Lecture 46

Wednesday, April 22, 2015 10:09 AM

__Claim__ (a) $M = Ry_1 \oplus \ker(\nu)$

(b) $N = Ra_1y_1 \oplus (N \cap \ker \nu)$

__Pf__ (a) For $x \in M$, $x = \nu(x)y_1 + (x - \nu(x)y_1)$

$$\nu(x - \nu(x)y_1) = \nu(x) - \nu(x)\nu(y_1)$$

$$= \nu(x) - \nu(x) \cdot 1$$

$$= 0$$

$\Longrightarrow x - \nu(x)y_1 \in \ker(\nu)$

Thus $M = Ry_1 + \ker(\nu)$

$Ry_1 \cap \ker \nu = 0$?

If $ry_1 \in \ker \nu \Longrightarrow 0 = \nu(ry_1) = r\nu(y_1)$

$= r \Longrightarrow r = 0$

$\Longrightarrow Ry_1 \cap \ker \nu = 0$.

(b) Since $(a_1) = \nu(N)$, $a_1 \mid \nu(x') \;\forall x' \in N$.

If $\nu(x') = ba_1$, then $x' = \nu(x')y_1 + (x' - \nu(x')y_1)$

$$= ba_1y_1 + \underbrace{(x' - ba_1y_1)}_{\in \ker \nu \cap N}.$$

$Ra_1y_1 \cap (N \cap \ker\nu) = 0$ as before, so

$N = Ra_1y_1 \oplus (N \cap \ker\nu)$.

Pf of ① : By induction on rank of N, m:

If $m=0$, $N=0$, done. If $m>0$, then $N \cap \ker\nu$ has rk $m-1$. By ind hyp, $N \cap \ker\nu$ is free of rk $m-1$. Thus N is free of rk $m-1$ by adding a_1y_1 to basis.

Pf of ② By induction on $rk(M) = n$:

$\ker(\nu)$ is free of rk $n-1$. By ind hyp applied to $N \cap \ker(\nu) \subseteq \ker(\nu)$, get a basis $y_2, \ldots, y_n$ of $\ker(\nu)$ and $a_i \in R$ s.t. $a_2y_2, \ldots, a_my_m$ are a basis of $N \cap \ker(\nu)$ and $a_2 | \cdots | a_m$. Done if $a_1 | a_2$.

Define $\varphi : M \longrightarrow R$ by $y_1, y_2 \longmapsto 1$, $y_i \longmapsto 0$ for $i>2$.

$a_1 = \varphi(a_1 y_1)$ so $a_1 \in \varphi(N)$ so $(a_1) \subseteq \varphi(N)$.

By maximality, $(a_1) = \varphi(N)$.

$a_2 = \varphi(a_2 y_2) \in \varphi(N) \Rightarrow a_2 \in (a_1)$

i.e. $a_1 \mid a_2$. $\square$

<u>Thm</u> R a PID, M a f.g. R-mod

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

for some $r \geq 0$, $a_i \in R \setminus (R^\times \cup 0)$ s.t.

$$a_1 \mid a_2 \mid \cdots \mid a_m .$$

<u>Cor</u> • M is torsion free iff M is free

• $\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$. $\square$

<u>Pf of Thm</u> Take $\{x_1, \ldots, x_n\}$ a set of generators of M of minimal cardinality. Define

$$\pi : R^n \twoheadrightarrow M \quad \text{surj } R\text{-mod hom}$$
$$e_i \longmapsto x_i \qquad \text{so } M \cong R^n/\ker \pi .$$

Use the main lemma to choose a basis $y_1, \dots, y_n$ of R^n & $a_1 y_1, \dots, a_m y_m$ of $\ker(\pi)$ where $a_1 | \cdots | a_m$. Then

$$M \cong R^n / \ker \pi = (Ry_1 \oplus \cdots \oplus Ry_n) / (Ra_1y_1 \oplus \cdots \oplus Ra_my_m)$$

Consider $Ry_1 \oplus \cdots \oplus Ry_n \longrightarrow R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$

$$(\alpha_1 y_1, \dots, \alpha_n y_n) \longmapsto (\alpha_1 \bmod (a_1), \dots, \alpha_m \bmod (a_m), \alpha_{m+1}, \alpha_{m+2}, \dots, \alpha_n)$$

Ther kernel is clearly $Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_m \oplus 0 \oplus \cdots \oplus 0$. $= \ker \pi$. Thus $M \cong R^{n-m} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$.

If $a \in R^\times$, then $R/(a) = 0$, so we can remove any $R/(a_i)$'s w/ $a_i \in R^\times$. What remains is the structure thm!

$\square$

Elementary divisor form of the structure thm:

M is a f.g. module over a PID R, then

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$$

for some $r \geq 0$ & $p_i^{\alpha_i}$ positive powers of primes in R. (Note p_i's not necessarily distinct.)

e.g. $R = \mathbb{Z}$.

$$\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Defn In str thm decomposition, r = free rank of M, a_i invariant factors of M, $p_i^{\alpha_i}$ elementary divisors of M.

Q How do we translate b/w a_i's & $p_i^{\alpha_i}$'s?

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/225\mathbb{Z}$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}/169\mathbb{Z}$$

$$\cong \mathbb{Z}/(3\cdot 13) \oplus \mathbb{Z}/(9\cdot 169)$$

<u>Thm</u> Invt factor & elementary divisor forms are unique. (up to mult ~~by~~ a unit & permutation [for elementary divisors])