 1_1$.

$a1_0 + b1_1$ spans an invariant subspace iff

$$1_1(a1_0 + b1_1) = \begin{cases} 0 \\ a1_0 + b1_1, \text{ or} \\ 2a1_0 + 2b1_1 \end{cases}$$

$$\parallel$$

$b1_0 + a1_1$ $\therefore$, either $a = b$ or $a = 2b$ & $b = 2a$.

$R = \langle 1_0 + 1_1 \rangle \oplus \langle 1_0 + 21_1 \rangle$ as an R-module.

64 Defn (Completely reducible module)

M is a completely reducible or semi-simple R-module if M is isomorphic to a direct sum of simple R-modules.

Example 1 was completely reducible, but example 2 was not.

Defn (nilpotent ideal)

Let R be any ring. A (left, right or two-sided) ideal I is said to be nilpotent if $I^n = 0$ for some $n \in \mathbb{N}$

Propn: The sum of two nilpotent (left, right, or two sided) ideals is nilpotent

Pf For left ideals:

Let I, J be left ideals in R, $I^m = J^n = 0$

If $x \in (I+J)^{m+n}$, then $x = (a_1+b_1)(a_2+b_2)\dots(a_{m+n}+b_{m+n})$

where $a_1, \dots, a_{m+n} \in I$, $b_1, \dots, b_{m+n} \in J$

The expansion of x consists of monomials

$$\varepsilon_1 \dots \varepsilon_{m+n}, \qquad \varepsilon_i = \text{either } a_i \text{ or } b_i \ \forall i$$

Either $\varepsilon_i = a_i$ for at least m i's

or $\varepsilon_i = b_i$ for at least n i's

Suppose the former

Then $\exists\ 1 \le i_1 \le \dots \le i_m \le m+n \ni \varepsilon_{i_j} = a_i$ for $j=1,\dots,m$.

$$x = (\varepsilon_1 \cdots \varepsilon_{i_1-1} a_{i_1})(\varepsilon_{i_1+1} \cdots \varepsilon_{i_2-1} a_{i_2}) \cdots (\varepsilon_{i_{m-1}+1} \cdots \varepsilon_{i_m-1} a_{i_m})\varepsilon_{i_m+1} \cdots \varepsilon_{m+n}$$

$\therefore \; x \in A^m \varepsilon_{i_m+1} \cdots \varepsilon_{m+n} = 0$

$\therefore \; (I+J)^{m+n} = 0$.

Corollary: Let R be any left Noetherian ring. Then R contains a unique maximal nilpotent left ideal.

Proof: By the ascending chain condition, R contains a maximal nilpotent left ideal I.

If I_1 and I_2 are two maximal nilpotent left ideals, then $I_1 + I_2$ is also a nilpotent left ideal. By maximality, must have

$$I_1 = I_2 = I_1 + I_2.$$

Lecture 12

Lemma: Let R be a left Noetherian ring. Then the maximal nilpotent left ideal of R is a two-sided ideal.

Proof: Let I be the maximal nilpotent two-sided ideal of R.

$JRIR$

Consider the left ideal IR

$$(IR)^2 = I^2R$$

$$(IR)^3 = I^3R$$

$\therefore$ IR is nilpotent. $\because$ $IR \subset R \Rightarrow I$ is a right ideal.

Proposition: Let R be a left Noetherian ring. Then R has a unique maximal nilpotent left ideal. This ideal is a two-sided ideal, and contains every nilpotent right ideal.

Pf: Only remains to show that the maximal nilpotent left ideal contains every nilpotent right ideal.
Let I be a nilpotent right ideal.

$$(RI)^n = RI^n = 0 \text{ for } n \text{ suff. large.}$$

$\therefore RI$ is a nilpotent left ideal.

Defn (radical)
The unique maximal nilpotent (left, right or two-sided) ideal of a left or right Noetherian ring is called its radical. The radical of R is denoted $Rad(R)$.

Theorem: Let R be a unital ring satisfying the Noetherian and Artinian conditions for left ideals. Then ${}_RR$ is semisimple if and only if $Rad(R) = 0$.

Proof ${}_RR = {}_RM_1 \oplus \cdots \oplus {}_RM_n$, M_i's simple.
If M is a left ideal in R, let $J \subseteq \{1, \ldots, n\}$ be maximal such that

$$M \cap \bigoplus_{j \in J} M_j = \{0\}.$$

Suppose $i \notin J$. Since M_i is simple,

$$M_i \cap \left(M \oplus \bigoplus_{j \in J} M_j \right) = \begin{cases} \{0\} \text{ or} \\ M_i \end{cases}$$

If the intersection is $\{0\}$ then

$$M \cap \bigoplus_{j \in J} M_j \oplus M_i = \{0\}$$

(because if $\underset{\substack{\cap \\ M}}{m} = \sum_{j \in J} \underset{\substack{\cap \\ M_j}}{m_j} + \underset{\substack{\cap \\ M_i}}{m_i}$, then

$$m_i = m - \sum_{j \in J} m_j \in M_i \cap \left(M + \bigoplus_{j \in J} M_j \right))$$

Contradicting the maximality of J

$$\therefore M_i \subset M \oplus \left(\bigoplus_{j \in J} M_j \right)$$

$$\therefore R = M \oplus \left(\bigoplus_{j \in J} M_j \right)$$

$$1 = e \oplus e_J, \quad e, e_J \text{ idempotents}$$

If M is nilpotent, then $M^n = 0$ for some $n \in \mathbb{N}$

$\Rightarrow e^n = 0$ for some $n \in \mathbb{N}$

$\Rightarrow e = 0 \Rightarrow M = 0$.

$\therefore R$ has no non-trivial nilpotent left ideals

$\Rightarrow \operatorname{Rad} R = 0$.

For the converse, we will show that if $\operatorname{Rad} R = 0$, then every left ideal in R is a direct summand.

Each non-trivial left ideal is non-nilpotent.

<u>Lemma</u> (Wedderburn): Assume ${}_R R$ is Artinian.
Every non-nilpotent left ideal has an idempotent element.

<u>Proof</u>: Let I be a non-nilpotent left ideal in R
w.l.o.g. assume that I is <u>minimal</u> with this property (using dcc).

$I^2 \neq 0$. $\therefore \exists$ minimal non-trivial left ideal $K \subset I$ such that $IK \neq 0$. (using dcc).

Take $x \in K \ni Ix \neq 0$

Then $Ix = \underset{\ni x}{K}$ (by minimality of K)

$\therefore ax = x$ for some $a \in I$.

$$x = ax = a^2 x = \cdots$$

In particular, a is not nilpotent.

If $a^2 = a$ ok. ~~Else~~

Else let $N = \{ b \in I \mid bx = 0 \}$.

$$a - a^2 \in N$$

N is a non-trivial left ideal properly contained in I, since $Nx = 0$ but $Ix \neq 0$.

$\therefore$ N is nilpotent.

Let $a_1 = 3a^2 - 2a^3$.

Then $a_1 x = 3a^2 x - 2a^3 x = x$

so $x = a_1 x = a_1^2 x = \dots$,

hence a_1 is not nilpotent.

$$a_1 - a_1^2 = (3a^2 - 2a^3) - (3a^2 - 2a^3)^2$$
$$= (3a^2 - 2a^3)\{1 - (3a^2 - 2a^3)\}$$
$$= a^2(3-2a)(1-a^2)(2a+1)$$
$$= (3-2a)(2a+1)(a^2-a^3)^2 \in N^2.$$

Continuing in this way, can construct a sequence $a_1, a_2, a_3, \dots$ such that each a_i is not nilpotent and $a_i - a_i^2 \in N^{2^i}$

Take i so large that $N^{2^i} = 0$.

Then a_i will be a non-trivial idempotent contained in I.

If $\operatorname{Rad} R = 0$, then every non-trivial ideal contains a non-zero idempotent.

Let M_1 be a minimal left ideal.

Let $e \in M_1$ be a non-zero idempotent. $M_1 = Re_1$

$\forall a \in R$, $a = ae_1 + (a - ae_1)$

Let $M_1' = \{a - ae_1 \mid a \in R\}$. This is another left ideal

$\Rightarrow M_1' e_1 = 0$

$\therefore M_1 \cap M' = \{0\}$

we have $R = M_1 \oplus M'$

If M_2 is minimal, then done.

