4/22/16

1

Lecture 37 Friday April 22

Assume R is a PID

We now consider the implications of Thm 25 for finitely generated R-modules.

Given a fg R-module U

Given a finite generating set for U:

$$u_1, u_2, \ldots, u_n$$

So

$$U = Ru_1 + Ru_2 + \cdots + Ru_n$$

The map

$$\varphi \quad \begin{array}{ccc} R^n & \longrightarrow & U \\ (a_1, a_2, \ldots, a_n) & \longrightarrow & a_1u_1 + a_2u_2 + \cdots + a_nu_n \end{array}$$

is a surjective R-module hom.

Write

$$W = \ker(\varphi)$$

The map φ induces an R-module iso

$$\begin{aligned} R^n/W &\longrightarrow \mathcal{U} \\ x+W &\longrightarrow \varphi(x) \end{aligned}$$

Write

$$m = \operatorname{rank}(W)$$

By Thm 25 $\exists$ lin indep gens $v_1, v_2, \ldots, v_n$ for R^n and nonzero $d_1, d_2, \ldots, d_m$ in R such that both

(i) $\quad d_1 / d_2 / \cdots / d_m$

(ii) $\quad W = R d_1 v_1 + R d_2 v_2 + \cdots + R d_m v_m$

The sum

$$R^n = R v_1 + R v_2 + \cdots + R v_n$$

is direct

For $m+1 \le i \le n$ define

$$d_i = 0$$

the sum

$$W = Rd_1v_1 + Rd_2v_2 + \cdots + Rd_nv_n$$

is direct

For $1 \le i \le n$ define

$$U_i = \varphi(Rv_i)$$

So U_i is an R-submodule of U

the R-module $U_i = R\varphi(v_i)$ is cyclic

By constr the sum

$$U = \sum_{i=1}^{n} U_i$$ is direct *

For $1 \le i \le n$

$$\mathrm{Ann}(U_i) = Rd_i$$

So

$$U_i \text{ is torsion-free iff } d_i = 0$$

$$U_i = 0 \quad \text{iff} \quad d_i \text{ is a unit in } R$$

Assume d_i is non0 and not a unit in R.

Then the map

$$R/Rd_i \longrightarrow U_i$$

$$r + Rd_i \longrightarrow r\varphi(v_i)$$

is an R-module iso.

Define

$$s = \left| \left\{ i \,/\, 1 \le i \le m,\ d_i \text{ not a unit in } R \right\} \right|$$

So for $1 \le i \le m$

d_i is a unit if $i \le m-s$

d_i is not a unit if $i > m-s$

Define

$D_i = d_{m-s+i} \qquad 1 \le i \le s$

Each of

$D_1, D_2, \ldots, D_s$ is nonzero, not a unit in R

Also

$D_1 \mid D_2 \mid \cdots \mid D_s$

Define $t = n - m$

By * and above comments $\exists$ R-module iso

$$U \cong R/RD_1 \times R/RD_2 \times \cdots \times R/RD_s \times R^t \quad ☆$$

From ☆ we see

$$t = \operatorname{rank}(U)$$

$$\operatorname{Tor}(U) \underset{\binom{R\text{-mod}}{\text{iso}}}{\cong} R/RD_1 \times R/RD_2 \times \cdots \times R/RD_s \quad ☆☆$$

So

U is tor-free iff $s = 0$

U is torsion iff $t = 0$

In this case

$$\operatorname{Ann}(U) = RD_s$$

Comparing ☆, ☆☆ we see $\exists$

R-submodule F of U st both

(i) the sum $U = Tor(U) + F$ is direct

(ii) $\exists$ R-module iso $F \simeq R^t$

(F not unique in general)

Refering to ☆ we will show

- the integers s, t are uniquely determined by U
- For $1 \le i \le s$
  D_i is uniquely determined up to mult by a unit in R

Call t the <u>free rank</u> of U.

For $1 \le i \le s$ Call

D_i the <u>ith invariant factor</u> of U.

Call ☆ the <u>invariant factor decomp</u> of U.

We now modify ☆ to get the elementary divisor decomp of $\mathcal{U}$.

<u>Aside</u> Given a commutative ring R with $1 \neq 0$.

Given ideals A, B of R st $A+B = R$

By Chinese Remainder thm $\exists$ ring iso

$$\theta : \begin{array}{ccc} R/AB & \longrightarrow & R/A \times R/B \\ r + AB & \longrightarrow & (r+A, \ r+B) \end{array}$$

Each of R/AB, R/A, R/B

has an R-module structure.

For instance take R/A. Consider R-module R

Ideal A is an R-submodule of R

this yields quotient R-module R/A

LEM 26 With above notation

θ is an iso of R-modules.

pf Fix $x \in R/AB$ and $s \in R$ show

$$s\,\theta(x) \overset{?}{=} \theta(sx)$$

Write

$$x = r + AB$$

$$\underbrace{s\,\underbrace{\theta(r+AB)}_{(r+A,\ r+B)}}_{(s(r+A),\ s(r+B))} \overset{?}{=} \underbrace{\theta(\underbrace{s(r+AB)}_{sr+AB})}_{(sr+A,\ sr+B)}$$

$$(s(r+A),\ s(r+B)) = (sr+A,\ sr+B)$$

OK

$\square$

Back to U

Assume $s \geq 1$

Consider D_s

Factor D_s into irreducibles: up to associates

$$D_s = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \qquad r, e_1, e_2, \ldots e_r > 0$$

p_i, p_j not associates if $i \neq j$ $\quad (1 \leq i, j \leq r)$

For $1 \leq k \leq s$ recall $D_k \mid D_s$,

WLOG

$$D_k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$0 \leq \alpha_1 \leq e_1, \quad 0 \leq \alpha_2 \leq e_2, \quad \ldots, \quad 0 \leq \alpha_r \leq e_r$

For $1 \leq i, j \leq r$ with $i \neq j$

$p_i^{\alpha_i}, \quad p_j^{\alpha_j}$ rel prime

So $\quad R = R p_i^{\alpha_i} + R p_j^{\alpha_j}$

Now by CH REM thm and the aside

$\exists$ R-module iso

$$R/R\alpha \cong R/Rp_1^{\alpha_1} \times R/Rp_2^{\alpha_2} \times \cdots \times R/Rp_r^{\alpha_r}$$

Now ✡ yields the following result.

Thm 27 Assume R is a PID

Let U denote a fg R-module

Then U is a direct sum of finitely many cyclic R-modules, each of whose annihilator is 0 or generated by a power of a prime in R.

"elementary divisor decomp"

— o —

Referring to Thm 27, we will see that the prime powers are uniquely determined by U (up to associates)

We call these prime powers the <u>elementary divisors</u> of U.