Lecture 35 Monday April 18

Recall R is a commutative ring with $1 \neq 0$

Assume R is an integral domain

Consider the free R-module R^n

Given an R-submodule W of R^n

Recall W is torsion-free with $\underset{m}{\underset{\shortparallel}{\operatorname{rank}(W)}} \leq n$

<u>Question</u>: Does there exist an R-module iso

$W \cong R^m$?

We will show: ans is "No" in general
ans is "yes" if R is a PID

The next example shows that the ans is "No" in general.

Ex 20 Assume R is an integral domain.

Consider the R-module R, which is free of rank 1

For a subset $W \subseteq R$, W is an R-submodule of R

iff W is an ideal of the ring R

Assume W is an R-submodule of R

Obs $\qquad \mathrm{rank}(W) \leq 1$

Assume $W \neq 0$

Pick $\quad 0 \neq w \in W$

w is torsion-free, hence lin indep.

So $\qquad \mathrm{rank}(W) \geq 1$

So $\qquad \mathrm{rank}(W) = 1$

We claim TFAE:

(i) $\exists$ R-module iso $W \cong R$

(ii) the ideal W is principal

pf claim

$(i) \to (ii)$ $\exists$ R-module iso $\varphi: R \to W$

write

$$a = \varphi(1)$$

For $r \in R$,

$$\varphi(r) = r\varphi(1) = ra$$

the map φ is surjective so

$$W = Ra$$

the ideal W is principal

$(ii) \to (i)$ write $W = Ra$

the map

$$\varphi: \begin{array}{l} R \to W \\ r \mapsto ra \end{array}$$

is an R-module iso $\square$

—— o ——

Next goal: For R a PID, show the above question has answer "yes".

Assume R is an integral domain.

Given an R-module V and an integer $n \geq 0$

Given a surjective R module hom

$$\varphi : V \to R^n$$

For $1 \leq i \leq n$ pick $v_i \in V$ such that

$$\varphi(v_i) = (0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0) = e_i$$

obs

$v_1, v_2, \ldots, v_n$ lin indep.

So the R-submodule

$$W = \sum_{i=1}^{n} R v_i$$ is iso to R^n

LEM 21 With above notation,

$$V = W + \underset{\overset{\shortparallel}{K}}{\ker(\varphi)} \qquad \text{(dir sum)}$$

pf <u>Show $W \cap K = 0$</u>

For $w \in W \cap K$ show $w = 0$.

4/18/16

5

Write
$$w = \sum_{i=1}^{n} a_i v_i \qquad a_i \in R$$

Apply φ:
$$0 = \varphi(w) = (a_1, a_2, \ldots, a_n)$$

So
$$a_i = 0 \qquad 1 \le i \le n$$

So
$$w = 0$$

Show $V = W + K$

For $v \in V$
$$\varphi(v) \in R^n$$

Write
$$\varphi(v) = (b_1, b_2, \ldots, b_n) \qquad b_i \in R$$

Also
$$\varphi\left(\sum_{i=1}^{n} b_i v_i\right) = (b_1, b_2, \ldots, b_n)$$

So
$$\varphi\left(v - \sum_{i=1}^{n} b_i v_i\right) = 0$$

So
$$v - \sum_{i=1}^{n} b_i v_i \in K$$

Now
$$v = \underbrace{\sum_{i=1}^{n} b_i v_i}_{\in W} + \underbrace{v - \sum_{i=1}^{n} b_i v_i}_{\in K}$$

$\square$

Prop 22 Assume R is a PID

Consider the free R-module R^n

Given an R-submodule W of R^n

Write $m = \text{rank}(W)$

Then $\exists$ R-module iso $W \simeq R^m$

pf By induction on m [Recall $0 \le m \le n$]

<u>Case $m=0$</u> Here $W=0$ ✓

<u>Case $m \geq 1$</u> Here $W \neq 0$

$\exists$ $0 \neq w \in W$

Write $w = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ $\alpha_i \in R$

$\exists i$ $(1 \le i \le n)$ st $\alpha_i \neq 0$

The map

$$\phi: \quad W \xrightarrow[\text{incl}]{} R^n \longrightarrow R$$
$$(a_1, \ldots a_n) \to a_i$$

is an R-module hom

The image $\phi(W)$ is a nonO ideal of R

Write

$$\phi(W) = R\theta \qquad 0 \neq \theta \in R$$

$\exists \ w_1 \in W$ such that

$$\phi(w_1) = \theta$$

$\forall \ w \in W$, $\exists$ unique element in R, denoted $\varphi(w)$, st

$$\phi(w) = \varphi(w)\theta$$

the map

$$\varphi : \begin{array}{ccc} W & \longrightarrow & R \\ w & \longrightarrow & \varphi(w) \end{array}$$

is an R-module hom.

Obs

$$\underset{\theta}{\underset{\|}{\phi(w_1)}} = \varphi(w_1)\theta$$

So

$$\varphi(w_1) = 1$$

So φ is surjective.