Else repeat this process taking a minimal submodule M_2 of M'. (take $e_2 \in M_2 \ni Re_2 = M_2$,

$$a = e_1 a + e_2 a + (a - e_1 a - e_2 a)$$

$$M'' = \{a - e_1 a - e_2 a \mid a \in R\} \ldots$$

By the a.c.c., this process will stop after a finite number of steps giving

$$R = M_1 \oplus \cdots \oplus M_n . \qquad \text{QED}$$

Defn: (Semisimple ring):

A ring R is said to be semisimple if ${}_R R$ is semisimple

Theorem Let R be a semisimple Artinian ring. Then

$$R = R_1 \oplus \cdots \oplus R_n,$$

where $R_1, \ldots, R_n$ are minimal two-sided ideals. Each R_i is a simple ring (i.e., it has no proper two sided ideals), and are uniquely determined.

Proof: Let R_1 be a minimal two sided ideal in R

As left ideals, we have a decomposition:

$$R = R_1 \oplus R' = Re_1 \oplus Re'$$

$$1 = e_1 + e'$$

$e_1R \cap Re_1$ is a two sided ideal contained in R_1

$\therefore\ e_1R = Re_1 = R_1$

On the other hand

$$R = e_1R \oplus e'R$$

Suppose $a_1 \in R_1$, then $a_1 = \overset{Re_1 \oplus Re'}{a_1 e_1} = \overset{e_1R \oplus e'R}{e_1 a_1}$

$$Re' = \{a \in R \mid ae_1 = 0\}$$

$$0 = ae_1 = ae_1^2 = e_1 \underbrace{ae_1}_{\in R_1} = e_1^2 a = e_1 a$$

e_1 is a central idemp.

$$\therefore\ Re' = \{a \in R \mid e_1 a = 0\} = e'R$$

$\therefore\ R'$ is also a two sided ideal.

If R' is not a minimal two sided ideal, continue this process, as in the proof of the previous theorem.

Will get $R = R_1 \oplus \cdots \oplus R_n$ a direct sum of minimal two sided ideals.

$$1 = e_1 \oplus \cdots \oplus e_n$$

sum of primitive central idempotents

Defn (primitive idempotent)

e is a primitive (central) idempotent if e can not be written as $e = e' + e''$, where e' & e'' are (central) idempotents.

If $R = R_1' \oplus \cdots \oplus R_{n'}'$ is another such decomposition, then $1 = e_1' + \cdots + e_{n'}'$.

72 for any i, j

$e_i e'_j$ is also a primitive central idempotent or 0.

$e_i = e_i 1 = e_i (e'_1 + \cdots + e'_{n'})$

$\therefore e_i = e_i e'_j$ for unique j.

$e'_j = 1 e'_j = (e_1 + \cdots + e_n) e'_j$

$\therefore e'_j = e_i e'_j$

$\therefore \forall i \; e_i = e'_j$ for a unique j QED.

$R_1, \ldots, R_n$ - Wedderburn components of R.

<u>Defn</u> (Simple ring)

R is simple if R has no non-trivial proper two sided ideals.

<u>Theorem</u> (Wedderburn)

Every simple Artinian ring R for which ${}_R R$ is semisimple is isomorphic to the ring of $n \times n$ matrices with entries in a division ring D.

n and D are uniquely determined.

<u>Proof</u>: ${}_R R = M_1 \oplus \cdots \oplus M_n$

Sum of minimal left ideals.

<u>Claim</u>: M_i's are all isomorphic

<u>Pf</u>. $1 = e_1 + \cdots + e_n$

$M_i = Re_i$

$Re_i R$ is a two-sided ideal in R

$\therefore Re_i R = R$

$Re_i Re_j = Re_j \neq 0$

Ex: $\mathrm{Hom}_R(Re_i, Re_j) = (e_i R e_j)^{opp}$

$\therefore Re_j = Re_i a$ for some $a \in e_i R e_j$ $a \neq 0$.

$\therefore$ $x \mapsto xa$ is an iso $Re_i \to Re_j$ of R-modules.

Let $D = \mathrm{End}_R M_i$ (does not depend on i)

Now, let $\gamma_{11} = id_{M_1}$

γ_{i1} = fixed isomorphism $M_1 \to M_i$ $\forall i$.

Let $\gamma_{ij} = \gamma_{i1}\gamma_{j1}^{-1} : M_j \to M_i$ (iso.)

and $\gamma_{ij}\gamma_{jk} = \gamma_{ik}$ $\forall i, j, k$.

γ_{ij} is of the form: $x \mapsto x c_{ji}$ for some $c_{ji} \in e_j R e_i$

$c_{ji} c_{ik} = c_{jk}$ $\forall i, j, k$

$c_{ji} c_{lk} = 0$ if $i \neq l$.

Now: $e_1 R e_1 \cong \mathrm{End}_R(M_1)^{opp}$

$\forall$ $a_{11} \in e_1 R e_1$ put $a_{ii} = c_{i1} a_{11} c_{1i} \in e_i o e_i$

& $a_{11} \to a_{ii}$ is an iso of rings.

Let $\mathcal{D} = \{ \overset{\alpha}{a_{11}} + \cdots + a_{nn} \mid a_{11} \in e_1 R e_1 \}$

$\mathcal{D}$ is a division ring iso. to $e_1 o e_1$

$\forall i, j$, $\alpha c_{ij} = c_{ij} \alpha$ $\forall \alpha \in \mathcal{D}$.

$\therefore$ $R = \sum_{i,j} \mathcal{D} c_{ij}$

R Noetherian & Artinian ring.

$_R R = P_1 \oplus \cdots \oplus P_k$ indecomposable left modules.

$1 = e_1 + \cdots + e_k$

$P_i = Re_i$, $e_1, \ldots, e_k$ are primitive idempotents in R

(Recall: an idempotent e is called primitive if e can not be written as a sum $e = e' + e''$, where e' & e'' are orthogonal idempotents (i.e., $e'e'' = e''e' = 0$))

P_i's are called the principal indecomposable R-modules.

Defn: $M \subset {}_R R$, $\mathrm{Rad}(M) := M \cap \mathrm{Rad}\, R$.

Theorem: Let P and Q be principal indecomposable R-modules. Then ① $\mathrm{Rad}\, P$ is the unique maximal submodule of P

② $P \cong Q$ iff $P/_{\mathrm{Rad}\, P} \cong Q/_{\mathrm{Rad}\, Q}$.

Proof: ① Suppose $_R M \subsetneq {}_R P$ $\quad P = Rp$.

If M is not nilpotent, then M contains an idempotent $e \neq p$.

$$p = pe + p(p-e)$$

Note: p acts on $P = Rp$ as a right identity

$\therefore \; p\underbrace{ep}_{e}e = pe$ $\quad \therefore pe$ idemp.

(76)

$$p(p-e)p(p-e) \overset{?}{=} p(p-e)^2$$
$$= p(p^2 - pe - ep + e^2)$$
$$= p(p - pe - \cancel{e} + \cancel{e})$$
$$= p(p-e).$$

$\therefore$ $p(p-e)$ is idempotent.

$$pe\, p(p-e) = pe - pe = 0$$
$$p(p-e)pe = pe - pe = 0.$$

$\therefore$ pe and $p(p-e)$ are orthogonal idempotents, contradicting the fact that p is a primitive idempotent.

$\therefore$ every proper submodule of P is nilpotent.

<u>Recall</u>: Sum of nilpotent left ideals is nilpotent.

The sum of all proper submodules of P is therefore proper. Hence it is a maximal proper submodule of P.

Moreover, this submodule contains all the nilpotent left ideals contained in P.

$\therefore$ it must equal $P \cap \operatorname{Rad} R$

(2) By (1) if $P \cong Q$ then $\text{Rad } P \cong \text{Rad } Q$ (they are the maximal proper submodules).

$\therefore \; P/\text{Rad } P \cong Q/\text{Rad } Q$

Conversely, suppose $\varphi : P/\text{Rad } P \xrightarrow{\sim} Q/\text{Rad } Q$ is an iso.

Suppose $\varphi(p + \text{Rad } P) = x + \text{Rad } Q \quad x \in Q$

$\varphi(p^2 + \text{Rad } P) = px + \text{Rad } Q$

Define $\hat{\varphi} : P \to Q$ by

$Rx = Rq$

$Rpx = Rq$

$\hat{\varphi}(ap) = apx = ax$ (forced)

Similarly, given $\psi : Q/\text{Rad } Q \xrightarrow{\sim} P/\text{Rad } P$ define

$\hat{\psi}(aq) = aqy = ay$ where y is such that $\psi(q + \text{Rad } Q) = y + \text{Rad } P$

$Ry = Rp$

$\hat{\psi} \circ \hat{\varphi} \in \text{End}_R(P)$ this is a local ring $\quad Rqy = Rp$.

