Lecture 0 (04-01-2022)

04 January 2022 17:05

Text: T.Y. Lam - A First Course in Noncommutative Rings

Reference: R.S. Pierce - Associative Algebras

Grading : 2 Quizzes 10% each, Midsem 30%, Endsem 50%.

Ring $\longrightarrow$ R with binary operations $+$, $\cdot$, and elements $0, 1 \in R$.

① $(R, +, 0)$ is an abelian group.

② $\cdot$ is associative.

③ $1 \cdot a = a \cdot 1 = a \quad \forall a \in R.$

④ $a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$
$\}\ \forall a, b, c \in R$

($a \cdot b \neq b \cdot a$ is possible.)

Left ideal: $I \subseteq R$ is a left ideal if

① $0 \in R$,

② I is an additive subgroup of R,

③ $a \in R,\ i \in I \implies ai \in I.$

Right ideal : similar.

I is an ideal $:=$ I is a left and right ideal.

Left R-module : $(M, +, \cdot)$ is a left R-module

$+ : M \times M \longrightarrow M, \quad \cdot : R \times M \longrightarrow M$

① $(M, +)$ is an abelian group.

② $a \cdot (b \cdot m) = (ab) \cdot m \quad \forall a, b \in R \ \forall m \in M$

③ $1 \cdot m = m \quad \forall m \in M$

④ distributivity of both.

④ distributivity of both.

Lecture 1 (07-01-2022)

07 January 2022 17:30

$R \longrightarrow$ Ring.

1. $Z(R)$ = center of R
$= \{a \in R : ar = ra \ \forall r \in R\}$ (Always a subring of R.)

2. $a \in R$ is a unit if $\exists b \in R$ s.t. $ab = 1 = ba$.

3. R is called a division ring if every $a \in R \setminus \{0\}$ is a unit and $1 \neq 0$. (Field if commutative, i.e., $R = Z(R)$.)

Examples. ① Hamiltonians (Quaternions)

$\mathbb{H} \cong \mathbb{R}^4$ $\quad \leftrightarrow (a, b, c, d)$

$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$.

$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k.$

$\mathbb{R} \hookrightarrow \mathbb{H}$

$r \mapsto (r, 0, 0, 0)$

$Z(\mathbb{H}) = \mathbb{R}$.

$\alpha = a + bi + cj + dk,$

$\bar{\alpha} = a - bi - cj - dk.$

$\|\alpha\|^2 = \alpha \cdot \bar{\alpha} = a^2 + b^2 + c^2 + d^2.$

$\alpha \cdot \frac{\bar{\alpha}}{\|\alpha\|} = 1$ for $\alpha \neq 0$.

$\therefore \mathbb{H}$ is a division ring (non commutative).

② Let k be a field.

$M_n(k) = n \times n$ matrices over k.

$M_n(k)$ is NEVER commutative if $n \geq 2$ and k is arbitrary.

Check that $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ do not commute.

$M_n(k)$ is NEVER commutative if $n \geq 2$ and k is arbitrary.

Check that $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ do not commute. $(0 \neq 1)$

In fact, given a commutative ring R, one can construct $M_n(R)$. This will again be non-comm for $n \geq 2$ if $R \neq 0$.

One can even do this if R non-comm.

③ Let M, N be left R-modules.

$\mathrm{Hom}_R(M, N) = \{ f : M \longrightarrow N \mid f \text{ is } R\text{-linear} \}$.

In general, $\mathrm{Hom}_R(M, N)$ is only an abelian group.

$(f+g)(m) = f(m) + g(m)$.

If R is comm., we can define

$(rf)(m) := r \cdot f(m)$.

But for non commutative, above definition may not be R-linear. Indeed, if $a \in R$, then we want

$(rf)(am) = a((rf)(m)) = arf(m)$.

OTOH, $(rf)(am) = f(ram) = ra \cdot f(m)$.

However, $\mathrm{Hom}_R(M, N)$ is an S-module for any subring $S \subseteq Z(R)$.

Defn. $S \subseteq R$ is said to be a subring of R if

- S is an additive subgroup,
- S is a multiplicative submonoid (in particular, $1_R \in S$).

Example. $R = \mathbb{Z}/10\mathbb{Z}$.

$S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$.

This is additive and multiplicatively closed.

Moreover, $\bar{6} \cdot x = x \quad \forall x \in S$.

Thus, $\bar{6}$ acts as a unit for S.

Thus, S is a ring BUT NOT A SUBRING OF R.

Remark. If $f : M \to N$ is R-linear and $S \subseteq R$ a subring, then f is S-linear.

Example. $R = \mathbb{C}[x] \to$ inf. dim. vspace over $\mathbb{C}$.

$\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[x], \mathbb{C}[x])$.

$$T = A_1(\mathbb{C}) = R\left\langle \begin{array}{ll} \mu_r : R \to R, & \mu_r(t) = rt \ ; r \in R \\ \frac{\partial}{\partial x} : R \to R, & \frac{\partial}{\partial x}(f) = f' \end{array} \right\rangle.$$

↳ subring of $\mathrm{Hom}_{\mathbb{C}}(R, R)$ generated by μ_r ($r \in R$) and $\frac{\partial}{\partial x}$.

Bernstein: If M is an $A_1(\mathbb{C})$-module s.t. $\dim_{\mathbb{C}}(M) < \infty$, then $M = 0$.

Note: Over $R = \mathbb{C}[x]$, we can get nontrivial such modules. For example, $M_n = R/(x^n)$ is an R-module with $\dim_{\mathbb{C}}(M_n) = n < \infty$ and $M_n \neq 0$.

Proof. Let $\beta = \frac{d}{dx} \cdot \mu_x - \mu_x \cdot \frac{d}{dx}$.

Let $f \in \mathbb{C}[x]$.

Then,

$$\beta(f) = \frac{\partial}{\partial x}(xf) - x\left(\frac{\partial}{\partial x} f\right)$$

$$= f + x \cdot \frac{\partial f}{\partial x} - x \cdot \frac{\partial f}{\partial x}$$

$$= f.$$

$\therefore \beta = 1_{A_1(\mathbb{C})}$.

Suppose $\exists M \neq 0$ over $A_1(\mathbb{C})$ s.t. $\dim_{\mathbb{C}}(M) = n > 0$ with $n < \infty$.

Fix basis for M over $\mathbb{C}$.

$\mu_x : M \to M$ is $\mathbb{C}$-linear. Let A be matrix rep.

$\frac{\partial}{\partial x} : M \to M$ is also $\mathbb{C}$-linear. — " — B — " —.

Then, $BA - AB = I_{n\times n}$.

But taking trace gives a contradiction since $tr(AB) = tr(BA)$

but $tr(I_{n\times n}) = n \neq 0$. ∎

Recall: G is simple if $|G| \leq 59$ unless $G \cong \mathbb{Z}/p\mathbb{Z}$.

For $|G| = 60$, $G \cong A_5$ is precisely the non-simple group.

Groups of order p^n are not simple for $n \geq 2$.

(The center is normal and nontrivial.)

Burnside: $|G| = p^a q^b$, p, q primes, $a+b \geq 2 \Rightarrow G$ not simple.

