Lecture 28: Modules over PID's II

Recall: • Last time we talked about free modules over a PID R

$M \cong \bigoplus_{i \in I} R$ via a basis $\{e_i\}_{i \in I}$ (generates + LI/R)

• Defined Torsion elements: $x \in M$ with $\mathrm{Ann}(x) \neq (0)$

$M_{Tor} = \{$torsion elements$\}$ submodule of M

• M is Torsion free module $\iff M_{Tor} = \{0\}$

Theorem 1: Size of the basis of a free module is unique ($= \mathrm{rank}(M)$)

Theorem 2: F free module over PID & M submodule, then

M is free & $\mathrm{rank}(M) \leq \mathrm{rank}(F)$

• Torsion free + f.g $\not\Rightarrow$ free for general R

Proposition: M is f.g over a PID & M is torsion free $\Rightarrow$ free.

Theorem 3: Fix R a PID and M a f.g R-module. Then, M/M_{Tor} is a free R-module. Furthermore, there exists a free submodule F of M with $M = M_{Tor} \oplus F$. & rank(F) is uniquely determined by M.

Proof: • **Claim 1**: $\overline{M} = M/M_{Tor}$ is torsion free.

Pf/
Let $\overline{x} \in \overline{M}$ and $b \in R$ with $b\overline{x} = 0$ in $\overline{M}$. Then, $bx \in M_{Tor}$ so $\mathrm{Ann}(bx) \neq (0)$.
But $\mathrm{Ann}(bx) = (c)$ $c \neq 0$ gives $(bc)x = 0$ in M.

So either $bc = 0$ or $x \in M_{Tor}$ $(\Rightarrow \overline{x} = 0)$
$\Downarrow c \neq 0$
$b = 0$. & $\overline{x}$ is not a torsion element of $\overline{M}$

- M is fg, so $\overline{M}$ is fg
- $\overline{M}$ is fg & Torsion free. By Proposition, it is free as an R-module. It's rank is uniquely determined by M. To finish, build $\underset{\text{free}}{F \subseteq M}$ with $F \cong M/M_{Tor}$
- To find F, we need a lemma applied to $\varphi: M \twoheadrightarrow M/M_{Tor}$:

Lemma: Consider M & M' two modules over a PID R with M' free. Fix $f: M \longrightarrow M'$ a surjective homomorphism of R-modules. Then, there exists a free submodule N of M such that

(1) $f|_N$ induces an isomorphism $f|_N : N \xrightarrow{\sim} M'$.

(2) $M = N \oplus \operatorname{Ker} f$.

Proof: Pick a basis $B = \{x_i'\}_{i \in I}$ for M'. For each i, let $x_i \in M$ with $f(x_i) = x_i'$

Take $N = (x_i : i \in I)$

Claim: $\{x_i : i \in I\}$ is l.i.

Pf/ $\sum_{\substack{i \in I \\ \text{finite}}} a_i x_i = 0 \rightsquigarrow \sum_{\substack{i \in I \\ \text{finite}}} a_i \underbrace{f(x_i)}_{= x_i'} = 0 \underset{B \text{ basis}}{\Longrightarrow} a_i = 0 \ \forall i.$

Conclusion: N is free with basis $\{x_i\}_{i \in I}$. & $f|_N : N \twoheadrightarrow M'$

For $x \in M$ write $f(x) = \sum_{\substack{i \in I \\ \text{finite}}} a_i f(x_i) \Longrightarrow x - \sum_{\substack{i \in I \\ \text{finite}}} a_i x_i \in \operatorname{Ker} f$

. $\operatorname{Ker} f \cap N = (0)$. So $f|_N$ is iso & $M = N \oplus \operatorname{Ker} f$. $\square$

Definitions / Notation for Classification Thm

Fix R PID

Def: We say $p \in R$ is a prime element if $(0) \neq (p)$ is a prime ideal

Notation: given $a \in R \setminus \{0\}$, we write $\boxed{M_a} = \mathrm{Ker}(M \xrightarrow{a\cdot} M)$, $x \longmapsto a\cdot x$

We refer to a as an exponent for M

Def: An R-module M is cyclic if $M \simeq R/(a)$ for some a.

Recall: given $a \neq 0$ we can write $\boxed{a = u p_1^{n_1} \cdots p_s^{n_s}}$ ($u \in R^\times$, p_i primes, $n_i \geq 1$)

where $(a) = (p_1^{n_1}) \cap \cdots \cap (p^{n_s})$ is the unique prim decomp (R is PID)

- We select representatives for the prime elements of R, modulo units

$\rightsquigarrow$ factorization of any $a \in R \setminus \{0\}$ is unique!