$\hat{\psi} \circ \hat{\varphi}$ is either a unit or nilpotent.

$\hat{\psi} \circ \hat{\varphi}(p) = \hat{\psi}(x) = xy$

$Rxy = Rqy = Rp$

$\therefore \hat{\psi} \circ \hat{\varphi}$ is not nilpotent, hence it is an automorphism. $\therefore$ ψ & φ are also isomorphisms, and $P \cong Q$

Defn: The Jacobson radical of R is the intersection of all maximal ideals in R

Theorem: The Jacobson Radical of R is $\text{Rad } R$

Pf: $R = P_1 \oplus \cdots \oplus P_k$

Every maximal ideal of R is of the form $M_i = \text{Rad } P_i \oplus \left(\bigoplus_{j \neq i} P_j\right)$

$\bigcap_i M_i = \text{Rad } P_1 \oplus \cdots \oplus \text{Rad } P_k = \text{Rad } R$.

Theorem: $P \to P/\mathrm{Rad}\,P$ gives a bijection between the set of isomorphism classes of principal indecomposable R-modules and the set of iso classes of irreducible R-modules.

Defn (Projective module)

An R-module P is projective if whenever there exist $\alpha : P \to N$ & $\beta : M \to N$ with β surjective, $\exists$ $\gamma : P \to M$ such that $\beta \circ \gamma = \alpha$:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\gamma"'] \arrow[d, "\alpha"] & \\ M \arrow[r, "\beta"'] & N \arrow[r] & 0 \end{tikzcd}$$

Theorem: P is projective iff P is isomorphic to a direct summand of a free module.

Pf: Always have a free module F and

$$\begin{tikzcd} & P \arrow[dl, dashed, "s"'] \arrow[d, "id"] & \\ F \arrow[r, "q"'] & P \arrow[r] & 0 \end{tikzcd}$$

$\Rightarrow$ mono

$$\begin{tikzcd} & P\oplus Q \arrow[dl, dashed] \arrow[d] & \\ M\oplus Q \arrow[r] & N\oplus Q \arrow[r] & 0 \end{tikzcd}$$

$F = s(P) \oplus \ker q$. Conversely, $P \oplus Q = F$

Remark: If P is finitely generated, F can be taken to be finitely generated.

Theorem: The principal indecomposable R-modules are precisely the indecomposable projective R-modules

Pf: Clearly, princip. indec $\Rightarrow$ direct summand of free.

Conversely, Suppose $P \oplus Q = R \oplus \cdots \oplus R$

$$P \oplus Q_1 \oplus \cdots \oplus Q_\ell = (P_1 \oplus \cdots \oplus P_k) \oplus \cdots \oplus (P_1 \oplus \cdots \oplus P_k)$$

By the Krull-Remak-Schmidt theorem $P \cong P_i$ for some $1 \le i \le k$.

Defn (multiplicity)

M any Noetherian and Artinian R-module

D any irreducible R-module.

$[M : D]$ = # of subquotients in a composition series for M which are isomorphic to D.

(Jordan-Hölder thm $\Rightarrow$ $[M : D]$ does not depend on the choice of composition series.)

Proposition: ${}_R M$ any Artinian and Noetherian R-module, $P = Re$ a principal indecomposable R-module. Then $P/\mathrm{Rad}\,P$ is a composition factor of M iff $eM \neq 0$.

Proof:

Suppose $[M : P/\mathrm{Rad}\,P] \neq 0$. $0 = M_0 < \cdots < M_n = M$ Comp. ser.

Have

$$\begin{tikzcd} & P \arrow[dl, "\theta \neq 0"'] \arrow[d] & \\ M_i \arrow[r] & P/\mathrm{Rad}\,P \arrow[r] & 0 \end{tikzcd}$$

Let $m = \theta(e)$. Since $\theta \neq 0$, $m \neq 0$.

$m = \theta(e) = \theta(e^2) = e\theta(e) = em \neq 0$

$\therefore eM \neq 0$.

(80) Conversely, if $eM \neq 0$, have

$$0 = M_0 < \cdots < M_n = M$$

$$0 = eM_0 < \cdots < eM_n = eM \neq 0.$$

Claim: $eM_i \not\subseteq M_{i-1}$ for some i.

Pf: Suppose not

$eM_1 \subseteq M_0 = 0 \Rightarrow eM_1 = 0$.

$eM_2 \subseteq M_1 \Rightarrow eM_2 \subseteq eM_1 = 0 \Rightarrow eM_2 = 0$.

$eM_3 \subseteq M_2 \Rightarrow eM_3 \subseteq eM_2 = 0 \Rightarrow eM_3 = 0$

$\vdots$

$\Rightarrow eM = 0$

Picke $0 \neq m \in M_i / M_{i-1}$.

Define $P \to M_i / M_{i-1}$ by

$ae \mapsto aem \quad \forall a \in R$. Sine $eM_i \subseteq$

Since M_i / M_{i-1} is simple, this map is surjective

and its kernel is Rad P.

$\therefore P / \text{Rad} P \cong M_i / M_{i-1}$.

The Blocks of R

$$R = B_1 \oplus \cdots \oplus B_c \qquad (*)$$

a direct sum of two-sided ideals.

$$1 = e_1 + \cdots + e_c \qquad (\dagger)$$

Defn (primitive central idempotent):

Proposition: A decomposition $(*)$ of R into a direct sum of minimal two sided ideals is equivalent to a decomposition $(\dagger)$ of 1 into a sum of primitive central idempotents which are pairwise orthogonal.

Pf: Start with $(*)$, get $(\dagger)$

$$e_a = e_a e_1 + \cdots + e_a e_c$$

If $a \neq b$, $e_a e_b \in B_a \cap B_b \Rightarrow e_a e_b = 0$

similarly, $e_a B_b = B_a e_b = 0$ if $a \neq b$.

Moreover, $e_a B_a = (e_1 + \cdots + e_c) B_a = B_a = B_a (e_1 + \cdots + e_c) = B_a e_a$.

$\therefore$ e_a acts as left and right identity on B_a and as 0 on B_b if $b \neq a$.

Given $x \in R$, write $x = x_1 + \cdots + x_c$ with $x_a \in B_a \, \forall a$

$$e_a x = e_a x_a = x_a = x_a e_a$$

$\therefore$ $e_1, \ldots, e_c$ are all central.

If e_a were not a primitive central idempotent, could write $e_a = e_{a'} + e_{a''}$ both non-zero where $e_{a'}$ & $e_{a''}$ are orthogonal primitive central idempotents

Have $B_a = B' \oplus B''$ where $B' = e_{a'} B_a = B_a e_{a'}$

$B' \cap B'' = e_{a'} e_{a''} B = 0$ | $B'' = e_{a''} B_a = B_a e_{a''}$

are non-trivial two sided ideals, contradicting the indecomposability of B_a.

Conversely, given a decomposition (†) of 1 into a sum of primitive central idempotents, will ~~set~~ $B_a = Be_a = e_a B$.

~~B_a is a two-sided ideal.~~

$$B_a \cap \Big(\bigoplus_{b \neq a} B_b \Big) = e_a \Big(\sum_{b \neq a} e_b \Big) = 0$$

$$\therefore \; B = B_1 \oplus \cdots \oplus B_c$$

As before, the fact that each B_a is indecomposable implies that e_a is a primitive central idempotent.

<u>Proposition</u>: The decomposition (†), and hence the decomposition (*) are unique (not just up to isomorphism, if $1 = e_1 + \cdots + e_c$ ~~=~~ $= f_1 + \cdots + f_d$, then $\forall\ 1 \leq a \leq c\ \exists!\ b \ni e_a = f_b$ and $\forall\ 1 \leq b \leq d\ \exists!\ a \ni f_b = e_a$)

<u>Proof</u>: $1 = e_1 + \cdots + e_c = f_1 + \cdots + f_d$

$$e_a = e_a f_b + (e_a - e_a f_b)$$

Either $e_a f_b = 0$ or $e_a = e_a f_b$

Moreover, $e_a = e_a f_1 + \cdots + e_a f_d$, summands are orthogonal central idempotents.

$\forall b \quad e_a f_b = e_a$ for exactly one a, and is 0 otherwise

$\overset{\shortparallel}{f_b}$ QED.

