Lecture 32: Structure theorem continued.

27 November 2020
10:22

Recall:

Thm (Str thm): Let R be a PID and M be a f.g. R-mod. Then

$$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

where $k = \text{rank}(M)$ and $a_1, \dots, a_m \in R$ are nonzero nonunits s.t. $a_1 | a_2 | a_3 | \cdots | a_m$. Here k and m could be 0.

Prop: Let R be a PID and F be a free R-module of rank n. Let N be a submodule of F. Then N is a free R-mod of rank $m \leq n$. Moreover there is a basis $x_1, \dots, x_n$ of F and $\exists\, a_1, \dots, a_m \in R^\times$ s.t. $a_1 | a_2 | \cdots | a_m$ and $\{a_1 x_1, a_2 x_2, \dots, a_m x_m\}$ is a basis of N.

Prop $\Longrightarrow$ str thm ✓

Pf of Prop: $N = 0$ ✓. So assume $N \neq 0$.

Let $\Sigma = \{ \varphi(N) \mid \varphi : F \to R \text{ is } R\text{-linear map} \}$.

The Σ is a collection of ideals of R. Since R is noeth & Σ is nonempty, it has a maximal element say $\nu(N)$ for some $\nu : F \to R$ R-linear. i.e. $\nu \in \text{Hom}_R(F, R)$.

$\nu(N)$ is a principal ideal generated by say a_1

i.e. $(a_1) = \nu(N) = a_1 R$.

Note $a_1 \neq 0$ $\left(\because \begin{array}{l} \pi_i : \underset{R^n}{\overset{\shortparallel}{F}} \longrightarrow R \quad 1 \leq i \leq n \\ \pi_i(N) = 0 \ \forall \ i \Rightarrow N = 0 \end{array} \right)$

$\exists \ x \in N$ s.t. $\nu(x) = a_1$. $\Leftarrow$

<u>Claim</u>: $a_1 \mid \varphi(x) \quad \forall \ \varphi \in \mathrm{Hom}_R(F, R)$

<u>Pf</u>: Let $d = \gcd(a_1, \varphi(x))$

$d = r_1 a_1 + r_2 \varphi(x)$ for some $r_1, r_2 \in R$.

$\psi : F \longrightarrow R$ is R-lin

$\psi = r_1 \nu + r_2 \varphi$

$\Rightarrow \psi(N) \ni \psi(x) = r_1 \nu(x) + r_2 \varphi(x)$
$= d$

$\Rightarrow \psi(N) \in \Sigma$ & $a_1 \in (d)$

$\Rightarrow (a_1) = \nu(N) \subseteq (d) \subseteq \psi(N)$

<u>By maximality $\nu(N)$</u> $\Rightarrow$ $(a_1) = (d)$

$\Rightarrow a_1 \mid \varphi(x)$.

$a_1 \mid \pi_i(x) \quad \forall\, 1 \le i \le n \qquad \pi_i : F \to R$ are projection maps.

Let $b_i = \pi_i(x) \quad 1 \le i \le n$

$b_i = a_1 c_i \quad 1 \le i \le n$ for some $c_i \in R$

Note $x = \sum b_i e_i = \sum_{i=1}^{n} a_1 c_i e_i$ where e_i are the std basis $F = R^n$.

$= a_1 \sum_{i=1}^{n} c_i e_i$

Let $x_1 = \sum_{i=1}^{n} c_i e_i \Rightarrow a_1 x_1 = x$

Claim ①: (i) $F = Rx_1 \oplus \ker(\nu)$

(ii) $N = Ra_1x_1 \oplus (\ker(\nu) \cap N)$

Let $y \in F$ then

$$y = \underbrace{\nu(y)x_1}_{\in Rx_1} + \overbrace{y - \nu(y)x_1}^{\in \ker(\nu)}$$

$\nu(y - \nu(y)x_1)$

$= \nu(y) - \nu(y)\nu(x_1)$

$\left(\because a_1 = \nu(x) = \nu(a_1 x_1) = a_1 \nu(x_1) \Rightarrow \nu(x_1) = 1 \quad (\because a_1 \ne 0) \right)$

$= 0$

$\Rightarrow F = Rx_1 + \ker(\nu)$

Let $y \in Rx_1 \cap \ker(\nu)$

$\Rightarrow y = rx_1$ for some $r \in R$

& $\nu(y) = 0 \Rightarrow \nu(rx_1) = 0$

$\Rightarrow r\,\nu(x_1) = 0 \Rightarrow r = 0 \quad (\because \nu(x_1) = 1)$

$\Rightarrow y = 0.$ Hence (i)