By LEM 21,

$$W = Rw_1 + \underset{K}{\underset{\|}{\ker(\varphi)}} \qquad \text{(dir sum)}$$

By Prop 19,

$$\underset{\overset{\shortparallel}{m}}{\operatorname{rank}(W)} = \underset{\overset{\shortparallel}{1}}{\operatorname{rank}(Rw_1)} + \operatorname{rank}(K)$$

So

$$\operatorname{rank}(K) = m-1$$

By induction $\exists$ R-module iso

$$K \cong R^{m-1}$$

We have R-module isomorphisms

$$\begin{array}{ccccc} W & \cong & Rw_1 & \times & K \\ & & \text{is} & & \text{is} \\ & & R & & R^{m-1} \end{array}$$

So

$$W \cong R^m$$

$\square$

To motivate the next thm we investigate some small examples.

LEM 23 Assume R is a PID

Consider the free R-module R^2 of rank 2.

Given an R-submodule W of R^2 with

$$\text{rank}(W) = 1.$$

Then $\exists$ lin indep gens v_1, v_2 of R^2 and $0 \neq d_1 \in R$ such that

$$W = R d_1 v_1$$

pf By Prop 22, W is cyclic:

$$W = Rw \qquad 0 \neq w \in R^2$$

Write

$$w = (a, b) \qquad a, b \in R \text{ not both } 0$$

<u>Case $a = 0$</u>

take $v_1 = (0, 1)$ $\quad v_2 = (1, 0)$

$$d_1 = b$$

<u>Case $b = 0$</u>

take $v_1 = (1, 0)$ $\quad v_2 = (0, 1)$

$$d_1 = a$$

Case $a \neq 0,\ b \neq 0$

Define $d_1 = GCD(a,b)$

Write $a = d_1 \alpha, \quad b = d_1 \beta \quad \alpha, \beta \in R$

So $GCD(\alpha, \beta) = 1$

$\exists\ r, s \in R$ st

$$r\alpha + s\beta = 1$$

Define

$$v_1 = (\alpha, \beta) \in R^2$$
$$v_2 = (-s, r) \in R^2$$

Define $A = \begin{pmatrix} \alpha & -s \\ \beta & r \end{pmatrix} \in Mat_2(R)$

$$\det(A) = r\alpha + s\beta = 1$$

So A^{-1} exists in $Mat_2(R)$

So v_1, v_2 lin indep gens for R^2

Obs $d_1 v_1 = (d_1\alpha, d_1\beta) = (a, b) = w$

So $W = Rw = R d_1 v_1$

$\square$

LEM 24 Assume R is a PID

Consider the free R-module R^2 of rank 2

Given an R-submodule $W \neq R^2$ that has

$$\mathrm{rank}(W) = 2.$$

Then $\exists$ lin indep gens v_1, v_2 of R^2 and

$\exists$ nonzero $d_1, d_2 \in R$ such that both

(i) $d_1 \mid d_2$

(ii) $W = R d_1 v_1 + R d_2 v_2$

pf (sketch) By Prop 22 $\exists$ lin indep

$$w_1, w_2 \in R^2$$

st

$$W = R w_1 + R w_2$$

[View elements in R^2 as col vectors]

Write $w_1 = \begin{pmatrix} a \\ c \end{pmatrix}$ $\quad w_2 = \begin{pmatrix} b \\ d \end{pmatrix}$

Define $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(R)$

$\det(A) \neq 0$ since w_1, w_2 lin indep.

Consider ideal of R

$$J = Ra + Rb + Rc + Rd$$

J is principal and $J \neq 0$

Write $J = Rd_1$ $\quad 0 \neq d_1 \in R$

Write $a = d_1\alpha$ $\quad b = d_1\beta$

$c = d_1\gamma$ $\quad d = d_1\delta$

$$\det(A) = ad - bc$$

$$= d_1 \underbrace{d_1(\alpha\delta - \beta\gamma)}_{\overset{\text{def}}{=} d_2}$$

So

$d_2 \neq 0$

$\det(A) = d_1 d_2$

$d_1 \mid d_2$

Write $v_1 = \begin{pmatrix} x \\ z \end{pmatrix}$ $\quad v_2 = \begin{pmatrix} y \\ w \end{pmatrix}$

Require

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \quad \text{a unit in } Mat_2(R)$$

Write

$$d_1 v_1 = r w_1 + t w_2 \qquad r, s, t, u \in R \qquad *$$

$$d_2 v_2 = s w_1 + u w_2 \qquad **$$

Require $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ a unit in $Mat_2(R)$

$*, **$ becomes

$$\underbrace{\begin{pmatrix} x & y \\ z & w \end{pmatrix}}_{P^{-1}} \underbrace{\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}}_{D} = \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} r & s \\ t & u \end{pmatrix}}_{Q}$$

Show $\exists$ units P, Q in $Mat_2(R)$ st

$$PAQ = D$$

This is routinely checked (ex)

$\square$