The indecomposable two sided ideals $B_1, \ldots, B_c$ are called the blocks of A.

If M is any R-module,

$$M = e_1 M \oplus \cdots \oplus e_c M$$

($e_a M \cap (\sum_{b \neq a} e_b M) \subseteq e_a (\sum_{b \neq a} e_b) M = 0$ so the sum is direct).

$\therefore$ if M is indecomposable, then $M = e_a M$ for unique a & $e_b M = 0$ for all $b \neq a$. Say M belongs to the block B_a

Can refine the block decomposition to write ${}_R R$ as a direct sum of indecomposable left ideals:

$$\begin{aligned} R &= B_1 \oplus \cdots \oplus B_c \\ &\quad (P_{11} \oplus \cdots \oplus P_{1k_1}) \oplus \cdots \oplus (P_{c1} \oplus \cdots \oplus P_{ck_c}) \end{aligned}$$

$$\begin{aligned} 1 &= e_1 + \cdots + e_c \\ &\quad (e_{11} + \cdots + e_{1k_1}) + \cdots + (e_{c1} + \cdots + e_{ck_c}) \end{aligned}$$

(each primitive central idempotent is written as a sum of orthogonal primitive idempotents)

Claim: If $P_{ai} \cong P_{bj}$ then $a = b$

Pf: $[P_{bj} : P_{ai}/\mathrm{Rad}\, P_{ai}] \neq 0 \Leftrightarrow e_{ai} P_{bj} \neq 0 \Rightarrow e_a P_{bj} \neq 0$

$\Rightarrow a = b$

(84) It follows that the block of a projective indecomposable R-module is invariant under isomorphism.

Given an irreducible R-module D all the principal indecomposable R-modules $P \ni D \cong P/\mathrm{Rad}\,P$ lie in the same block B_a. We say that D belongs to the block B_a.

<u>Theorem</u>: All the composition factors of an indecomposable R-module lie in the same block

<u>Pf</u>: $[M:D] \neq 0 \iff eM \neq 0$ where $D \cong Re/_{Rad(Re)}$ for some primitive idempotent e. $\underset{e''}{ee_a} \neq 0$ for a unique primitive central idempotent e_a $\therefore$ D belongs to the block B_a and $e_a M \neq 0$

Since $e_a M \neq 0$ for a unique primitive central idempt, all composition factors of M lie in the same block.

<u>Example</u>: R semisimple

$$R = \underset{\underset{(F_1^{n_1})^{\oplus n_1}}{\|}}{M_{n_1}(F_1)} \oplus \cdots \oplus \underset{\underset{(F_s^{n_s})^{\oplus n_s}}{\|}}{M_{n_s}(F_s)}$$

the blocks are the matrix algebras

All the principal indecomposables in a block are isomorphic.

Definition: Two principal indecomposable R-modules P and Q said to be linked if $\exists$ a sequence $P = P_0, P_1, \ldots, P_n = Q$ such that P_{i-1} and P_i have a common composition factor for each $i = 1, \ldots, n$

Theorem: P and Q lie in the same block iff they are linked.

Proof: Since P_{i-1} and P_i have a common composition factor, they must belong to the same block $\forall i$. $\therefore$ Q belongs to the same block at P if P & Q are linked.

Foo the converse: Say $p \sim q$ if Rp & Rq are in the same linkage class.

$$RpR \subseteq \bigoplus_q RpRq$$

$$RpRq \begin{cases} = 0 & \text{if } q \text{ is not liched to } P \\ \subseteq Rq & \text{otherwise} \end{cases}$$

$$\therefore \; RpR \subseteq \bigoplus_{q \sim p} Rq$$

$\therefore$ the sum of all indecomposables in a linkage class is a two-sided ideal contained in a single block B_a. This two sided ideal has a complement (as a left ideal) $R = Re \oplus Re'$ $\quad 1 = e + e'$.

$$Re = ReR$$

$$Re' = R(1-e) = R(1-e)R = Re'R$$

$\therefore$ its complement is a two sided ideal

$\therefore$ $ReR \subset B_a$

86

Example: $A \in M_n(k) \quad R = Z(A)$

$$Z(A) = \bigoplus_p Z(A_p) \quad \text{(primary decomposition)}$$

$$A_p \sim J_\lambda(p) = J_{\lambda_1}(p) \oplus \cdots \oplus J_{\lambda_\ell}(p)$$

where $J_{\lambda_i}(p) = \begin{pmatrix} C_p & & 0 \\ I & \ddots & \\ 0 & I & C_p \end{pmatrix}_{d\lambda_i \times d\lambda_i}$ $\quad d = \deg p$

$$Z(A_p) \cong \operatorname{End}_{K[u]}\left(K[u]/u^{\lambda_1} \oplus \cdots \oplus K[u]/u^{\lambda_\ell} \right)$$

where $K = k[t]/p(t)$

$$\cong \operatorname{End}_{K[u]}(M_\lambda)$$

Let K be an algebraically closed field of characteristic 0. 1

$K[G]$ is semisimple G a finite group.

and $K[G] \cong M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K)$

$$= B_1 \oplus \cdots \oplus B_c$$

$n_1^2 + \cdots + n_c^2 = |G|$

$c = \# \{$ iso classes of simple $K[G]$-modules $\}$

Theorem: (Frobenius?)

$c = \# \{$conjugacy classes in $G\}$

Proof: Any algebra A is an (A,A)-bimodule. ~~fin. dim/K~~

Lemma: For any algebra A, $\mathrm{End}_A A_A = ZA$

Pf: Given $z \in ZA$, define $\varphi_z : A \to A$ by

$$\varphi_z(a) = za.$$

Then $\forall\ b \in A$, $\varphi_z(ba) = zba = bza = b\varphi_z(a)$

$\varphi_z(ab) = zab = \varphi_z(a)b$

$\therefore \varphi_z \in \mathrm{End}_A A_A$

Conversely, given $\varphi \in \mathrm{End}_A A$ define $z_\varphi = \varphi(1)$

Then $\varphi(a) = a\varphi(1) = az$

$$\varphi(1)a = za.$$

$\therefore z \in ZA$

Consider $A = k[G]$. What is ZA?

$f \in ZA \iff f \cdot e_g = e_g f \quad \forall\ g \in G$

i.e., $f(xg^{-1}) = f(g^{-1}x) \quad \forall\ x, g \in G$

$\iff f(gxg^{-1}) = f(x) \quad \forall\ x, g \in G$

Proof:

Lemma: Let A be a finite dimensional algebra over k.

$S := \text{span}_k \{ ab - ba \mid a, b \in A \}$

$T := \{ r \in A \mid r^q \in S \text{ for some power } q \text{ of } p \}$.

Then ⓐ T is a subspace of A containing S

ⓑ $\#\{\text{iso classes of simple } A\text{-modules}\} = \dim_k A/T$.

Proof: ⓐ $(a+b)^p = \sum_{(\varepsilon_1, \dots, \varepsilon_p) \in \{a,b\}^p} \varepsilon_1 \cdots \varepsilon_p$

Group the summands of the form:

$$\underbrace{\underset{\overset{\|}{t_1}}{\varepsilon_1 \cdots \varepsilon_p} \sim \underset{\overset{\|}{t_2}}{\varepsilon_2 \cdots \varepsilon_p \varepsilon_1} \sim \underset{\overset{\|}{t_3}}{\varepsilon_3 \cdots \varepsilon_p \varepsilon_1 \varepsilon_2} \sim \cdots \sim \underset{\overset{\|}{t_p}}{\varepsilon_p \varepsilon_1 \cdots \varepsilon_{p-1}}}_{p \text{ terms}}$$

$t_2 = \varepsilon_1^{-1} t_1 \varepsilon_1$ $\quad \therefore t_2 - t_1 = \varepsilon_1^{-1} t_1 \varepsilon_1 - t_1$

$t_3 = \varepsilon_2^{-1} t \varepsilon_2$ $\quad = \varepsilon_1^{-1}(t_1 \varepsilon_1) - (t_1 \varepsilon_1)\varepsilon_1^{-1} \in S$.

etc.

$\therefore t_1 \equiv t_2 \equiv \cdots \equiv t_p \pmod S$

$\therefore t_1 + \cdots + t_p \equiv p t_1 \equiv 0 \pmod S$

Only when $\varepsilon_1 = \cdots = \varepsilon_p$ are the summands all not pairwise distinct, and so

$(a+b)^p \equiv a^p + b^p \pmod S$.