Rep theory: Study of group homomorphisms $\rho : G \longrightarrow GL_n(\mathbb{C})$.

f.g. modules over $\mathbb{C}[G]$ $\equiv$ Group rep of G.

Emmy Noether:

Group rings $k[G]$

- modular case: $|G| = 0$ in k
- non modular case: $\frac{1}{|G|} \in k$.

Def^. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group and k a field.

$k[G] := kg_1 \oplus kg_2 \oplus \cdots \oplus kg_n$.

Addition is defined component wise.

$$\left(\sum_{g\in G} a_g\, g\right)\left(\sum_{g\in G} b_g\, g\right) = \sum_{g\in G}\left(\sum_{\sigma\tau = g} a_\sigma b_\tau\right) g.$$

EXAMPLE. $G = S_3 = \{1, a, a^2, b, ab, a^2b\}$, $a^3 = b^2 = 1$, $ba = a^2b$.

$k = \mathbb{Q}$.

$\alpha = 2 + 3a + 4b + 5a^2b$,

$\beta = a + 2b$.

Then, $\alpha\beta = (2 + 3a + 4b + 5a^2b)(a + 2b)$

$= 2a + 3a^2 + 4ba + 5a^2ba$

$+ 4b + 6ab + 8b^2 + 10a^2b^2$

$= 2a + 3a^2 + 4a^2b + 5ab + 4b + 6ab + 8 + 10a^2$

$= 8 + 2a + 13a^2 + 4b + 11ab + 4a^2b.$

Let k be a field. Let G act on k, i.e., $G \to \mathrm{Aut}(k)$ is a homom.

$k^G = \{a \in G : \sigma(a) = a \quad \forall \sigma \in G\}.$

Artin: $\begin{matrix} k \\ | \\ k^G \end{matrix}$ finite normal sep ext^n of k^G.

- $R = k[x_1, \ldots, x_n]$.
  $G \leq GL_n(k)$ finite.
  G acts on R. R^G is a subring. (Hilbert showed this is Noetherian!)

Defn. Let G be a finite group.
Let R be a ring.
Let $\rho : G \to \mathrm{Aut}(R)$ be a group homomorphism.
Define the skew group ring $R *_\rho G$ as follows:

$$R *_\rho G = \left\{ \sum_{g \in G} r_g \cdot g \;\; : \;\; r_g \in R \right\}.$$

$$(a_\sigma \sigma) \cdot (b_\tau \tau) := a_\sigma \rho(\sigma)(b_\tau)(\sigma\tau)$$

(Basically: $g \cdot r := \rho(g)(r)$.)

Lecture 2 (11-01-2022)

11 January 2022 17:30

Convention: A module by default means "left module".
The definitions are analogous for right modules.

Def^n. An R-module M is said to be **simple** if
- $M \neq 0$,
- $N \leq M \Rightarrow N = 0$ or $N = M$.
  ↳ N is an R-submodule of M

Q. Are simple modules f.g.?
Yes. Pick any $m \in M \setminus \{0\}$. Then, $\langle m \rangle = M$.

EXAMPLES

1) $k \longrightarrow$ field. $(R = k.)$
If M is a f.g. k-module, then M is a f.dim k-vec space.
Thus, $M \cong k^n$.
In particular, M is simple $\iff M \cong k$.
There is only one simple module!

2) $R = M_n(k)$
$\cong \mathrm{Hom}_k(k^n, k^n)$. $(n=1 \uparrow)$

Assume $n \geq 2$. Note: R is noncommutative for any choice of k.
(e.g.: for $n=2$, consider $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.)

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & * \\ 1 & * \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

We have $k \cong Z(R)$ by $a \longmapsto a I_{n \times n}$.

Let $V = k^n$ as column vectors.

$$= \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in k \right\}.$$

R acts on V by left multiplication.

Lemma. V is a simple R-module.

Proof. Pick $0 \neq v \in V$. To show: $\langle v \rangle = V$.

Extend $\{v\}$ to a k-basis $\{v = v_1, v_2, \ldots, v_n\}$ of V.

For each $i \in [n]$, we can find a matrix $A_i \in R$ s.t.

$$A_i v = v_i.$$

(Think in terms of linear transformation by sending all the basis elements to v_i)

Thus, $v_1, \ldots, v_n \in \langle v \rangle$.

Note that $\langle v \rangle$ is also a k-vec space.

$\therefore$ all k-linear combinations of $v_1, \ldots, v_n$ are in $\langle v \rangle$.

$\therefore V \subseteq \langle v \rangle$. ∎

FACTS: (will prove later.)

① V is the unique simple R-module.

② M is any f.g. left R-module $\Rightarrow M \cong V \oplus \cdots \oplus V$.

Again, unique simple module!

3) $R = \mathbb{Z}$.

$\mathbb{Z}/p\mathbb{Z}$ is simple for all primes $p \geq 2$.

Infinitely many simple modules this time!

Theorem. Let R be a ring such that $k \hookrightarrow Z(R)$.

Assume that $\dim_k(R) < \infty$.

Then, there are only finitely many simple R-modules.

Proof Later. ∎

4) $T_n(k) :=$ $n \times n$ upper triangular matrices over k.

$$k \hookrightarrow Z(T_n(k))$$
$$a \longmapsto a I_{n\times n}, \qquad \dim_k T_n(k) < \infty.$$

Define the R-modules $V_1, \dots, V_n$ as follows:
$V_i \cong k$ as k-vector spaces.

The action on V_i is as follows:

$$\begin{pmatrix} a_{11} & * & * \\ & \ddots & * \\ 0 & & a_{nn} \end{pmatrix} \cdot x := a_{ii} x.$$

(Multiplication by a_{ii}. Check that above is indeed a module.)

Prop $V_1, \dots, V_n$ are all distinct simple R-modules.

Proof Simplicity is clear since $\dim_k(V_i) = 1$.
Now, let $1 \le i < j \le n$ be given. Let

$$f : V_i \to V_j$$

be an R-linear map. We show that $f = 0$. In particular, there is no R-linear isomorphism for V_i to V_j.
Let $x \in V_i$.
Consider the element $A = E_{ii}$. ← 1 in (i,i), 0 else
Then, $x = A \cdot x$.
Applying f gives $f(x) = f(A \cdot x)$
$= A \cdot f(x)$ in V_j
$= 0$. ∎

$= A \cdot f(x)$ in V_j

$= 0$. ∎

Theorem (Schur's Lemma) Let M, N be simple modules.

(i) $\mathrm{Hom}_R(M, N) = 0$ if $M \not\cong N$.

(ii) $\mathrm{Hom}_R(M, M)$ is a division ring.

Proof We show that if $f: M \to N$ is nonzero, then it is an isomorphism. Both parts follow at once.

$f \neq 0 \Rightarrow \ker(f) \neq M \Rightarrow \ker(f) = 0$ since M is simple.

$\Downarrow$

f is one-one.

$f \neq 0 \Rightarrow \mathrm{im}(f) \neq 0 \Rightarrow \mathrm{im}(f) = N$ since N is simple

$\Downarrow$

f is onto. ∎

EXAMPLES SO FAR:

① $R_1 = R$.

