Lecture 24: More Module Basics.

Previously: R ring with 1. An R-module is an abelian gp $(M,+)$ with a $R \times M \to M$ where

① $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$

② $1_R \cdot m = m$

③ $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

④ $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

10.1–10.3 of [DF]
48–52 of [R2].

$N \subseteq M$ is a submodule when N is a subgp of $(M,+)$ and $r \cdot n \in N$ for all $r \in R$, $n \in N$.

$\psi : A \to B$ is a homom. of R-modules when it is a hom of $(A,+)$ to $(B,+)$ and $\psi(r \cdot a) = r \cdot \psi(a)$ for all $r \in R$, $a \in A$.

[Basics parallel theory of vector spaces, abelian groups, and ideals...]

$\psi : A \to B$ a hom. of R-modules.

$\ker(\psi) = \{ a \in A \mid \psi(a) = 0 \}$ a submodule of A

$\mathrm{im}(\psi) = \{ \psi(a) \mid a \in A \}$ a submodule of B.

If ψ is bijective, it's called an isomorphism of R-modules.

Consider a submodule N of M. The quotient group M/N is also an R-module via

$$r \cdot (m + N) = (r \cdot m) + N$$

Get usual isomorphism thms (see text).

If A, B are R-modules, set

$$\mathrm{Hom}_R(A, B) := \{\psi : A \to B \text{ an } R\text{-mod hom.}\}$$

1) An abelian gp under $\phi + \psi := (a \mapsto \phi(a) + \psi(a))$

2) If R is comm, its an R-module via
$r \cdot \psi := (a \mapsto r\psi(a))$.

For a subset $S \subseteq M$, set

$$RS = \underset{\text{submod} \supseteq S}{\text{smallest}} = \{r_1 s_1 + \cdots + r_k s_k \mid k \geq 0,\ r_i \in R,\ s_i \in S\}$$

If $RS = M$, say S generates M. M is <u>cyclic</u> when it can be generated by one elt.

<u>Ex</u>: R comm, $I \subseteq R$ an ideal ($\Leftrightarrow$ a submod of R). Then $M := R/I$ is cyclic, gen by $1_R + I$.

Prop: R comm. If M is cyclic R-module, then $M \cong R/I$ for some ideal I.

Pf: Suppose $R\{m_0\} = M$. Consider $\psi: R \to M$, $r \mapsto r.m_0$

a homom. of R-mods.

Set $I = \ker(\psi)$, an ideal/submod. of R.

As ψ is surjective, the 1^{st} isom thm gives $M \cong R/I$. ▨

Given R-mods M_1 and M_2, the product

$M_1 \times M_2$ is also an R-mod with

- $(m_1, m_2) + (m_1', m_2') := (m_1 + m_1', m_2 + m_2')$
- $r(m_1, m_2) := (r.m_1, r.m_2)$.

Some write $M_1 \oplus M_2$ for $M_1 \times M_2$.

Makes sense for more modules, e.g. $M_1 \times M_2 \times M_3 \times M_4$.

Warning: For an infinite collection of R-mods $\{M_i\}_{i \in I}$ there are two options:

Product $\prod M_i := \{(x_i)_{i \in I} \mid x_i \in M_i\}$

Direct sum $\bigoplus M_i := \left\{ (x_i) \in \prod M_i \;\middle|\; \begin{array}{l} \text{all but finitely} \\ \text{many } x_i = 0_{M_i} \end{array} \right\}$

Ex: $R = \mathbb{F}_2$, $I = \mathbb{Z}_{\geq 0}$. Then $\bigoplus M_i$ is countable but $\prod M_i$ is uncountable.

An R-module M is free on $S = \{s_1, \dots, s_n\} \subseteq M$ when for all $m \in M$ there exist unique $r_1, \dots, r_n \in R$ with $m = r_1 s_1 + \cdots + r_n s_n$.

Ex: $M = R^n = \bigoplus_{i=1}^{n} R$ with $S = \{e_1, \dots, e_n\}$ where

$$e_i = (0, \dots, 0, \underset{\text{ith pos.}}{1_R}, 0, \dots 0)$$

Ex: For R a field, M free on $S \iff S$ is a vector sp. basis for M.

Can define for $|S| = \infty$: M is free on S when $\forall m \in M$, $\exists$ unique $\{a_s \in R\}_{s \in S}$, with $a_s \neq 0$ for only finitely many s where $m = \sum_{s \in S} a_s s$.

Note: Given any set S, we can make an R-module

$$M = \{ \underbrace{\sum_{s \in S} a_s s}_{\text{formal sum.}} \mid a_s \in R \text{ nonzero for only finitely many } s \}$$

which is free on S. Really, this is just $\bigoplus_{s \in S} R$ with $e_t = \{(\delta_{st})\}$ where $\delta_{st} = \begin{cases} 1 & \text{if } s = t \\ 0 & \text{otherwise.} \end{cases}$

identifield with $t \in S$.

Thm: An R-module M is free on S $\iff$ for all fns $\phi : S \to N$ where N is an R-module, there exists a unique R-mod homom $\tilde{\phi} : M \to N$ with $\tilde{\phi} \circ i = \phi$.

$$\begin{tikzcd} S \arrow[r, "\phi"] \arrow[d, "i"'] & N \\ M \arrow[ur, dashed, "\tilde{\phi}"'] & \end{tikzcd}$$

$\exists!$ R-mod hom

Cor: Any M that is free on a set S with $|S| = n < \infty$ is isomorphic to R^n.

Pf: Given $m \in M$, write $m = \sum_{s \in S} a_s m$ for $a_s \in R$ unique per the def. Define $\tilde{\phi}(m) = \sum a_s \phi(s)$. and check that this works. ▨

Ex: Non free modules for $R = \mathbb{Z}$: $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/5 \oplus \mathbb{Z}$, etc.