$\Leftrightarrow$ f is a constant on conjugacy classes.

Conclusion: $\dim_K \left(\mathrm{End}_{K[G]} K[G]_{K[G]} \right) = \#\left\{ \substack{\text{conjugacy classes} \\ \text{in } G} \right\}$

On the other hand:

$$\dim_K \left(\mathrm{End}_{K[G]} K[G]_{K[G]} \right) = \sum_{i=1}^{c} \sum_{j=1}^{c} \mathrm{Hom}_{(K[G], K[G])}(B_i, B_j)$$

$$= \sum_{i=1}^{c} \sum_{j=1}^{c} \delta_{ij} = c$$

$\therefore$ $c = \#\{\text{conjugacy classes in } G\}$

Theorem (Brauer):

Let K be an algebraically closed field of characteristic $p>0$, and let G be a finite group. The number of isomorphism classes of simple $K[G]$-modules is the number of p-regular conjugacy classes in G.

Defn (p-regular element)

An element $x \in G$ is p-regular if its order is coprime to p.

(Order of $x = \min\{ n \in \mathbb{N} \mid x^n = 1 \}$)

$\therefore r^q \in S$

$s^q \in S$

Then $(r+s)^q \in S$ for any power q of p

$\therefore T$ is a subspace

Moreover: $(ab-ba)^p = (ab)^p + (ba)^p = ac - ca,$

where $c = (ba)^{p-1}b$

But $ac - ca \in S$.

$\therefore S \subset T$.

If A is simple, Wedderburn's thm $\Rightarrow A \cong M_n(K)$ for some n. S consists of trace 0 matrices

$\therefore \dim_K (A/S) = 1$

But $T \neq A$ because an idempotent with trace not zero can not belong to T.

$\therefore \dim_K (A/T) = 1 = \#\{$iso. classes of simple A-mod$\}$

In the general case:

$\operatorname{Rad} A \subset T$

$\#\{$iso classes of irred. A-modules$\} = \#\{$iso classes of irred $A/\operatorname{Rad} A$ modules$\}$

$\frac{A}{\operatorname{Rad} A}$ = direct sum of simples algebras

$= B_1 \oplus \cdots \oplus B_c$

define $T_i \subset B_i$ as we define ~~$A\subset$~~ $T \subset A$.

$$\dim(A/T) = \sum_{i=1}^{c} \dim(A_i/T_i) = c$$

(because $T = T_1 \oplus \cdots \oplus T_c$) QED

It remains to show that when $A = k[G]$,

$$\dim_k A/T = \#\{p\text{-regular conjugacy classes in } G\}$$

Recall : Each $x \in G$ can be written as su where s and u are powers of x, s is p-regular and the order of u is a power of p.

$$(x-s)^{pq} = (su-s)^q = s^q u^q - s^q = s^q - s^q = 0$$

$\therefore$ $x - s \in T$

$\therefore$ $x \equiv s \pmod T$

$\therefore$ any element of $k[G]$ is congruent modulo p to a p-regular element

Let $r_1, \dots, r_d$ be representatives of the p-reg conj classes

We will now show ~~that p-regular~~ these elements are linearly independent modulo T

Suppose $\sum_{i=1\, p\text{-regular}}^{d} a_i r_i = 0 \pmod T$ $\quad a_i = a_{g r_i g^{-1}}$ $\forall r_i, g \in G$, r p-reg

Let o_i be the order of r_i. Then $(o_i, p) = 1$

$\therefore$ $q \equiv 1 \bmod o_i$ for some power q of p (why?)

because φ is a unit in $\mathbb{Z}/\mathcal{O}_r$, $\varphi \in (\mathbb{Z}/\mathcal{O}_r)^\times$ finite gp

$\therefore \varphi^{\text{sthg}} \equiv 1 \mod \mathcal{O}_r$

Similarly, can find q such that

$$q \equiv 1 \mod \mathcal{O}_{r_i} \quad \forall\, \cancel{r_i \in G}\ i \quad \cancel{r\ p\text{-regular}}$$

Then $\left(\sum_{i=1}^{d} a_i r_i\right)^{q} \equiv \sum_{i=1}^{d} a_i^{q} r_i \equiv 0 \pmod{S}$

Lemma: $S \subset \left\{ f \in K[G] \;\middle|\; \sum_{g \in G/G_x} f(gxg^{-1}) = 0 \quad \forall\, x \in G \right\}$

Pf. $\sum_{g \in G/G_x} (h_1h_2 - h_2h_1)(gxg^{-1})$

$$= \sum_{g \in G/G_x} \left(\sum_{uv = gxg^{-1}} h_1(u)\, h_2(v) - \sum_{vu = gxg^{-1}} h_1(u)\, h_2(v) \right)$$

$$= \sum_{g \in G/G_x} \left(\sum_{vu = vgxg^{-1}v^{-1}} h_1(u)\, h_2(v) - \sum_{vu = gxg^{-1}} h_1(u)\, h_2(v) \right) = 0$$

because $\{g \mid g \in G/G_x\} = \{vg \mid g \in G/G_x\}$.

Conversely, if $\sum_{g \in G/G_x} f(gxg^{-1}) = 0 \quad \forall\, x \in G$,

then $\sum_{g \in G/G_x} e_{g^{-1}} f\, e_g = 0$

$\sum_{g \in G/G_x} (e_{g^{-1}} f\, e_g - f) = $ mult. f ✓

$\in S$

$$\therefore q \sum_{i=1}^{d} a_i^q r_i \equiv 0 \pmod{S}$$

$$\Rightarrow a_i^q = 0 \ \forall i \Rightarrow a_i = 0 \quad \forall i \qquad \text{QED.}$$

LECTURE NOTES

AMRITANSHU PRASAD

1. Basic definitions

Let K be a field.

Definition 1.1. A K-algebra is a K-vector space together with an associative product $A \times A \to A$ which is K-linear, with respect to which it has a unit.

In this course we will only consider K-algebras whose underlying vector spaces are finite dimensional. The field K will be referred to as the *ground field* of A.

Example 1.2. Let M be a finite dimensional vector space over K. Then $\mathrm{End}_K M$ is a finite dimensional algebra over K.

Definition 1.3. A morphism of K-algebras $A \to B$ is a K-linear map which preserves multiplication and takes the unit in A to the unit in B.

Definition 1.4. A module for a K-algebra A is a vector space over K together with a K-algebra morphism $A \to \mathrm{End}_K M$.

In this course we will only consider modules whose underlying vector space is finite dimensional.

2. Absolutely irreducible modules and split algebras

For any extension E of K, one may consider the algebra $A \otimes_K E$, which is a finite dimensional algebra over E.

For any A-module M, one may consider the $A \otimes_K E$-module $M \otimes_K E$. Even if M is a simple A-module, $M \otimes_K E$ may not be a simple $A \otimes_K E$-module:

Example 2.1. Let $A = \mathbf{R}[t]/(t^2+1)$. Let $M = \mathbf{R}^2$, the A-module structure defined by requiring t to act by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then M is an irreducible A-module, but $M \otimes_{\mathbf{R}} \mathbf{C}$ is not an irreducible $A \otimes_{\mathbf{R}} \mathbf{C}$-module.

Date: 2006-2007.

Definition 2.2. Let A be a K-algebra. An A-module M is said to be *absolutely irreducible* if for every extension field E of K, $M \otimes_K E$ is an irreducible $A \otimes_K E$-module.

Example 2.1 gives an example of an irreducible A-module that is not absolutely irreducible. For any A-module M multiplication by a scalar in the ground field is an endomorphism of M.

Theorem 2.3. *An irreducible A-module M is absolutely irreducible if and only if every A-module endomorphism of M is multiplication by a scalar in the ground field.*

Proof. We know from Schur's lemma that $D := \mathrm{End}_A M$ is a division ring. This division ring is clearly a finite dimensional vector space over K (in fact a subspace of $\mathrm{End}_K M$). The image B of A in $\mathrm{End}_K M$ is a matrix algebra $M_n(D)$ over D. M can be realised as a minimal left ideal in $M_n(D)$. M is an absolutely irreducible A-module if and only if it is an absolutely irreducible B-module.

If $\mathrm{End}_A M = K$, then $B = M_n(K)$, and $M \cong K^n$. $B \otimes_K E = M_n(E)$, and $M \otimes_K E \cong E^n$. Thus $M \otimes_K E$ is clearly an irreducible $B \otimes_K E$-module. Therefore, M is absolutely irreducible.