② $R_2 = M_n(K) = \mathrm{Hom}_K(K^n, K^n)$.

③ $R_3 = \mathbb{Z}$.

④ $R_4 = \mathbb{H}(K)$.

EXAMPLE 5 $V = K^n$.

$\mathrm{Hom}_K(V, V) \cong R_2$. (1)

Note that V is also an R_2-module.

Claim $\mathrm{Hom}_{R_2}(V, V) \cong K$. (Compare with (1)!) The map constructed will also be a ring isomorphism!

(Iso. as k-vec spaces. Recall that Hom is a $Z(R)$-module.)

Proof $\Psi: K \longrightarrow \mathrm{Hom}_{R_2}(V, V)$.

$a \longmapsto \varphi_a$, where $\varphi_a: V \to V$ is

$u \mapsto a \cdot u$.

Easy to see that Ψ is well-defined, k-linear, and one-one.

Onto:

Step 1. Let $f: V \to V$ be R_2-linear.

Let $\{e_1, \dots, e_n\}$ be the standard k-basis for V.
Define $v_i := f(e_i)$.

Step 2. For all i: $\{e_i, v_i\}$ is lin. dep.

Proof. Suppose they are lin. indep for some i.
Can find $A \in R_2$ s.t. $Av_i = e_i$ and $Ae_i = 0$.
$f(Ae_i) = A \cdot f(e_i) = Av_i = e_i$.
$\|$
0

$\rightarrow\leftarrow$

Step 3. By Step 2, $\exists \alpha_1, \dots, \alpha_n \in k$ s.t. $v_i = \alpha_i e_i \quad \forall i \in [n]$.
Suffices to show that all α_i are same.

Let $i \neq j$. Pick a perm. matrix $P \in R_2$ s.t.
$Pe_i = e_j$, $Pe_j = e_i$.

$\alpha_i e_i = v_i = f(e_i) = f(Pe_j) = Pf(e_j)$
$= Pv_j$
$= \alpha_j Pe_j = \alpha_j e_i$.

$\therefore \alpha_i = \alpha_j$. ∎

Opposite Ring : R^{op}

- Let $(R, +, \cdot)$ be a ring.
- As an abelian group, $(R^{op}, +) = (R, +)$.

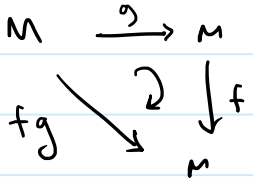
Multiplication is defined as

$$a \cdot b := ba.$$

↗ in R^{op}

- $R \rightarrow$ ring. $S := \mathrm{Hom}_R(M, M) = \mathrm{End}_R(M)$ is a ring with multiplication being composition.

- $\mathrm{Hom}_R(R,R) \cong R^{op}$ as rings.
  $f \longmapsto f(1)$



- More generally,

$$\mathrm{Hom}_R(R^n, R^n) \cong M_n(R^{op}).$$

(In particular, R comm $\Rightarrow$ $\mathrm{Hom}_R(R^n, R^n) \cong M_n(R)$, $\mathrm{Hom}_R(R, R) \cong R$.)

- Let M be a LEFT R-module.
  Then, M is a RIGHT S-module. ($S := \mathrm{Hom}_R(M,M)$.)

$$m \cdot f := f(m).$$

M is an R-S-bimodule.

Proof. $\Psi : \mathrm{Hom}_R(R^n, R^n) \longrightarrow M_n(R^{op})$

$$f \longmapsto \begin{bmatrix} | & | & & | \\ f(e_1) & f(e_2) & \cdots & f(e_n) \\ | & | & & | \end{bmatrix}.$$

$$\Psi(fg) = \begin{bmatrix} | & & | \\ fg(e_1) & \cdots & fg(e_n) \\ | & & | \end{bmatrix}.$$

$$\Psi(f)\Psi(g) = \begin{bmatrix} | & \\ f(e_1) & \cdots \\ | & \end{bmatrix} \begin{bmatrix} | & \\ g(e_1) & \cdots \\ | & \end{bmatrix}$$

Lecture 3 (13-01-2022)

13 January 2022 15:26

(1) $R_1 = k \longrightarrow$ field.

M f.g. over $k \iff M \cong k^n$.

k is the unique simple module over R_1.

(2) $R_2 = M_n(k)$, $V = k^n \longleftrightarrow$ unique simple R_2-module.

(Will show: f.g. modules over R_2 are $V \oplus V \oplus \dots \oplus V$)

(3) $R_3 = \mathbb{Z}$.

For each prime p, $\mathbb{Z}/p\mathbb{Z}$ is a simple $\mathbb{Z}$-module.

(In particular, there are infinitely many!)

(4) $R_4 = T_n(k) \longrightarrow$ upper triangular matrices

$V_i = ke_i$. $V_i \not\cong V_j$ for $1 \le i < j \le n$.

Def^n. $R \longrightarrow$ ring

$M \longrightarrow$ (left) R-module

We say that M is Noetherian if every ascending chain of submodules of M stabilises.

Exercise. TFAE:

(i) M is Noetherian.

(ii) Every nonempty collection of submodules of M has a maximal element.

Def^n. $0 \longrightarrow N \xrightarrow{\alpha} E \xrightarrow{\beta} L \longrightarrow 0$ is said to be a short exact sequence of left R-modules if

(i) α is one-one,

(ii) $\text{im}(\alpha) = \ker(\beta)$,

(iii) β is onto.

Exercise. Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a s.e.s.

TFAE:

(i) M_2 is Noe.

(ii) M_1 and M_3 are Noe.

Note: R has two obvious structures as an R-module.

As a left module, we write ${}_RR$ and as a right we write R_R.

Defn. R is said to be left Noetherian if ${}_RR$ is Noetherian. (Similarly for right.)

Note: There exist (necessarily noncommutative) rings which are left Noetherian but not right.

Dual condition of Noetherian: Artinian (descending chains stabilize). Similarly, a ring is left (resp. right) Artinian if it Artinian as a left (resp. right) module over itself.

Remark: Again left Artinian $\not\Rightarrow$ right Artinian $\not\Rightarrow$ left Art.

Hopkin-Levitzki: ${}_RR$ Artin $\Rightarrow$ ${}_RR$ Noetherian.

R_R Artin $\Rightarrow$ R_R Noetherian.

Examples. • $\mathbb{Z}$ is Noetherian but not Artinian. Thus, converse of above is not true.

• $k \hookrightarrow R$ s.t. • $k \subseteq Z(R)$,

• $\dim_k(R) < \infty$.

Then, R is left Artin and left Noe.

Then, R is left Artin and left Noe.
(Any left ideal is a k-vector space...)

did not REALLY require this for this example
(Then we would talk about dim as left/right k-vec space.)

- Every PID (or more generally PIR) is Noetherian.
  Every ID which is not a field is not Artin. Take $a \in R \setminus \mathcal{U}(R)$, then
  $$aR \supsetneq a^2R \supsetneq a^3R \supsetneq \cdots.$$

- $R = k[x_1, x_2, x_3, \ldots]$.
  $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ NOT Noe.
  $(x_1) \supsetneq (x_1^2) \supsetneq (x_1^3) \supsetneq \cdots$ NOT Artinian.

