Lecture 26: R[X]-module & R-linear Endomorp; Caley-Hamilton thm

11 November 2020
20:36

Recall: Let R be a comm ring with unity and M, N be R-mod

then 1) $\mathrm{Hom}_R(M,N)$ is an R-mod.

2) $\mathrm{End}_R(M)$ is an R-algebra (i.e. $\mathrm{End}_R(M)$ is a ring & there is a ring homo $R \to \mathrm{End}_R(M)$)

$r \mapsto \mu_r : M \to M$, $m \mapsto rm$

- Finitely generated R-modules
- Free modules. f.g. free R-mod is isom to R^n for some n.
- M, N are R-modules then $M \oplus N$ is an R-module via the scalar multip. $r\cdot(m,n) = (r\cdot m, r\cdot n)$

Example: 1) $R = \mathbb{Z}$, $M = \mathbb{Z}/5\mathbb{Z}$

$$\mathrm{End}_{\mathbb{Z}}(M) = \mathrm{Hom}(\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$$
$$f \longmapsto f(1)$$

$$\mathbb{Z} \longrightarrow \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z}) \longrightarrow \mathbb{Z}/5\mathbb{Z}$$
$$1 \longmapsto \bar{1}$$

2) $R = \mathbb{Q}$, $M = \mathbb{Q}^n$ then $\mathrm{End}_{\mathbb{Q}}(M) \overset{?}{=} M_{n\times n}(\mathbb{Q})$

$$\mathbb{Q} \longrightarrow M_{n\times n}(\mathbb{Q})$$
$$r \longmapsto rI$$

Facts:
- M an R-mod then $\mathrm{Hom}_R(R, M) \cong M$
- M, N, K R-mod then $\mathrm{Hom}_R(M, N\oplus K) \cong \mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(M,K)$

  and $\mathrm{Hom}(M\oplus N, K) \cong \mathrm{Hom}(M,K) \oplus \mathrm{Hom}(N,K)$

- $\mathbb{Q}$ is a $\mathbb{Z}$-module which is not free.
- R a comm ring with unity & S a mult subset of R then $S^{-1}R$ is an R-mod.
- In fact $\varphi: R_1 \to R_2$ is a ring homo. then R_2 is a R_1-mod via for $r \in R_1$ & $m \in R_2$

$$r \cdot m := \varphi(r) \cdot_{R_2} m.$$

⊛ Let R be a ring and M be an $R[x]$-mod where $R[x]$ is the poly ring over R.

Then note that M is also an R-module since R is a subring of $R[x]$.

Note $\varphi : M \longrightarrow M$ is a R-lin map.
$m \longmapsto x \cdot m$

$$\{R[X]\text{-modules}\} \underset{\theta_2}{\overset{\theta_1}{\rightleftarrows}} \left\{\begin{array}{c}R\text{-modules} + \\ \text{an } R\text{-lin endo of the module}\end{array}\right\}$$

⊛ Conversely let M be an R-mod & $\varphi \in \mathrm{End}_R(M)$ then

for $f(x) \in R[x]$ and $m \in M$ define

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$

$$f(x)\cdot m := a_n \cdot \varphi^n(m) + a_{n-1}\cdot \varphi^{n-1}(m) + \dots + a_1\varphi(m) + a_0 \cdot m$$
$$:= f(\varphi)(m)$$

Claim: This makes M into an $R[x]$-module

* $f(x), g(x) \in R[x]$ then

$$\begin{aligned}(f(x)+g(x))\cdot m &= (f+g)(\varphi)(m) \\ &= (f(\varphi)+g(\varphi))(m) \\ &= f(\varphi)(m) + g(\varphi)(m) \\ &= f(x)\cdot m + g(x)\cdot m\end{aligned}$$

Note that $x \cdot m = \varphi(m)$ and hence

$$\begin{aligned}x^2 \cdot m = x\cdot(x\cdot m) &= x \cdot \varphi(m) \\ &= \varphi(\varphi(m)) = \varphi^2(m)\end{aligned}$$

So more generally $f(x)\cdot m = f(\varphi)(m)$.

Hence $\Theta_2 \circ \Theta_1$ gives you isom objects. i.e. we recover the $R[x]$-module M.

Now going the other way, we start with R-mod M & $\phi \in End_R(M)$ then $R[x]$-mod str on M is defined so that $x \cdot m = \phi(m)$.

And then from this $R[x]$-mod M we get linear map. by mult. by x.

Hence the linear map is ϕ.

⊛ If $\mu: R \longrightarrow End_R(M)$ is injective then M is called a faithful

$r \longmapsto \mu_r : m \longmapsto rm$

R-module.

⊛ Let M be an R-mod $m \in M$, then annhilator of m,

$$ann(m) = \{ r \in R \mid rm = 0_M \} \subseteq R \quad \text{is an } R\text{-ideal}.$$

Let $N \subseteq M$ be R-submod then annhilator of N,

$$Ann(N) = \bigcap_{m \in N} ann(m) = \{ r \in R \mid rm = 0 \ \forall m \in N \}$$ is also an R-ideal.

HW Show that M is a faithful R-mod iff $Ann(M) = 0$.

Caley-Hamilton theorem: Let R be a ring and $A \in M_{n \times n}(R)$. Let $p_A(x) = \det(XI - A) \in R[X]$. Then $p_A(A) = 0$ in $End_R(R^n)$.

Thm: Let M be a f.g. R-mod. and $\phi \in End_R(M)$ s.t. $\phi(M) \subseteq IM$ where I is an R-ideal.

Then $\phi^n + a_1 \phi^{n-1} + \dots + a_{n-1}\phi + a_n = 0$ for some $a_i \in I^i$, $1 \le i \le n$.

Cor (Nakayama's): Let M be f.g. R-module s.t. $M = IM$ for some ideal $I \subseteq Jac(R)$ then $M = 0$.