Conversely, suppose M is an absolutely irreducible A-module. Let $\overline{K}$ denote an algebraic closure of K. Then $M \otimes_K \overline{K}$ is an irreducible $A \otimes_K \overline{K}$-module. Moreover, it is a faithful $B \otimes_K \overline{K}$-module. $B \otimes_K \overline{K} \cong M_m(\overline{K})$ and $M \otimes_K \overline{K} \cong \overline{K}^m$ for some m. Consequently $\dim_K B = \dim_{\overline{K}}(B \otimes_K \overline{K}) = m^2$, and similarly, $\dim_K M = m$. On the other hand, $\dim_K B = n^2 \dim_K D$ and $\dim_K M = n \dim_K D$. Therefore $\dim_K D = 1$, showing that $D = K$. ☐

Definition 2.4. Let A be a finite dimensional algebra over a field K. An extension field E of K is called a *splitting field* for A if every irreducible $A \otimes_K E$-module is absolutely irreducible. A is said to be *split* if K is a splitting field for A. Given a finite group G, K is said to be a splitting field for G if $K[G]$ is split.

Example 2.5. $\mathbf{Z}/4\mathbf{Z}$ is not split over $\mathbf{Q}$. It splits over $\mathbf{Q}[i]$.

Example 2.6. Consider Hamilton's quaternions: $\mathbf{H}$ is the $\mathbf{R}$ span in $M_2(\mathbf{C})$ the matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

$\mathbf{H}$ is a four-dimensional simple $\mathbf{R}$ algebra (since it is a division ring), which is not isomorphic to a matrix algebra for any extension of $\mathbf{R}$. $\mathbf{H}$ is an irreducible $\mathbf{H}$-module over $\mathbf{R}$, but $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$ is isomorphic to $M_2(\mathbf{C})$

and the $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$-module $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$ is no longer irreducible. Therefore $\mathbf{H}$ does not split over $\mathbf{R}$.

Theorem 2.7 (Schur's lemma for split finite dimensional algebras)**.** *Let A be a split finite dimensional algebra over a field K. Let M be an irreducible A-module. Then* $\mathrm{End}_A M = K$.

Proof. Let $T : M \to M$ be an A-module homomorphism. T is a K-linear map. Fix an algebraic closure L of K. Let λ be any eigenvalue of $T \otimes 1 \in \mathrm{End}_{A\otimes_K L} M \otimes L$. Then $T \otimes 1 - \lambda I$, where I denotes the identity map of $M \otimes_K L$ is also an $A \otimes_K L$-module homomorphism. However, $T \otimes 1 - \lambda I$ is singular. Since M is irreducible, this means that $\ker(T\otimes 1-\lambda I) = M$, or in other words, $T\otimes 1 = \lambda I$. It follows that $\lambda \in K$ and that $T = \lambda I$ (now I denotes the identity map of M). □

Corollary 2.8 (Artin-Wedderburn theorem for split finite dimensional algebras)**.** *If A is a split semisimple finite dimensional algebra over a field K if and only if*

$$A = M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K)$$

for some positive integers $n_1, \ldots, n_k$.

Proof. A priori, by the Artin-Wedderburn theorem, A is a direct sum of matrix rings over division algebras containing K in the centre. However, each such summand gives rise to an irreducible A-module whose endomorphism ring is the opposite ring of the division algebra. From Theorem 2.7 it follows therefore that the division algebra must be equal to K. □

Proposition 2.9. *A finite dimensional algebra A is split over a field K if and only if $\frac{A}{\mathrm{Rad} A}$ is a sum of matrix rings over K.*

Proof. The simple modules for A and $\frac{A}{\mathrm{Rad} A}$ are the same. □

Theorem 2.10. *Every finite group splits over some number field.*

Proof. Let $\overline{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$. Then by Corollary 2.8,

$$\overline{\mathbf{Q}}[G] = M_{n_1}(\overline{\mathbf{Q}}) \oplus \cdots \oplus M_{n_c}(\overline{\mathbf{Q}})$$

Let e^k_{ij} denote the element of $\overline{\mathbf{Q}}[G]$ corresponding to the (i, j)th entry of the kth matrix in the above direct sum decomposition. The e^k_{ij}'s for $1 \le k \le c$, and $1 \le i, j \le n_k$ form a basis of A. Each element $g \in G$ can be written in the form

$$g = \sum_{i,j,k} \alpha^k_{ij}(g) e^k_{ij}$$

for a unique collection of constants $\alpha_{ij}^k(g) \in \overline{\mathbf{Q}}$. Similarly, define constants $\beta_{ij}^k(g)$ by the identities

$$e_{ij}^k = \sum_{g \in G} \beta_{ij}^k(g) g.$$

Let K be the number field generated over $\mathbf{Q}$ by

$$\{\alpha_{ij}^k(g), \beta_{ij}^k(g) | 1 \leq k \leq c,\ 1 \leq i, j \leq n_k\ g \in G\}.$$

Set $\tilde{A} = \bigoplus_{i,j,k} K e_{ij}^k$. Then $\tilde{A}$ is a subalgebra of $\overline{\mathbf{Q}}[G]$ that is isomorphic to $K[G]$. Moreover,

$$\tilde{A} = M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K).$$

It follows that every irreducible $\tilde{A}$-module is absolutely irreducible. Therefore, $\tilde{A}$, and hence $K[G]$ is split. □

Proposition 2.11. *Let K be a splitting field for G. Then every irreducible $\mathbf{C}[G]$-module is of the form $M \otimes_K \mathbf{C}$ for some irreducible $K[G]$-module.*

Proof. This follows from the fact that $\mathbf{C}[G] \cong K[G] \otimes_K \mathbf{C}$, and that

$$K[G] = M_{n_1}(K) \oplus \cdots \oplus M_{n_c}(K).$$

□

Theorem 2.12. *Suppose that A is split over K. Then an irreducible A-module $Ae/\mathrm{Rad}Ae$ (where e is a primitive idempotent) occurs $\dim_K eM$ times as a composition factor in a finite dimensional A-module M.*

Proof. Let

$$0 = M_0 \subset \cdots M_m = M$$

be a composition series for M. Suppose that k of the factors M_{i_j}/M_{i_j-1}, $1 \leq i_1 < \cdots < i_k$ are isomorphic to $Ae/\mathrm{Rad}Ae$. Recall that $M_i/M_{i-1} \cong Ae/\mathrm{Rad}Ae$ if and only if eM_i is not contained in M_{i-1}. Therefore, can find $m_{i_1}, \ldots, m_{i_k}$ in $M_{i_1}, \ldots, M_{iK}$ respectively such that $em_{i_j} \notin M_{i_j-1}$. Replacing m_{i_j} by em_{i_j} may assume that $m_{i_j} \in eM$. Since M_{i_j}/M_{i_j-1} is irreducible,

$$Am_{i_j} + M_{i_j-1} = M_{i_j},$$

and hence

$$eM_{i_j} = eAem_{i_j} + eM_{i_j-1}.$$

On the other hand if $i \notin \{i_1, \ldots, i_k\}$ then

$$eM_i \subset M_{i-1}.$$

Let $a \mapsto \overline{a}$ be the mapping of A onto the semisimple algebra $\overline{A} = A/RadA$. Then $\mathrm{End}_{\overline{A}} \overline{A}\overline{e} = \overline{e}\overline{A}\overline{e}$. Since K is a splitting field for A,

$\bar{e}\bar{A}\bar{e} = K$. Therefore $eAe = Ke + e\mathrm{Rad}Ae$. Moreover, $e\mathrm{Rad}AeM_i \subset M_{i-1}$ for all i, and we have that

$$eM_{i_j} = Km_{i_j} + eM_{i_j-1}.$$

We prove that $\{m_{i_1}, \ldots, m_{i_k}\}$ is a basis of eM. It is clear that it is a linearly independent set. If $m \in eM$, then $em = m$. Therefore, $m \in M_{i_k}$. There exists $\xi_k \in K$ such that $m - \xi_k m_k \in eM_{i-1}$. Now $m - \xi_k m_k \in M_{i_{k-1}}$. Continuing in this way, we see that $m - \xi_1 m_1 - \cdots - \xi_k m_k \in M_0 = 0$. □

3. Associated modular representations

Let K be a number field with ring of integers R. Let $P \subset R$ be a prime ideal in R. Denote by $\mathbf{k}$ the finite field R/P. Consider

$$R_P := \{x \in K | x = a/b \text{ where } a \in R,\ b \notin P\}.$$

R_P is called the *localisation of R at P*.