Question: When is an (left) R-module both Artinian and Noetherian?

Def'n We say that a left R-module M has a composition series

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

if M_{i+1}/M_i is a simple (left) R-module for all $i \in \{0, \ldots, n-1\}$.

Theorem. TFAE:
(i) M is Artinian and Noetherian.
(ii) M has a composition series.

Proof (ii) $\Rightarrow$ (i)

Observation: E simple $\Rightarrow$ E is Art + Noe.

M_1, M_2/M_1 are simple $\Rightarrow$ M_1, M_2/M_1 are A + N

M_2 is $A+N$.

Then consider $0 \to M_2 \to M_3/M_2 \to M_3 \to 0$ and so on.

(i) $\Rightarrow$ (ii) Assume $M \neq 0$.

$\mathcal{C}_1 := \{ N : N \subsetneq M \}$.

$0 \in \mathcal{C}_1$. $\therefore \mathcal{C}_1 \neq \emptyset$.

By Noe., pick $M_1 \in \mathcal{C}_1$ maximal.

- $M_1 \subsetneq M$
- M/M_1 is simple.

If M_1 is simple, then we are done.

Else take $\mathcal{C}_2 := \{N : N \subsetneq M_1\}$ and keep going on to get

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots.$$

Since M is Art, this process must terminate and we are done. ∎

Lecture 4 (18-01-2022)

18 January 2022 17:26

- Artin + Noether $\Leftrightarrow$ $\exists$ composition series
- $k \hookrightarrow Z(A)$, $\dim_k A < \infty \Rightarrow$ A is both left Artin and Noe.

Recalling the proof of Jordan-Hölder, one similarly has:
Any two composition series (if they exist) are of same length, and the quotients appearing are permutations of each other.

Corollary. $k \hookrightarrow Z(A)$, $\dim_k(A) < \infty$.
There are only finitely many simple A-modules (up to isomorphism).

Proof. M simple $\Rightarrow$ $M \cong A/\mathfrak{q}$ $\leftarrow$ simple.

$$A \supsetneq \mathfrak{q} \supsetneq \mathfrak{q}_r \supsetneq \cdots \supsetneq \mathfrak{q}_1 \supsetneq 0.$$

Thus, $A/\mathfrak{q}$ is a module appearing as one of the finitely many quotients in a comp. series of A. ∎

- **Bimodule**: R, S ring.
  $M \longrightarrow$ $(R\text{-}S)$-bimodule, denote ${}_RM_S$.
  - left R-module
  - right S-module

  $r \cdot (m \cdot s) = (r \cdot m) \cdot s \quad \forall r \in R,\ s \in S.$

- Triangular rings.

Let R, S, ${}_RM_S$ be given. Define

$$A := \left\{ \begin{pmatrix} r & m \\ & s \end{pmatrix} : r \in R,\ m \in M,\ s \in S \right\}$$

$$A := \left\{ \begin{pmatrix} r & m \\ & s \end{pmatrix} : r \in R,\ m \in M,\ s \in S \right\}$$

$$\equiv \begin{pmatrix} R & M \\ & S \end{pmatrix}.$$

A is a ring with obvious addition and multiplication as

$$\begin{pmatrix} r & m \\ & s \end{pmatrix} \cdot \begin{pmatrix} r' & m' \\ & s' \end{pmatrix} = \begin{pmatrix} rr' & rm' + ms' \\ & ss' \end{pmatrix}.$$

	R	M	S
R	R	M	0
M	0	0	M
S	0	0	S

Proposition. (Self-study)

① Left ideals of A are of the form $I_1 \oplus I_2$, I_2 is a left ideal in S, I_1 is a left R-submodule of $R \oplus M$ containing MI_2.

② Right ideals of A are of the form $J_1 \oplus J_2$, where J_1 is a right ideal in R, and J_2 is a right S-submodule of $M \oplus S$ containing $J_1 M$.

Corollary. $\begin{pmatrix} \mathbb{C} & \mathbb{C} \\ & \mathbb{R} \end{pmatrix}$ is left-Noe. and left Artin but NOT right-Art nor right-Noe. ($\dim_{\mathbb{R}} \mathbb{C} = \infty$.)

Recall: Let V be a f.d. k-vec. space.
Let $f : V \to V$ be k-linear.
Then, f is one-one $\Leftrightarrow$ f is onto.
The above is false if $\dim_k(V) = \infty$. (Consider the shift-operators.)

Def^n ① A ring R is Dedekind-finite if:

$\forall a, b \in R : \quad ab = 1 \Rightarrow ba = 1.$

② $a \in R$ is called a left zerodivisor if $a \neq 0$ and $\exists\, b \neq 0$ s.t. $ab = 0$.

③ $R^{\neq 0}$ is called a domain if $ab = 0 \Rightarrow a = 0$ or $b = 0$ $\forall\, a, b \in R$.

④ R is called reduced if $a^n = 0 \Rightarrow a = 0$ $\forall a \in R$ $\forall n \in \mathbb{N}$.

EXAMPLES.

(1) $k \to$ field, $\sigma : k \to k$ field endomorphism (not necessarily onto)

HILBERT TWIST.

$$k[x, \sigma] := \left\{ \sum_{\text{finite sum}} a_n x^n \; : \; a_n \in k \right\}.$$

Addition is usual.

$$x \cdot a := \sigma(a)\, x.$$

(i) $\sigma \neq id \Rightarrow k[x, \sigma]$ is not commutative.

(ii) left polynomials $\left\{ \sum a_i x^i \right\}$

right polynomials $\left\{ \sum x^i b_i \right\}$

If σ is not onto, then not all left polynomials are also right polynomials.

- Similarly, can do this with power series to get $k[[x, \sigma]]$.
- $k((x)) = \left\{ \sum_{a_r = 0} a_r x^r \; : \; a_r \in k \right\}$ = Laurent series.

for $r<<0$

Can talk about $k((x;\sigma))$. Here, one takes $\sigma \in Aut(k)$.

$k = \mathbb{Q}(t)$. $\quad \sigma : t \longmapsto 2t$.

$k((x;\sigma))$ is a division ring.

(2) Let G act on a ring A by automorphisms.

$$A * G = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \;:\; a_\sigma \in A,\ \sigma \in G \right\}.$$

Addition component wise. Multiplication:

$$(a\sigma)\cdot(b\tau) = \underbrace{a \cdot \sigma(b)}_{\in R}\ \underbrace{(\sigma\tau)}_{\in G}.$$

3) $k[G]$ $\longrightarrow$ group ring, G finite group

Algebras.

- $A \longrightarrow$ commutative ring.

  $R \longrightarrow$ ring.

  R is said to be an A-algebra via φ if $\varphi : A \longrightarrow Z(R)$ is a ring homomorphism.

Example. $k \hookrightarrow A$, $i(k) \subseteq Z(A)$, $\dim_k A < \infty$.

$\mathrm{Hom}_k(A, k) \longrightarrow$ injective A-module

↳ f.g. as an A-module

$\mathrm{mod}(A) = \{M : M \text{ is a f.g. left } A\text{-module}\}$

has proj. + inj. modules in this case.