Examples: $\mathbb{Z}$ $\rightsquigarrow$ positive prime numbers

$\mathbb{K}[x]$ $\rightsquigarrow$ monic irreducible polynomials ($LT(f) = 1$)

Def: A p-Torsion element is any $x \in M$ with $x \in M_{p^n}$ for some $n \geq 1$.

Def: A fg p-module M ($M = M_{p^n}$ for some n) has type $(p^{r_1}, \dots, p^{r_s})$ if it is isomorphic to $\bigoplus_{i=1}^{s} R/(p^{r_i})$

If p is understood, we say M has type $(r_1, \dots, r_s)$

Classification Thm: If $M \neq 0$ is a fg torsion module over a PID R, then:

$$(*) \quad M = \bigoplus_{p_i \text{ prime}} M_{p_i^{n_i}} \quad \text{for } n_i \geq 1 \ \text{(unique choice)}$$

Furthermore $(p = p_i)$: $M_{p^n} \cong R/(p^{\nu_1}) \oplus \cdots \oplus R/(p^{\nu_s})$ with $n = \nu_1 \geq \nu_2 \geq \cdots \geq \nu_s$

The sequence (ν_i) is uniquely determined by M & p. (Type of M_{p^n})

Proof: Today: Existence of the decomposition $(*)$ & uniqueness
Next time: type & uniqueness of type.

PART 1: $M = \bigoplus_{j=1}^{s} M_{p_{ij}^{n_{ij}}}$ $n_{ij} \geq 1$ p_{ij} prime reps in R

Claim 0: M has an exponent $a \neq 0$ with $\boxed{\mathrm{Ann}(M) = (a)}$ $a \notin R^{\times}$

Pf/ Write $M = (x_1, \ldots, x_n)$. We know $\mathrm{Ann}(x_i) = (a_i) \neq (0)$ because $M_{tor} = M$

Take $a = a_1 \cdots a_n \neq 0$ then $aM = \{0\}$.

$M \neq \{0\}$ so $\mathrm{Ann}(M) \neq R$ ☐

• Assume $a = bc$ with $(b,c) = 1$. Pick x, y with $1 = xb + yc$

Claim 1: $M = M_b \oplus M_c$

Pf) • $M_b \cap M_c = \{0\}$ since $m \in M_b \cap M_c$ forces $bm = 0$ & $cm = 0$

$\leadsto 1 \cdot m = (xb + yc) \cdot m = 0 + 0 = 0$

• $(\subseteq)$ Pick $m \in M$ Then $m = (xb + yc)m = \underbrace{xbm}_{=m_1} + \underbrace{ycm}_{=m_2} \in M_c + M_b$

$cm_1 = x\underbrace{cb}_{=a}m = x \cdot 0 = 0$ as $m_1 \in M_c$

$bm_2 = y\underbrace{bc}_{=a}m = y \cdot 0 = 0$ $\leadsto$ $m_2 \in M_b$ ☐

- We <u>factor</u> a as: $a = u p_{i_1}^{n_{i_1}} \cdots p_{i_r}^{n_r}$ $u \in R^\times$, p_{i_j} primes $n_{i_j} > 0$.

(via Primary decomp of (a)).

<u>CASE 1</u>: $r = 1$ Then $a = up^n$ & $M = M_a = M_{p^n}$

<u>CASE 2</u>: $r > 1$ Then $a = bc$ with $b = u p_{i_1}^{n_{i_1}}$ & $c = p_{i_2}^{n_{i_2}} \cdots p_{i_r}^{n_{i_r}}$

<u>Claim 2</u>: $(b,c) = 1$

Pf/ $(b,c) = (d)$ (R is a PID) so $b = dx$ & $c = dy$

But $b = u p_{i_1}^{n_{i_1}} = dx$ forces $d = w p_{i_1}^{s_{i_1}}$ with $0 \leq s_{i_1} \leq n_{i_1}$ $w \in R^\times$ (prim dec is unique for PID)

Also $c = p_{i_2}^{n_{i_2}} \cdots p_{i_r}^{n_{i_r}} = dy$ forces $d = v p_{i_2}^{s_{i_2}} \cdots p_{i_r}^{s_{i_r}}$ $v \in R^\times$ $s_{i_j} \geq 0$

But $p_{i_1}^{s_{i_1}}, p_{i_2}^{s_{i_2}} \cdots p_{i_r}^{s_{i_2}}$ are coprime, so only option is $s_{i_j} = 0$ $\forall j$ ie $d \in R^\times$.

By our Claim 1 $M = M_b \oplus M_c$.

- From Cases 1 & 2, we induct on # prime factors of a, b, c:

$$M = M_{p_{i_1}^{n_{i_1}}} \oplus \cdots \oplus M_{p_{i_r}^{n_{i_r}}}$$

p's & n's are unique (they come from $\mathrm{Ann}(M) = (a)$)