Lemma 3.1. *The natural inclusion $R \hookrightarrow R_P$ induces an isomorphism $\mathbf{k} = R/P \tilde{\to} R_P/PR_P$.*

Proof. The main thing is to show surjectivity, which is equivalent to the fact that $R_P = R + PR_P$. Given a/b, with $a \in R$ and $b \notin P$, by the maximality of P, we know that $R = bR + P$. Therefore a can be written in the form $a = bx + c$, with $x \in R$ and $c \in P$. We then have that $a/b = x + c/b \in R + PR_P$. □

It is easy to see that R_P is a local ring and that PR_P is its unique maximal ideal.

Proposition 3.2. *Let π be any element of $P \setminus P^2$. Then PR_P is a principal ideal generated by π. Every element x of K can be written as $x = u\pi^n$ for a unique unit $u \in R_P$ and a unique integer n. The element $x \in R_P$ if and only if $n \geq 0$.*

For a proof, we refer the reader to [Ser68, Chapitre I]. The integer n is called the *valuation* of x with respect to P (usually denoted $v_p(x)$) and does not depend on the choice of π. The ring R_P is an example of a *discrete valuation ring*.

The following proposition follows from the fact that R_P is a principal ideal domain. We also give a self-contained proof below.

Proposition 3.3. *Every finitely generated torsion-free module over R_P is free.*

Proof. Suppose that M is a finitely generated torsion free module over R_P. Then $\overline{M} := M/PR_PM$ is a finite dimensional vector space over $\mathbf{k}$. Let $\{\overline{m}_1, \ldots, \overline{m}_r\}$ be a basis of $\overline{M}$ over $\mathbf{k}$. For each $1 \leq i \leq r$ pick an arbitrary element $m_i \in M$ whose image in $\overline{M}$ is $\overline{m}_i$. Let M' be the R_P-module generated by $m_1, \ldots, m_r$. Then $M = M' + PR_PM$. In other words, $M/M' = PR_P(M/M')$.

Denote by N the R_P-module M/M'. Now take a set $\{n_1, \ldots, n_r\}$ of generators of N. The hypothesis that $PR_PN = N$ implies that for each i, $n_i = \sum a_{ij}n_j$ where $a_{ij} \in PR_P$ for each j. Now regard N as an $R_P[x]$-module where x acts as the identity. Let A denote the $r \times r$-matrix whose (i,j)th entry is a_{ij}. Let $\mathbf{n}$ denote the column vector whose entries are $n_1, \ldots, n_r$. We have

$$(xI - A)\mathbf{n} = 0.$$

By Cramer's rule,

$$\det(xI - A)\mathbf{m} = 0.$$

All the coefficients of $\det(xI - A)$ lie in PR_P. Therefore, we see that $(1 + c)\mathbf{m} = 0$ for some $c \in PR_P$. Since PR_P is the unique maximal ideal of R_P, it is also the Jacobson radical, which means that $(1 + c)$ is a unit. It follows that $N = 0$.[1]

Consequently M is also generated by $\{m_1, \ldots, m_r\}$. Consider a linear relation

$$\alpha_1 m_1 + \cdots + \alpha_r m_r = 0$$

between that m_i's and assume that $v := \min\{v_P(\alpha_1), \ldots, v_P(\alpha_r)\}$ is minimal among all such relations. The fact that the $\overline{m}_i$'s are linearly independent over $\mathbf{k}$ implies that $v > 0$. Therefore each α_i is of the form $\pi\alpha_i'$, for some $\alpha_i' \in R_P$. Replacing the α_i's by the α_i''s gives rise to a linear relation between the m_i's where the minimum valuation is $v - 1$, contradicting our assumption that v is minimal.

Therefore M is a free R_P-module generated by $\{m_1, \ldots, m_r\}$. $\square$

Let G be a finite group. Let M be a finitely generated $K[G]$-module.

Proposition 3.4. *There exists a $R_P[G]$-module M_P in M such that $M = KM_P$. M_P is a free over R_P of rank $\dim_K M$.*

Proof. Let $\{m_1, \ldots, m_r\}$ be a K-basis of M. Set

$$M_P = \sum_{g \in G} \sum_{j=1}^{r} R_P e_g m_j.$$

Then M_P is a finitely generated torsion-free module over R_P. By Proposition 3.3 it is free. Since each $m_i \in M_P$, $M = KM_P$. An

[1] This is a special case of *Nakayama's lemma*.

R_P-basis of M_P will also be a K-basis of M. Therefore the rank of M_P as an R_P-module will be the same as the dimension of M as a K-vector space. □

Start with a finite dimensional $K[G]$-module M. Fix a prime ideal P in R. By Proposition 3.4 there exists an $R[G]$-module M_P in M such that M_R such that $KM_R = M$. $\overline{M} := M_P/PR_PM_P$ is a finite dimensional $\mathbf{k}[G]$-module. We will refer to any module obtained by such a construction as *a* $\mathbf{k}[G]$*-module associated to* M. However, the module M_P is not uniquely determined. Different choices of M_P could give rise to non-isomorphic $\mathbf{k}[G]$-modules, as is seen in the following

Example 3.5. Let $G = \mathbf{Z}/2\mathbf{Z} = \{0, 1\}$. Consider the two dimensional $\mathbf{Q}[G]$ modules M_1 and M_2 where e_1 acts by

$$T_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad T_2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

respectively. T_1 and T_2 are conjugate over $\mathbf{Q}$, and therefore the $\mathbf{Q}[G]$-modules M_1 and M_2 are isomorphic. However, taking $P = (2) \subset \mathbf{Z}$, we get non-isomorphic modules of $\mathbf{Z}/2\mathbf{Z}[G]$ (T_2 is not semisimple in characteristic 2!). Note, however, that they have the same composition factors.

Theorem 3.6 (Brauer and Nesbitt)**.** *Two* $\mathbf{k}[G]$*-modules associated to the same* $K[G]$*-module have the same composition factors.*

Proof. Let M_P and M'_P be a pair of $R_P[G]$-modules inside M, with R_P-bases $\{m_1, \dots, m_r\}$ and $\{m'_1, \dots, m'_r\}$ respectively. Then there exists a matrix $A = (a_{ij}) \in GL_r(K)$ such that

$$m'_i = a_{i1}m_1 + \cdots + a_{ir}m_r.$$

Replacing M'_P with the isomorphic R_P-module $\pi^a M'_P$ would result in replacing A by $\pi^a A$. We may therefore assume that A has all entries in R_P and that at least one entry is a unit. Replacing A by a matrix XAY, where $X, Y \in GL_r(R_P)$ amounts to changing bases for M_P and M'_P. Let $\overline{A}$ be the image of $A \in M_r(R_P)$ in $M_r(\mathbf{k})$. $\overline{A}$ is equivalent to a matrix of the form $\begin{pmatrix} \overline{B} & 0 \\ 0 & 0 \end{pmatrix}$, where $B \in GL_2(\mathbf{k})$. A little work shows that A is equivalent in $M_r(R_P)$ to a matrix of the form $\begin{pmatrix} B & 0 \\ 0 & \pi C \end{pmatrix}$, where $B \in GL_r(R_P)$. For each $x \in K[G]$ let $T(x)$ and $T'(x)$ denote the matrices for the action of x on M with respect to the bases $\{m_1, \dots, m_r\}$ and $\{m'_1, \dots, m'_r\}$ respectively. T and T' are matrix-valued functions on R. Decompose them as block matrices (of matrix-valued functions on R):

$$T = \begin{pmatrix} X & Y \\ Z & W \end{pmatrix} \quad \text{and} \quad T' = \begin{pmatrix} X' & Y' \\ Z' & W' \end{pmatrix}.$$

Substituting in $TA = AT'$, we get

$$\begin{pmatrix} XB & \pi YC \\ ZB & \pi WC \end{pmatrix} = \begin{pmatrix} BX' & BY' \\ \pi CZ' & \pi CW' \end{pmatrix}.$$

Consequently $\overline{Y}' = 0$ and $\overline{Z} = 0$, and

$$\overline{T} = \begin{pmatrix} \overline{X} & 0 \\ \overline{Z} & \overline{W} \end{pmatrix} \quad \text{and} \quad \overline{T}' = \begin{pmatrix} \overline{X}' & \overline{Y}' \\ 0 & \overline{W'} \end{pmatrix}.$$

