Lecture 31: Modules over PID, Fundamental Th^{m}'s

We now turn to study R-modules over a PID, this means we assume R is a commutative ring with no zero-divisors and every ideal is principal. Here $1 \in R$. I'll begin with a few general results before we get to the main event,

Def^{n}/ The LEFT R-module M is a <u>Noetherian</u> R-module provided it satisfies the <u>ACC</u> (ascending chain condition) on submodules. That is, whenever (submodules)

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

then $\exists\, m \in \mathbb{N}$ such that $M_k = M_m \quad \forall k \geq m$

Th^{m} (1) T.F.A.E.

(1.) M is Noetherian R-module

(2.) every non-empty set of submodules contains a maximal element under inclusion

(3.) every submodule of M is finitely generated.

Corollary (2)

If R is a PID then every nonempty set of ideals of R has a maximal element and R is a Noetherian ring.

Proposition (3)

Let R be an $\int$-domain and M a free module over R of rank $n < \infty$. Then any $(n+1)$-elements are R-linearly dependent

(meaning, for any $y_1, y_2, \dots, y_{n+1} \in M$ there exist $r_1, r_2, \dots, r_{n+1} \in R$, not all zero s.t. $r_1 y_1 + r_2 y_2 + \cdots + r_{n+1} y_{n+1} = 0$)

Proof: suppose $y_1, y_2, \dots, y_{n+1} \in M$. If we extend R to its field of fractions then M defines a vector space of dimension n over F hence $y_1, y_2, \dots, y_{n+1}$ is linearly dependent so $\exists$ $a_1/b_1, a_2/b_2, \dots, a_{n+1}/b_{n+1} \in F = \{ \frac{a}{b} \mid a, b \in R, b \neq 0 \}$ for which

$$\left(\frac{a_1}{b_1}\right) y_1 + \left(\frac{a_2}{b_2}\right) y_2 + \cdots + \left(\frac{a_{n+1}}{b_{n+1}}\right) y_{n+1} = 0$$

Multiply by $b = b_1 b_2 \cdots b_{n+1}$ and note $\frac{a_j}{b_j} b = a_j b_1 \cdots b_{j-1} b_{j+1} \cdots b_{n+1} \in R$ and we have $\hat{b}_j = \frac{a_j b}{b_j} \in R$ not all zero s.t.

$$\hat{b}_1 y_1 + \hat{b}_2 y_2 + \cdots + \hat{b}_{n+1} y_{n+1} = 0$$

//

Remark: for a linearly dependent subset of an R-module it may or may not be possible to solve for one element as R-linear combo. of the remaining elements. Over a field we can solve for some vector as linear combo. of the others.

Def^n/ Let R be an integral domain and suppose M is any R-module then the <u>torsion</u>

$$\text{Tor}(M) = \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}$$

A submodule of $\text{Tor}(M)$ is a <u>torsion submodule</u> of M and $\text{Tor}(M)$ is the union of all such submodules, its maximal. We should also think about the annihilator of a submodule N of M,

Def^n/ $\text{Ann}(N) = \{r \in R \mid rn = 0 \;\; \forall n \in N\}$ where $N \subseteq M$ an R-module

The following proposition follows immediately from the def$^{\underline{n}}$ of torsion submodule,

<u>Proposition</u>: If N is not a torsion submodule of M then $\text{Ann}(N) = \{0\} = (0)$.

You can show if submodules N, L of M have $N \subseteq L$ then $\text{Ann}(L) \subseteq \text{Ann}(N)$. Hence for R a PID with $N \subseteq L \subseteq M$ if $\text{Ann}(N) = (a)$ and $\text{Ann}(L) = (b)$ then $a \mid b$

<u>Proposition</u>: "the annihilator of any $x \in M$ divides $\text{Ann}(M)$"; $\underbrace{\text{Ann}(M)}_{(b)} \subseteq \underbrace{\text{Ann}(x)}_{(a)}$ then $a \mid b$.

Def^{n} For any integral domain R, the <u>rank</u> of an R-module M is the maximum # of R-linearly independent elements of M

In §12.1 Dummit & Foote's Th^{m}(4) indicates that for any free R-module of rank$(M) = m$, if $N \subseteq M$ is a submodule then rank$(N) = n \leq m$ and ~~for any~~ there exists basis $y_1, y_2, \ldots, y_m$ for M s.t. $a_1 y_1, \ldots, a_n y_n$ is basis for N where $a_1, a_2, \ldots, a_n$ are nonzero elements of R for which $a_1 | a_2 | a_3 | \cdots | a_n$ (means $a_1 | a_2$ and $a_2 | a_3$ etc...)

Th^{m}(5) (FUNDAMENTAL Th^{m} for Classification of MODULES over a PID, INVARIANT FACTOR FORM)

Let R be a PID and let M be finitely generated R-mod.

(1.) Then M is isomorphic to direct sum of finitely many cyclic modules. In particular,

$$\boxed{M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)} \text{ — } (1.)$$

for some integer $r \geq 0$ and nonzero $a_1, a_2, \ldots, a_m \in R$ which are not units in R and satisfy the divisibility relations

$$a_1 | a_2 | a_3 | \cdots | a_m$$

(2.) M is torsion free iff M is free

(3.) In the decomposition in (1.),

$$\mathrm{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

In particular, M is a torsion module iff $r = 0$ and in this case $\mathrm{ann}(M) = (a_m)$.

SPECIAL CASES

1.) $M \cong R^r$ (M is free rank$(M) = r \leftarrow$ Betti #)
then $\underline{Tor(M) \cong 0}$. (torsion free)

2.) $r = 0$ so $\underbrace{M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) = Tor(M)}_{\text{module } M \text{ is pure torsion}}$

$\boxed{E1}$ Let V be finite dim'l vector space over F then form $F[x] = R$ - module V by the usual $f(x)v = f(T)v$ action of $F[x]$ on V.
Suppose rank$(V) = r > 0$, is this reasonable?

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

$R = F[x] \Rightarrow \dim(V) \neq n$
(R^r is infinite dim'l and would be isomorphic to subspace of V, this cannot be!)

Conclusion: $\underline{r = 0}$ hence

$V = Tor(V)$ as $F[x]$ - module
The vector space is pure torsion

$\boxed{E2}$ $M = \mathbb{Z}_{900} \times \mathbb{Z}_{300} \times \mathbb{Z}^2$

$$\cong \mathbb{Z}^2 \times \underbrace{\mathbb{Z}_{300} \times \mathbb{Z}_{900}}$$

$$Tor(M) = \mathbb{Z}/(300) \oplus \mathbb{Z}/(900)$$

$a_1 = 300$, $a_2 = 900$

$\boxed{E3}$ oh, maybe $\boxed{E2}$ too easy, sometimes need to process some to see how Th$^{\underline{m}}$ 5 plays out,

$$\mathbb{Z}_{300} = \mathbb{Z}_{3 \cdot 5^2 \cdot 2^2}$$

$$= \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_4$$

$$N = \mathbb{Z}^2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_{900}$$

$$N \cong \mathbb{Z}^2 \oplus \mathbb{Z}_{300} \oplus \mathbb{Z}_{900}$$

$rank(N) = 2$

$Tor(N) = \mathbb{Z}_{300} \oplus \mathbb{Z}_{900}$

We should discuss the other form of the Fundamental Th$^{\underline{m}}$, recall

$$PID \Rightarrow UFD$$

$$a = u\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

$$R/(a) \cong R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$$

(we can rewrite (a) in-terms of its decomposition into prime powers, and we can do that for each $a_1, a_2, \ldots, a_m$ in Th$^{\underline{m}}$ (5))