Lecture 26: Classification of f.g. modules over a PID. (1)

§58–61 of [R2]; §12.1 of [DF]

<u>Previously...</u> R int. domain, M an R-mod.

$m \in M$ is <u>torsion</u> when $\exists\, r \neq 0$ with $r \cdot m = 0$.

M_{tor} is a submodule.

$S \subseteq M$ is <u>R-linearly</u> <u>independent</u> $\iff$ for all distinct $s_1, \dots, s_n \in S$ then $r_1 s_1 + \cdots + r_n s_n = 0$ for $r_i \in R$ implies all $r_i = 0$.

M is cyclic when $M = R\{m_0\}$ for some $m_0 \in M$.

$\iff M \cong R/_I$ for some ideal I.

A cylic module is torsion $\iff I \neq \{0\}$.

M a module over an int. domain R.

The <u>rank</u> of M is the largest size of any R-lin. indep. subset.

<u>Ex</u>: R = field, rank = dimension.

<u>Ex</u>: M torsion $\Rightarrow$ rank $= 0$.

<u>Ex</u>: $R = \mathbb{Z}$, $\operatorname{rank}(\mathbb{Z}/_2 \oplus \mathbb{Z}/_6 \oplus \mathbb{Z}^3) = 3$.

<u>Ex</u>: $M \cong R^n \Rightarrow$ rank $= n$.

Need justification, on next page.

The rank behaves like dimension, e.g.

<u>Thm</u>: R int domain, M an R-module. Suppose $S \subseteq M$ is finite with M/RS torsion. Then $\exists$ a maximal R-lin. indep set with $\leq |S|$ elts and all such sets have the same size.

<u>Thm</u>: If N is a submodule of M, then $\text{rank}(N) \leq \text{rank}(M)$ and $\text{rank}(M) = \text{rank}(N) + \text{rank}(M/N)$.

Also $\text{rank}(A \oplus B) = \text{rank}(A) + \text{rank}(B)$.

[Proofs are basically the same as for vector spaces, using a replacement/interchange lemma.]

<u>Thm</u>: R a PID. Every finitely-generated R-module M is a finite direct sum of cyclic modules and so $M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ for some $a_i \in R$.

<u>Note</u>: R int. domain. If every f.g. R-mod is a finite product of cyclic mods, then R is a P.I.D. [Prob. skip argument.]

Reason: An ideal $I \subseteq R$ is a submod of R, so $I \cong R/_{I_1} \oplus \cdots \oplus R/_{I_k}$. As $I_{tors} \subseteq R_{tors} = \{0\}$, must have all $I_i = \{0\}$ and so $I \cong R^k$. As $\text{rank}(I) \leq \text{rank}(R) = 1$, get $I \cong R$, i.e. I is principal.

same as ideal $(2, x)$

Ex: $R = \mathbb{Z}[x]$, $M = R\{2, x\} \subseteq R$ is not cyclic nor a product of such (see #4 on HW 5).

Ex: The $\mathbb{Z}$-module $(\mathbb{Q}, +)$ is not cyclic nor the direct sum of any two submodules:

$$\left(\mathbb{Z}\left\{\frac{a_1}{a_2}\right\}\right) \cap \left(\mathbb{Z}\left\{\frac{b_1}{b_2}\right\}\right) \supseteq \mathbb{Z}\{a_1 b_1\}.$$

[Motivate next part by Class. of f.g. ab. gps]

Invariant factor decomposition: Suppose M is a f.g. module over a PID R. $\exists\, t \geq 0$ and proper ideals $R \supsetneq (a_1) \supseteq (a_2) \supseteq (a_3) \supseteq \cdots \supseteq (a_t)$ with $M \cong \bigoplus_{i=1}^{t} R/(a_i)$. The a_i are unique in that given $R \supsetneq (a_1') \supseteq \cdots \supseteq (a_s')$ with $\bigoplus_{i=1}^{s} R/(a_i')$ then $s = t$ and each $(a_i) = (a_i')$, that is, a_i and a_i' are assoc.

<u>Primary decomposition</u>: M as above. There exist $r, u \geq 0$ and a sequence of $p_1^{k_1}, \ldots, p_u^{k_u} \in R$ with p_i prime and $k_i \geq 1$ where

$$M \cong R^r \oplus R/(p_1^{k_1}) \oplus R/(p_2^{k_2}) \oplus \cdots \oplus R/(p_u^{k_u})$$

Here, r and u are unique, the $p_i^{k_i}$ are unique up to order and replacing p_i by associates.

[So you can do the HW, will postpone proof and devote the next lecture to applications.]

<u>Cor</u>: R a PID. A f.g. R-module is free $\iff$ torsion free $\iff \cong R^n$.

<u>Cor</u>: R a PID. If M is a free R-module of rank $\leq n$, then every submodule of M is free of rank $\leq n$.

<u>Pf</u>: Really this is a lemma used in the proof of the classification.

Suppose M is an R-module. Its <u>annihilator</u> is $\mathrm{Ann}(M) := \{x \in R \mid xM = \{0\}\}$
$= \{x \in R \mid x \cdot m = 0 \text{ for all } m \in M\}$.

<u>Ex</u>: If M is cyclic, then $M \cong R/\mathrm{Ann}(M)$

<u>Ex</u>: If M is in invariant factor form, then $\mathrm{Ann}(M) := (a_t)$.