Lecture 5 (21-01-2022)

21 January 2022 17:22

Semisimplicity

Recall: A left R-module M is called simple if $M \neq 0$ and $N \leq M \Rightarrow N = 0$ or $N = M$.

Def^n. M is semisimple if for every submodule $N \leq M$, there exists a submodule $K \leq M$ such that $M = N \oplus K$.
(Usual internal direct sum.)

Examples

① 0 module is semisimple.

② Every simple module is semisimple. $(M = M \oplus 0 = 0 \oplus M)$

③ Any (finite dimensional) vector space is semisimple.
↳ Can extend basis, assuming Axc.

④ $0 \to U \to V \to W \to 0$ s.e.s.

V semisimple $\Rightarrow$ U, W are semisimple
$\not\Leftarrow$

Proof ($\Rightarrow$) Let $K \leq U$. Then, $K \leq V$.

Write $V = K \oplus K'$.

Check: $U = K \oplus (K' \cap U)$.

Write $V = U \oplus U'$. Then, $W \cong U' \leq V$.

$\therefore$ W is semisimple by first part.

($\Leftarrow$) Take $R = \frac{k[x]}{(x^2)}$. ⇝ commutative ring!

$$0 \to (x) \to R \to R/(x) \to 0.$$

(x): simple since isomorphic to k

Claim: R is not semisimple.

We show that (x) does not have a complementary submodule.

Indeed, if possible, assume that $R = (x) \oplus W$.

Since $(x) \neq R$, $W \neq 0$.

Let $t = ax + b \in W$.

Since $W \cap (x) = 0$, we have $b \neq 0$.

But then, $1 + \frac{ax}{b} = \frac{t}{b}$.

But then, $1 + \left(\frac{ax}{b}\right) = \frac{t}{b}$.

↳ nilpotent

$\therefore \frac{t}{b}$ is a unit. But then $t \in W$ is a unit.

But W is a proper ideal. ⊠

Def^n. R is said to be left semisimple as a ring if any f.g. R-module is semisimple.

Remark! We will show that R is left s.s. as a ring iff R is s.s. as a left R-module. In fact, in such a case, EVERY R-module is a semisimple module! (See Remark 2.)

Theorem! Let $R = k[G]$. ($k \to$ field, $G \to$ finite group)

R is semisimple $\iff \frac{1}{|G|} \in k$.

$\iff \mathrm{char}(k) \nmid |G|$.

Proof ($\Leftarrow$) Let V be a f.g. R-module (also a f.g. k-v.space). Let $0 \subsetneq W \subsetneq V$ ($k[G]$-submodule!)

We show that $\exists\, h : V \to W$ $k[G]$-linear s.t.

$h(w) = w \quad \forall\, w \in W$.

(That is, $0 \to W \rightleftarrows V \to V/W \to 0$ splits.)

This directly gives $V = W \oplus \ker h$.

Let $\{w_1, \dots, w_r\}$ be a basis of W extended to $\{w_1, \dots, w_r, t_1, \dots, t_s\}$ of V.

Define the k-linear map $f : V \to W$ by

$w_i \mapsto w_i$,

$t_j \mapsto 0$.

Then, $f|_W = id_W$.

Define $h : V \to W$ by

$$h(v) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma v).$$

Then, $$h(w) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma w)$$ ($\sigma w \in W$ since W is a $k[G]$-submodule)

$$= \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1}(\sigma w)$$

$$= \frac{1}{|G|} \sum_{\sigma \in G} w = w.$$

Lastly, we wish to show that h is $k[G]$-linear.
Since it is k-linear, suffices to show that $h(gv) = gh(v)$ $\forall g \in G$.

$$h(gv) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma^{-1} f(\sigma g v)$$

$$= \frac{1}{|G|} \sum_{\sigma \in G} g \cdot g^{-1}\sigma^{-1} f((\sigma g) v)$$

$$= \frac{1}{|G|} \sum_{\tau \in G} g \cdot \tau^{-1} f(\tau v)$$

$$= g \cdot \left(\frac{1}{|G|} \sum_{\tau \in G} \tau^{-1} f(\tau v) \right) = g \cdot h(v).$$

($\Rightarrow$) Later, when we study radicals ∎

Q. How to construct semisimple modules?

Theorem 2. Let M be a left R-module.
TFAE:

1. M is semisimple.
2. M is a sum of simple R-submodules.
3. M is a direct sum of simple R-modules.

Before proof, some examples.

Cor. k field $\Rightarrow M_n(k)$ semisimple as a module over itself.

Proof. Recall that $V \cong k^n$ is a simple $M_n(k)$-module.
Then, $M_n(k) \cong \underbrace{V \oplus \cdots \oplus V}_{n}$ is semisimple. ∎

Cor. ${}_RR$ semisimple $\Rightarrow$ any R-module is simple.

Proof. Let M be any R-module. Map a free module $F = \bigoplus_I R$ onto M.
F is semisimple by Theorem 2.
M is a quotient of F and hence, semisimple by Example 4. ∎

Remark 2. The above reconciles Remark 1.

That is, TFAE:

(i) R is semisimple as a ring.
(That is, every f.g. R-module is a semisimple R-module)

(ii) R is semisimple as a left R-module.
(Note: R is f.g. over itself.)

(iii) Every R-module is semisimple.

Lemma. Let $M \neq 0$ be a semisimple module.
Then, N has a simple submodule.
(In particular, if $K \leq M$ is a nonzero submodule, then K has a simple submodule.)

Proof. Let $0 \neq m \in M$. $Rm \leq M$ is nonzero.
Can assume $Rm = M$.
Let

$$\mathcal{C} = \{ K \leq M : m \notin K \}.$$

$\{0\} \in \mathcal{C}$ and thus, $\mathcal{C} \neq \emptyset$. Partially order $\mathcal{C}$ by $\subseteq$.

Let $\{K_\alpha\}$ be a chain in $\mathcal{C}$. Then, $\bigcup K_\alpha$ is a submodule of M not containing m.
Thus, by Zorn's lemma, $\mathcal{C}$ has a maximal element, say T.

By semisimplicity, $M = T \oplus K$. Then K is simple. ∎

Proof of Thm 2:

(1) $\Rightarrow$ (2) Let M_0 = sum of all simple submodules of M.
If $M_0 \neq M$, then $M = M_0 \oplus K$ for some $K \neq 0$.
But K has a simple submodule then.
$\therefore K \cap M_0 \neq 0$. $\rightarrow\leftarrow$

(2) $\Rightarrow$ (1) $M = \sum_{i \in I} M_i$. Let $N \leq M$ be given.

$$\mathcal{C} = \left\{ J \subseteq I : \begin{array}{ll} (1) & \sum_{i \in J} M_i = \bigoplus_{i \in J} M_i \\ (2) & N \cap \left(\sum_{j \in J} M_i \right) = 0 \end{array} \right\}.$$

$\emptyset \in \mathcal{C}$. Partially order $\mathcal{C}$ by $\subseteq$.
Usual Zorn shows that $\mathcal{C}$ has a maximal J_0.