An algebra homomorphism from any algebra into a matrix ring naturally defines a module for the algebra. If we denote by $\overline{M}$ and $\overline{M}'$ the $\mathbf{k}[G]$-modules M_P/PR_PM_P and $M'_P/PR_PM'_P$ respectively, then $\overline{M}$ is defined by $\overline{T}$ and $\overline{M}'$ is defined by $\overline{T}'$. The composition factors of $\overline{M}$ are those of the module defined by $\overline{X}$ together with those of the module defined by $\overline{Z}$. Likewise the composition factors of $\overline{M}'$ are those of the module defined by $\overline{X}'$ together with those of the module defined by $\overline{Z'}$. Since X is similar to X' the former pair are isomorphic $\mathbf{k}[G]$-modules. To see that the latter pair have the same composition factors one may use an induction hypothesis on the dimension of M over K (the theorem is clearly true when M is a one dimensional K-vector space). □

Corollary 3.7. *If $(p, |G|) = 1$, M is a $K[G]$-module and P is a prime ideal containing p, then all $\mathbf{k}[G]$-modules associated to M are isomorphic.*

Proof. This follows from Theorem 3.6 and Maschke's theorem. □

4. Decomposition Numbers

Let G be a finite group and K be a splitting field for G. Denote by R the ring of integers in K. Fix a prime ideal P in R. Denote by $\mathbf{k}$ the field R/P. Given an irreducible $\mathbf{C}[G]$-module, we know from Prop 2.11 that it is isomorphic to $M \otimes_K \mathbf{C}$ for some irreducible $K[G]$-module. By Proposition 3.4, there is an $R_P[G]$-module M_P such that $M = KM_P$. Let $\overline{M}$ denote the $\mathbf{k}[G]$-module M_P/PR_PM_P. By Theorem 3.6, the composition factors of $\overline{M}$ and their multiplicities do not depend on the choice of M_P above.

Let $M_1, \ldots, M_c$ be a complete set of representatives for the isomorphism classes of irreducible representations of $\mathbf{C}[G]$. Likewise, denote by $N_1, \ldots, N_d$ a complete set of representatives for the irreducible representations of $\mathbf{k}[G]$. By the theorems of Frobenius and of Brauer and Nesbitt, we know that c is the number of conjugacy classes in G and d is the number of p-regular conjugacy classes in G, provided that $\mathbf{k}$ is a splitting field for G.

Definition 4.1 (Decomposition matrix)**.** The *decomposition matrix of G with respect to P* is the $d \times c$ matrix $D = (d_{ij})$ given by

$$d_{ij} = [\overline{M}_j : N_i].$$

The preceding discussion shows that D is well-defined.

5. Brauer-Nesbitt theorem

Let $1 = \epsilon_1 + \ldots + \epsilon_r$ be pairwise orthogonal idempotents in $\mathbf{k}[G]$.

Lemma 5.1. *Let $\epsilon \in \mathbf{k}[G]$ be an idempotent. There exists and idempotent $e \in \widehat{R}_P[G]$ such that $\overline{e} = \epsilon$.*

Proof. Consider the identity

$$1 = (x + (1-x))^{2n} = \sum_{i=0}^{2n} \binom{2n}{r} x^{2n-j}(1-x)^j.$$

Define

$$f_n(x) = \sum_{i=0}^{n} \binom{n}{r} x^{2n-j}(1-x)^j.$$

It follows that

$$f_n(x) \equiv 0 \mod x^n \text{ and } f_n(x) \equiv 1 \mod (1-x)^n.$$

Since $f(x)^2$ satisfies the same congruences,

$$f_n(x)^2 \cong f(x) \mod x^n(1-x)^n. \tag{5.2}$$

Replacing n by $n-1$ gives

$$f_n(x) \cong f_{n-1}(x) \mod x^{n-1}(1-x)^{n-1}. \tag{5.3}$$

Finally a direct computation yields

$$f_1(x) \cong x \mod x^2 - x. \tag{5.4}$$

Choose any $a \in R_P[G]$ such that $\overline{e} = \epsilon$. Then $a^2 - a \in PR_P[G]$. By (5.3)

$$f_n(a) - f_{n-1}(a) \in P^{n-1}R_P[G],$$

whence $f_n(a)$ is a P-Cauchy sequence. Let $e = \lim_{n\to\infty} f_n(a)$ (this is an element of $\widehat{R}_P[G]$). It follows from (5.2) that e is idempotent, and from (5.4) that $\overline{e} = \epsilon$. ∎

Lemma 5.5. *Let ϵ_1 and ϵ_2 be orthogonal idempotents in $\mathbf{k}[G]$ and let e be any idempotent in $\widehat{R}_P[G]$ such that $\overline{e} = \epsilon_1 + \epsilon_2$. Then there exist orthogonal idempotents $e_1, e_2 \in \widehat{R}_P[G]$ such that $\overline{e}_i = \epsilon_i$.*

Proof. Choose any $a \in \widehat{R}_P[G]$ such that $\overline{a} = \epsilon_1$. Set $b = eae$. Then $\overline{b} = \overline{eae} = (\epsilon_1 + \epsilon_2)\epsilon_1(\epsilon_1 + \epsilon_2) = \epsilon_1$. Also, $be = eb = b$. Therefore, $b^2 - b \in P\widehat{R}_P[G]$, whence $\{f_n(b)\}$ converges to an idempotent $e_1 \in \widehat{R}_P[G]$ such that

$$\overline{e}_1 = \overline{b}_1 = \epsilon_1, \quad e_1 e = e e_1 = e_1.$$

Set $e_2 = e - e_1$, then e_2 is idempotent, and $e_1 e_2 = e_2 e_1 = 0$ and $\overline{e}_2 = \overline{e} - \overline{e}_1 = \epsilon_2$, proving the result. □

Lemma 5.6. *There exist pairwise orthogonal idempotents $e_1, \ldots, e_r \in \widehat{R}_P[G]$ such that $\overline{e}_i = \epsilon_1$ and $1 = e_1 + \cdots + e_r$.*

Proof. For $r = 1$ the result is trivial. Assume therefore, that $r > 1$ and that the result holds for $r - 1$. Set $\delta = \epsilon_{r-1} + \epsilon_r$. Then

$$1 = \epsilon_1 + \cdots + \epsilon_{r-2} + \delta \tag{5.7}$$

is an orthogonal decomposition. By the induction hypothesis, there exist $1 = e_1 + \ldots + e_{r-2} + d$ in $\widehat{R}_P[G]$ lifting (5.7). The lemma now follows from Lemma 5.5. □

Now assume that $1 = \epsilon_1 + \cdots + \epsilon_r$ is a decomposition into pairwise orthogonal *primitive* idempotents. Fix a lifting $1 = e_1 + \cdots + e_r$ in $\widehat{R}_P[G]$ of orthogonal idempotents. Let $M_1, \ldots, M_s$ denote the isomorphism classes of irreducible $K[G]$-modules. Then $[K[G]e_i, M_j] = {}^2 \dim_K e_i M_j = \dim_{\mathbf{k}} \epsilon_i \overline{M}_j = {}^3\overline{M}_j, N_i] = d_{ij}$. Consequently,

$$K[G]e_j \sim \sum_{i=1}^{s} d_{ij} M_j.$$

Passing to associated $\mathbf{k}[G]$-modules,

$$\begin{aligned} P_j &\sim \sum_{i=1}^{s} d_{ij} \overline{M}_i \\ &\sim \sum_{i=1}^{s} d_{ij} \sum_{k=1}^{r} d_{ik} N_k. \end{aligned}$$

On the other hand

$$P_j \sim \sum_{k=1}^{r} c_{jk} N_k.$$

[2]Suppose $M = K[G]e$ for some primitive idempotent e. Then $\dim_K \mathrm{Hom}_{K[G]}(M_j, K[G]e_i) = \dim_K e_i K[G] f = \dim_K e_i M_j$

[3]Theorem 2.12.

Comparing the two expressions for P_j above shows that

$$c_{jk} = \sum_{i=1}^{s} d_{ij} d_{ik},$$

or that $C = D^t D$.

References

[Ser68] Jean-Pierre Serre. *Corps locaux.* Hermann, Paris, 1968. Troisième édition, Publications de l'Université de Nancago, No. VIII.

The Institute of Mathematical Sciences, Chennai.
URL: http://www.imsc.res.in/~amri