$y \in N$ then

$y = \nu(y)x_1 + y - \nu(y)x_1$

$\nu(y - \nu(y)x_1) = \nu(y) - \nu(y)\nu(x_1) = 0 \quad (\because \nu(x_1) = 1)$

$\Rightarrow \quad y - \nu(y)x_1 \in \ker(\nu)$

So enough to show $\nu(y)x_1 \in Ra_1x_1$

$\left(\because \; Ra_1x_1 = Rx \subseteq N \;\&\; y \in N \right.$
$\left. \Rightarrow \; y - \nu(y) \in N \right)$

$\nu(y) \in \nu(N) \quad (\because y \in N)$
$\qquad\;\; \| $
$\qquad a_1R$

$\Rightarrow \; \nu(y)x_1 \in a_1Rx_1 = Ra_1x_1$

$\Rightarrow N = Ra_1x_1 + (\ker(\nu) \cap N)$

$y \in Ra_1x_1 \cap (\ker(\nu) \cap N)$

$\Rightarrow \; y = ra_1x_1$ for some $r \in R$

and $\nu(y) = 0 \Rightarrow \nu(ra_1x_1) = 0$

$\Rightarrow ra_1 = 0$ in R

$\Rightarrow r = 0 \; . \; (\because a_1 \neq 0)$

$\Rightarrow y = 0$. Hence (ii) .

Note that $N = Ra_1x_1 \oplus (\ker(\nu) \cap N)$

$\Rightarrow \operatorname{rank}(N) = 1 + \operatorname{rank}(\ker(\nu) \cap N)$ -- ⊛

Induct on rank of N,

⊛ $\operatorname{rank}(\ker(\nu) \cap N) < \operatorname{rank}(N) = m$

and $\ker(\nu) \cap N$ is a R-submod of F.

Hence ind hyp $\ker(\nu) \cap N$ is free R-mod of rank $\operatorname{rank}(N) - 1$.

Also $Ra_1x_1 \cong R$ as R-module

$\Rightarrow N$ is free as N is direct sum of $\underset{R}{\underset{\cong}{Ra_1x_1}}$ & $\underset{R^{m-1}}{\underset{\cong}{\ker(\nu) \cap N}}$.

Now for the remaining part

We induct on $n = \text{rank}(F)$.

$\ker(\nu) \oplus Rx_1 = F$.

$\Rightarrow \text{rank}(\ker(\nu)) = n-1$ & $\ker(\nu)$ is free

(Since we showed every submod of F is free)

$\Rightarrow$ $\ker(\nu)$ is free of rank $n-1$

and $N \cap \ker(\nu) \subseteq \ker(\nu)$

So by ind hyp, $\ker(\nu)$ has a basis $\{x_2, \dots, x_n\}$ and $\exists a_2, \dots, a_m \in R^{\times}$ s.t. $a_2 | a_3 | \dots | a_m$

$\{a_2 x_2, \dots, a_m x_m\}$ is a basis of $N \cap \ker(\nu)$.

claim ⊛

$\Rightarrow$ $\{x_1, \dots, x_n\}$ is a basis of F

& $\{a_1 x_1, a_2 x_2, \dots, a_n x_n\}$ is a basis of N.

$\Sigma = \{ \varphi(N) \mid \varphi \in \mathrm{Hom}(F, R) \}$

& (a_1) is the maximal element of Σ.

a_2 is s.t.

the maximal element of

$\{ \varphi(N \cap \ker(\nu)) \mid \varphi \in \mathrm{Hom}(\ker(\nu), R) \}$

$a_2 = \nu_2(N \cap \ker(\nu))$

$\mu : Rx_1 \oplus \ker(\nu) \longrightarrow R$

$\mu(x_1) = \nu(x_1)$ & $\mu|_{\ker(\nu)} = \nu_2$

Then $\mu : F \to R$ is R-lin. $\mu(rx_1 + \kappa) = r\nu(x_1) + \nu_2(\kappa)$

$\mu(N) \ni \mu(a_1 x_1) = \nu(\underbrace{a_1 x_1}_{= x}) = a_1$

$\Rightarrow (a_1) \subseteq \mu(N) \Rightarrow (a_1) = \mu(N)$

$\mu(N) \supseteq \nu_2(\ker(\nu)) = (a_2)$

$\Rightarrow a_2 \in (a_1) \Rightarrow a_1 \mid a_2$.