Let $K = \bigoplus_{j} M_j$. Clearly, $N \cap K = 0$.

Let $K = \bigoplus_{j \in J_0} M_j$. Clearly, $N \cap K = 0$.

Let $M' = N \oplus K$. We show $M = M'$!

If not, then $M_i \not\subseteq M'$ for some $i \in I$. (Necessarily $i \notin J_0$.)

Then, $M' \cap M_i = \{0\}$ since M_i simple.

But then $J_0 \cup \{i\} \in \mathcal{C}$, contradicting maximality.

(2) $\Rightarrow$ (3) Same proof as above works with $N = 0$, since we produced a complement which was a direct sum of simple modules

Lecture 6 (28-01-2022)

28 January 2022 17:28

- Recall that for an R-module M, TFAE:
  1. M is semisimple.
  2. M is a sum of simple submodules.
  3. M is a direct sum of simple modules.

1. We also showed that if $\mathrm{char}(k) \nmid G$, then $k[G]$ is semisimple. Converse is true as well. (We did not show this.)

2. $R = M_n(K)$ is simple, $R = \bigoplus_{i=1}^{n} K^n$.

3. R is semisimple as a ring $\overset{\text{defn}}{\iff}$ every f.g. R-module is semisimple
   $\iff$ R is semisimple as a (left) module.
   $\iff$ every R-module is semisimple.

Q. If R is semisimple as a left module, is it also semisimple as a right module? As we shall see, yes!

Thm (Artin-Wedderburn)
Let $R \neq 0$ be a ring. TFAE
(i) R is a left semisimple ring.
(ii) $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, where D_i are division rings.
by uniqueness $(r, (n_1, D_1), \ldots, (n_r, D_r))$ is an invariant of R.
(iii) R is a right semisimple ring.

Recall R^{op}.

Left R-module $\equiv$ Right R^{op}-module.

$a \cdot m \longleftrightarrow m \cdot a$
$a \cdot (b \cdot m) \longleftrightarrow (m \cdot b) \cdot a$
$a \cdot b \longleftrightarrow b \cdot a$
} $a, b \in R$, $m \in M$

EXAMPLE. $D \longrightarrow$ Division ring.

Let $R = M_n(D)$, $V = D^n$. V is an R-module naturally.

Then,

1. R is semisimple.
2. ${}_RR \cong \underbrace{V \oplus \cdots \oplus V}_{n \text{ copies}}$.
3. $\mathrm{End}_R(V) \cong D^{op}$.

Proof of 3. Let $\mu_a : D^n \longrightarrow D^n$ denote multiplication ON THE RIGHT by $a \in D$.

Define $\phi : D^{op} \longrightarrow \mathrm{Hom}_R(D^n, D^n)$ by

$a \longmapsto \mu_a$.

Then, ϕ is 1-1 and onto. (We had seen this for fields in lecture 2 Example 5.)

$\phi(1) = 1$. ✓ (Same proof goes.)

Now, $\phi(a \cdot b) = \mu_{a \cdot b}$

$= \mu_{ba} = \mu_a \circ \mu_b$ (MULTIPLY ON THE RIGHT!)

$= \phi(a) \circ \phi(b)$. ∎

$\phi(a+b) = \phi(a) + \phi(b)$ is clearly true.

Theorem. $R_1, \ldots, R_n$ semisimple $\Rightarrow$ $R_1 \times \cdots \times R_n$ semisimple.

Proof. Suffices to show this for $n = 2$.

Write $R = \bigoplus_i U_i$, $S = \bigoplus_j V_j$.

Check $R \times S = \left(\bigoplus_i U_i \times S\right) \oplus \left(\bigoplus_j R \times V_j\right)$. ∎

EXERCISE. ① U simple R-module $\Rightarrow U \times S$ is a simple $(R \times S)$-module.

② V simple S-module $\Rightarrow R \times V$ is a simple $(R \times S)$-module.

Proof of Artin-Wedderburn :

① $\Rightarrow$ ②. Let R be left semisimple.

Write $R = \bigoplus_{i \in \Lambda} U_i$ for $U_i \subseteq R$ simple left ideals.

$1 \in U_{i_1} \oplus \cdots \oplus U_{i_s}$.

$\Rightarrow r = r.1 \in U_{i_1} \oplus \cdots \oplus U_{i_s}$ for all $r \in R$.

$\therefore R = \bigoplus_{i=1}^{s} U_i$: U_i simple.

$= \bigoplus_{i=1}^{r} V_i^{\oplus n_i}$: V_i simple, $n_i \in \mathbb{N}$, $r \geq 1$, $V_i \not\cong V_j$ for $i \neq j$.

$$R^{op} \cong \mathrm{Hom}_R(R, R) = \mathrm{Hom}_R\left(\bigoplus_{i=1}^{r} V_i^{n_i}, \bigoplus_{j=1}^{r} V_j^{n_j}\right)$$

$$\cong \bigoplus_{i,j} \mathrm{Hom}_R\left(V_i^{n_i}, V_j^{n_j}\right)$$

$$\cong \bigoplus_{i,j} \mathrm{Hom}_R(V_i, V_j)^{n_i n_j}$$ (Schur)

$$\cong \bigoplus_{i=1}^{s} \mathrm{Hom}_R\left(V_i^{n_i}, V_i^{n_i}\right)$$

$$= \prod_{i=1}^{s} \mathrm{End}_R\left(V_i^{n_i}\right).$$

$\mathrm{Hom}_R(V_i^{n_i}, V_i^{n_i}) \cong \mathrm{Hom}_R(V_i, V_i)^{n_i^2} \cong M_{n_i}(D_i)$.

($D_i := \mathrm{Hom}_R(V_i, V_i)$ div ring by Schur; decode)

Thus, $R^{op} \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.

$\Rightarrow R \cong M_{n_1}(D_1^{op}) \times \cdots \times M_{n_r}(D_r^{op})$.

Other directions now follow.

Proof also shows uniqueness : The V_i are characterised by the modules

appearing in any Jordan-Hölder decomposition. So are the n_i. ∎

Lecture 7 (01-02-2022)

01 February 2022 17:36

Last time, we characterised semisimple rings.

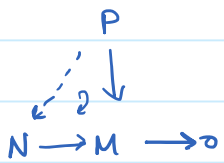
Thm. Let R be a ring. TFAE:
(i) R is left semisimple.
(ii) $R \cong \prod_{i=1}^{s} M_{n_i}(D_i)$.
(iii) R is right semisimple.

Semisimple ring $\equiv$ homological dim 0.

Defn. A left R-module P is called projective if for every diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \beta & & \\ N & \xrightarrow[\alpha]{} & M & \to & 0, \end{array} \qquad (\alpha \text{ is onto})$$

there exists $h: P \to N$ s.t. $\alpha \circ h = \beta$.



Examples. Any free R-module is projective.

Prop. Any direct summand of a free module is projective.
That is, if P is such that $\exists\, Q$ with $P \oplus Q$ free, P is projective.
($P \oplus Q = F$)

Proof. Exercise. Use the maps $P \xhookrightarrow{i} F$ and $F \twoheadrightarrow P$ along with projectivity of F. ∎

Remark.
① If $R \neq 0$ is a commutative ring and $R^n \overset{\text{as } R\text{-modules}}{\cong} R^m$, then $n = m$.
② $\exists$ a non comm. ring R s.t. $R \cong R^2$ as R-modules. Consequently $R^n \cong R^m \ \forall\, n, m \in \mathbb{N}$.

Example. Note $\mathbb{Z}/6 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$.

Thus, $\mathbb{Z}/2$ and $\mathbb{Z}/3$ are projective $\mathbb{Z}/6$-modules.
However, neither is free.

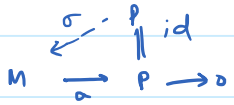
Prop^n. Let k be a field, R a ring.
Suppose $k \subseteq Z(R)$ with $\dim_k(R) < \infty$.
Then, $R^n \cong R^m \Rightarrow n = m$.

Proof. $R^n \cong R^m$ as R-mod $\Rightarrow R^n \cong R^m$ as k-mod

$\Rightarrow n \cdot \dim_k R = m \cdot \dim_k R \Rightarrow n = m$. ∎

Remark. If $\alpha : M \to P$ is surjective with P projective, then
$\exists \sigma : P \to M$ s.t. $\alpha \circ \sigma = id_P$.

Then, $M \cong P \oplus \ker \alpha$.



In particular, if P is f.g., one can find a f.g. Q s.t. $P \oplus Q \cong R^n$ with $n < \infty$.
(Map an R^n onto P and note Q is a quotient of R^n.)

Def^n. We say that the s.e.s. $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} L \to 0$ splits
if $\exists \sigma : L \to N$ s.t. $\beta \circ \sigma = id_L$.

Remark. ① In the above case, we have $N \cong M \oplus L$.
② The above is equivalent to: $\exists \pi : N \to M$ s.t. $\pi \circ \alpha = id_M$.

Thm. Let R be a semisimple ring.
Then, every R-module is projective.

Proof. Let M be any R-module.
We get a s.e.s. $0 \to K \hookrightarrow F \to M \to 0$ with F free.
$K \subseteq F$. We have $F = K \oplus L$ as F is semisimple.
Then, the above s.e.s. splits. Thus, $F \cong M \oplus K$ and hence,
M is projective. ∎

Lemma. $N \leq \mathbb{Z}^s \Rightarrow N \cong \mathbb{Z}^r$ for some $r \leq s$.

Submodule of a f.g. free module is free with rank not increasing.

Proof. Induction on s.

$s = 1$: Clear since ideals are 0 or $n\mathbb{Z} \cong \mathbb{Z}$ for $n \neq 0$.

$s \geq 2$: $N \leq \mathbb{Z}^s = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_s$.

Let π_i denote the natural proj. $\mathbb{Z}^s \to \mathbb{Z}e_i$ and $j : N \hookrightarrow \mathbb{Z}^s$ the nat. inclusion.

CASE 1. $\pi_i \circ j = 0$ for some i.

Then, $N \leq \mathbb{Z}^{s-1}$ and by induction...

CASE 2. $\pi_i \circ j \neq 0$ for all i.

Then, $\operatorname{im}(\pi_i \circ j) = n_i\mathbb{Z}$ for all i, $n_i \geq 1$.

We have the s.e.c.

$$0 \to \ker(\pi_i \circ j) \to N \xrightarrow{\pi_i \circ j} \mathbb{Z} \to 0.$$

As $\mathbb{Z}$ is projective, we get

$$N \cong \mathbb{Z} \oplus \ker(\pi_i \circ j)...$$

Lecture 8 (04-02-2022)

04 February 2022 17:26

Two classes of rings:

1. Noetherian rings : Hilbert Basis Theorem. → R commutative ⇓ R[x] commutative ⇓ R[x₁, ..., xₙ] is comm.
2. Quiver algebras

Theorem. Let R be a left (resp. right) Noetherian ring.
Then, R[x] is left (resp. right) Noetherian.

Proof. Let $I \subseteq R[x]$ be a left ideal. We wish to show that I is f.g.
Can assume $I \neq 0$.

Notation: for $f = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$,
define $LT(f) := x^n$, $LC(f) := a_n$.

For $n \geq 1$, define

$$J_n := R\langle LC(f) : 0 \neq f \in I,\ LT(f) = x^n \rangle.$$

↳ left ideal generated in R by leading coeffs of n^{th} deg polys in I.
Note: J_n could be zero if no such f.

If $f = a_0 + \cdots + a_n x^n \in I$ with $a_n \neq 0$, then
$LT(xf) = LT(f \cdot x) = x^{n+1}$, $LC(xf) = a_n$.
$\therefore J_n \subseteq J_{n+1}$.

We have an asc. chain of left ideals of R:
$J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$.

As R is left Noe., the above stabilises. Let n_0 be s.t. $J_n = J_{n_0}$ $\forall n \geq n_0$.

$J_{n_0} = (a_1, \ldots, a_s)$.

Let $M = (R \oplus Rx \oplus \cdots \oplus Rx^{n_0-1}) \cap I$.
↓
Noetherian since R is.

M is a Noetherian R-module.

Write $M = R\langle m_1, \dots, m_r \rangle$.

Pick $f_1, \dots, f_s \in I$ with $LT(f_i) = a_i$. (of largest deg no)

Claim: $I = R\langle m_1, \dots, m_r, f_1, \dots, f_s \rangle$.

Pf Let $N = R\langle m_1, \dots, m_r, f_1, \dots, f_s \rangle$.

Clearly, $N \subseteq I$.

Let $0 \neq f \in I$. We show $f \in N$ by induction on $\deg(f) =: n$.

If $n \leq n_0 - 1$, then $f \in M \subseteq N$.

Suppose $n \geq n_0$.

Then, $LC(f) \in J_n = J_{n_0}$.

Can subtract off leading term and decrease deg. ∎

Thus, we are done. ∎

Differential Rings

Let R be any ring.

$\delta : R \to R$ is a derivation if

$$\delta(a+b) = \delta(a) + \delta(b),$$
$$\delta(ab) = \delta(a)\,b + a\,\delta(b).$$

EXAMPLE. ① $R = k[x]$.

δ is $\frac{d}{dx}$.

② $R = k[x, y]$.

$\delta = x \frac{\partial}{\partial y}$.

$$R[x, \delta] := \left\{ \sum^{\infty} a_n x^n : a_n \in R,\ a_n = 0 \text{ for } n \gg 0 \right\}.$$

$$R[x,\delta] := \left\{ \sum_{n=0}^{\infty} a_n x^n \;:\; a_n \in R,\ a_n = 0 \text{ for } n \gg 0 \right\}.$$

Addition is usual.

Multiplication: $x \cdot a = ax + \delta(a)$.

EXAMPLE. ① $R = k[y,z]$, $\delta = \dfrac{\partial}{\partial y}$.

$S = R[x,\delta]$.

Let $a = y^2 + 2yz \in S$.

Then, $x \cdot a = a \cdot x + \delta(a)$

$= y^2 x + 2yzx + 2y + 2z$.

② Same as above but $\delta = \dfrac{\partial}{\partial z}$.

$x \cdot a = y^2 x + 2yzx + 2y$.

Theorem. Let R be left Noetherian, and $\delta : R \to R$ a derivation.
Then, $R[x,\delta]$ is left Noetherian.
("right" as well.)

Proof. $S := R[x,\delta]$. Let $0 \neq I \subseteq S$ be a left ideal.

x need not be in the center anymore. ($x \in Z(S) \iff \delta \equiv 0$.)

Let $f = a_0 + a_1 x + \cdots + a_n x^n \in I$, $a_n \neq 0$.

Then, $x \cdot f = a_0 x + \delta(a_0) + a_1 x^2 + \delta(a_1)x + \cdots + a_n x^{n+1} + \delta(a_n)x^n$.

Then, $LC(xf) = a_{n+1}$.

Thus, the same proof as earlier goes through. ∎

Lecture 10 (11-02-2022)

11 February 2022 17:34

Krull Schmidt Theorem

Defn. Let $R \neq 0$ be a ring. Let $E \neq 0$ be an R-module.
E is said to be decomposable if $E = E_1 \oplus E_2$ for some nonzero submodules E_1, E_2.
E is said to be indecomposable if it is not decomposable.

- Ring structure on $\underbrace{\mathrm{Hom}_R(E,E)}_{= \mathrm{End}_R(E)}$ is given by pointwise $+$ and composition $(f \cdot g := f \circ g)$ as the multiplication.

If $E \neq 0$, then $\mathrm{Hom}_R(E,E) \neq 0$ as 0 and id_E are distinct endomorphisms.

Defn. A ring $S \neq 0$ is said to be local if the set of nonunits is a two-sided ideal.

Lemma 1 $\mathrm{End}_R(E)$ is local $\Rightarrow$ E is indecomposable.
($\Downarrow E \neq 0$)

Proof. Suppose not. Write $E = E_1 \oplus E_2$ for $E_1, E_2 \neq 0$.
We have the projection maps $\pi_1, \pi_2 \in \mathrm{End}_R(E)$.
π_1, π_2 are not onto. Thus, π_1, π_2 are nonunits.
Thus, $\pi_1 + \pi_2$ ($= id_E$) is a nonunit. $\rightarrow\leftarrow$ ∎

EXAMPLE. Converse not true. $\mathbb{Z}$ is indecomposable but $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ is NOT local.

Lemma 2 Let $E \overset{\neq 0}{}$ be a finite length module (Noetherian + Artinian).
E indecomposable $\Rightarrow$ $\mathrm{End}_R(E)$ is local.

Before that, we prove something else:

Setup

Let $E \neq 0$ be a finite length module (possibly decomposable).
(Artinian + Noetherian)

By assumption, $(\ker(u^n))_{n\geq 1}$ and $(\operatorname{im}(u^n))_{n\geq 1}$ stabilise, say to $\ker(u^\infty)$ and $\operatorname{im}(u^\infty)$, respectively.

Lemma 3. (Fitting Lemma) With the above notation, we have:

(1) $E = \operatorname{im}(u^\infty) \oplus \ker(u^\infty)$.

(2) $u(\ker u^\infty) \subseteq \ker u^\infty$. $u|_{\ker u^\infty}$ is nilpotent.

(3) $u(\operatorname{im} u^\infty) \subseteq \operatorname{im} u^\infty$. $u|_{\operatorname{im} u^\infty}$ is an isomorphism.

Proof. Let $N \gg 0$ be s.t. $\ker u^N = \ker u^\infty$ and $\operatorname{im} u^\infty = \operatorname{im} u^N$.

(1) **Claim (i)** $\ker u^\infty \cap \operatorname{im} u^\infty = 0$.

Proof. Let $x \in \ker u^\infty \cap \operatorname{im} u^\infty$.

$x = u^N(y)$. Also, $0 = u^N(x) = u^{2N}(y)$.

$\therefore y \in \ker u^{2N} = \ker u^N$. $\therefore x = u^N(y) = 0$. ∎

Claim (ii) $\operatorname{im} u^\infty + \ker u^\infty = E$.

Proof. Let $x \in E$.

$u^N(x) \in \operatorname{im} u^N = \operatorname{im} u^{2N}$. $\therefore u^N(x) = u^{2N}(y)$ for some $y \in E$.

Now, $x = \underset{\in \operatorname{im} u^N}{u^N(y)} + \underset{\in \ker u^N}{\left(x - u^N(y)\right)}$. ∎

Thus, $E = \ker u^\infty \oplus \operatorname{im} u^\infty$.

(2) $u(\ker u^\infty) \subseteq \ker u^\infty$ is clear.

Indeed, if $x \in \ker u^\infty = \ker u^N$, then $u^N(ux) = 0$.

Thus, u is an endomorphism of $\ker u^\infty$.

Check that $(u|_{\ker u^\infty})^N = 0$.

Check that $(u|_{\ker u^\infty})^N = 0$.

If $x \in \ker u^\infty$, then $x \in \ker u^N$. Thus, $u^N(x) = 0$. ∎

(3) Check $u(\operatorname{im} u^\infty) \subseteq \operatorname{im} u^\infty$.

Let $\alpha = u|_{\operatorname{im} u^\infty} \in \operatorname{End}_R(\operatorname{im} u^\infty)$.

As $\operatorname{im} u^\infty$ is Artinian, it suffices to show that α is injective.

It follows that α is an iso.

But $\ker(\alpha) = 0$ follows essentially by proof of Claim (i). ∎

Now, we prove Lemma 2. : E indec + finite length $\Rightarrow \operatorname{End}_R(E)$ is local.

Proof. Let $S = \operatorname{End}_R(E) \neq 0$ (as $E \neq 0$).

Let $J = \{u : E \to E \mid u \text{ is a nonunit}\}$

Let $u \in J$ be arbitrary.

Fitting: $E = \operatorname{im} u^\infty \oplus \ker u^\infty$.

Indecom: $E = \operatorname{im} u^\infty$ or $\ker u^\infty$.

But $u|_{\operatorname{im} u^\infty}$ is iso. $\therefore \operatorname{im} u^\infty = 0$.

Thus, $\ker u^\infty = E$ and every $u \in J$ is nilpotent.

Conversely, any nilpotent is in J

To show: that J is an ideal.

As E is finite length, we see that nonunit $\Leftrightarrow$ not 1-1 $\Leftrightarrow$ not onto.

Let $u \in J$, $v \in S$. Then, $u \circ v$ is not onto and $v \circ u$ is not 1-1.

Lastly, let $u, v \in J$. TS: $u + v \in J$.

Suppose $u + v$ is invertible.

Let $\xi_1 = u \circ (u+v)^{-1}$, $\xi_2 = v \circ (u+v)^{-1}$.

Then, $\xi_1, \xi_2 \in J$ by earlier and $\xi_1 + \xi_2 = 1$.

Note $\xi_1 = 1 - \xi_2$ is invertible $\left((1-\xi_2)^{-1} = 1 + \xi_2 + \xi_2^2 + \dots\right)$.

This is a contradiction. ∎