2. Direct sums and free modules.

The class of all R-modules form a category denoted R-Mod.

Both products & coproducts of modules exist in R-Mod, but the latter play a much more central role.

Def: Suppose $\{M_\alpha : \alpha \in A\}$, $A \neq \emptyset$ is a family of R-modules. A direct sum of the M_α is an R-module M together with a family $i_\alpha : M_\alpha \longrightarrow M$, $\alpha \in A$ of R-homomorphisms with the following universal property: Given any R-module N and R-homomorphisms $f_\alpha : M_\alpha \longrightarrow N$, $\alpha \in A$, $\exists!\ f \in \mathrm{Hom}_R(M, N)$ such that $f i_\alpha = f_\alpha$ for all $\alpha \in A$.

$$\begin{tikzcd} M_\alpha \arrow[rr, "f_\alpha"] \arrow[dr, "i_\alpha"'] & & N \\ & M \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

Remark: This is just the coproduct of M_α, in the language of category theory.

Prop 2.1: If a direct sum exists for a family $\{M_\alpha\}$ of R-modules, then it is unique up to R-isomorphism, and each i_α is an R-monomorphism.

Pf: Exercise.

Thm 2.2: Every nonempty family $\{M_\alpha : \alpha \in A\}$ has a direct sum M.

Pf: Let M be the submodule of $\prod M_\alpha$ such that $m_\alpha = 0$ for all but finitely many $\alpha \in A$,

Define $i_\alpha : M_\alpha \longrightarrow M$, $\quad i_\alpha(x) = \begin{cases} m & m_\alpha = x \\ 0 & \beta \neq \alpha \end{cases}$.

Clearly, $i_\alpha \in \mathrm{Hom}_R(M_\alpha, M)$.

Given any R-module R-module N and family $f_\alpha : M_\alpha \to N$ of R-homomorphisms, define $f : M \longrightarrow N$, $\quad f(m) = \sum_{\alpha \in A} f_\alpha(m_\alpha)$.

Note: There are only finitely many non-zero summands.

Then $f \in \mathrm{Hom}_R(M, N)$, $f i_\alpha = f_\alpha \ \forall \alpha$, and f is unique (these are easy to verify). $\square$

We write $\bigoplus_{\alpha \in A} M_\alpha$ for the direct sum of $\{M_\alpha : \alpha \in A\}$, and $M_1 \oplus \cdots \oplus M_n$ for a finite collection.

Thm 2.3: Suppose M is an R-module, and $\{M_\alpha\}$ a family of submodules, satisfying

(i) $R\langle \bigcup_\alpha M_\alpha \rangle = M$

(ii) $M_\alpha \cap \sum_{\beta \neq \alpha} M_\beta = 0$ for each α

(iii) $\sum_\alpha M_\alpha = M$.

Then M is R-isomorphic with $\bigoplus_\alpha M_\alpha$.

Remark: This is the analog of Thm 6.3 Groups, for modules.

Exercise: $M = \bigoplus_\alpha M_\alpha$ for a family of submodules $\{M_\alpha\}$ iff each $x \in M$ has a unique expression $x = x_1 + \dots + x_k$, $x_i \in M_{\alpha_i}$.

Prop 2.4: If $M_1, \dots, M_n$ are Noetherian R-modules, then $M = M_1 \oplus \dots \oplus M_n$ is Noetherian.

Pf: It suffices to consider the case when $n = 2$.

Then $N_1 := \{(x,0) : x \in M_1\}$ is a submodule, R-isomorphic with M_1, so N_1 is Noetherian, and M/N_1 is R-isomorphic with M_2 via $(x,y) + N_1 \longmapsto y$, so M/N_1 is Noetherian.

By Prop 1.8, M is Noetherian.

Def. A ring R is called left (right) Noetherian if it satisfies the ascending chain condition for left (right) ideals, or equivalently, if R is Noetherian as a left (right) R-module.

Prop 2.5: Suppose R is a left Noetherian ring with 1 and M is a finitely generated unitary R-module. Then M is a Noetherian R-module.

Pf: Say $M = R\langle a_1, \dots, a_n \rangle$.

Let N be the R-module $R^n = R \oplus R \oplus \dots \oplus R$, which is Noetherian by Prop 2.4.

Define $f : N \longrightarrow M$, $\quad f(r_1, \dots, r_n) = r_1 a_1 + \dots + r_n a_n$

Clearly, $f \in \mathrm{Hom}_R(N, M)$ and f is onto since M is unitary. Thus, $M \cong N/\ker f$, and M is Noetherian by Prop 1.8. $\square$

<u>Def</u>: Let R be a ring with 1, and B an arbitrary set. A <u>free R-module</u> based on B is a unitary R-module F together with a function $\phi : B \longrightarrow F$ such that given any unitary R-module M and any function $\theta : B \longrightarrow M$, there is a unique $f \in \mathrm{Hom}_R(F, M)$ such that $f\phi = \theta$.

$$\begin{tikzcd} B \arrow[rr, "\phi"] \arrow[dr, "\theta"'] & & F \arrow[dl, dashed, "f"] \\ & M & \end{tikzcd}$$

<u>Exercise</u>: (i) If $B = \emptyset$, then $F = 0$ is a free R-module based on B.

(ii) If $B = \{b\}$, then $F = R$ is a free R-module based on B, with $\phi(b) = 1 \in R$.

As usual, free R-modules based on B are unique up to R-isomorphism (if it exists), and ϕ is 1-1.

<u>Prop 2.6</u>: Free R-modules exist.

<u>Pf</u>: Suppose $B \neq \emptyset$. Let $M_\beta = R$ (as a left R-module) for $\beta \in B$. Set $F = \bigoplus_{\beta \in B} M_\beta = \bigoplus_{\beta \in B} R$.

For each $\beta \in B$, let $\phi : B \longrightarrow F$ be the "canonical inclusion map," i.e, if $\phi(\beta) = m$, then $m_\beta = 1 \in M_\beta = R$ and $m_\alpha = 0$ if $\beta \neq \alpha$. Check that this works (Exercise). $\square$

Since $\phi : B \longrightarrow F$ is 1-1, we may identify β with $\phi(\beta)$ for each $\beta \in B$, and hence assume that $B \subseteq F$.

Remark: If $b_1, \dots, b_k \in B$, $r_1, \dots, r_k \in R$, then $\sum_{i=1}^{k} r_i b_i = 0 \Rightarrow r_i = 0 \; \forall i$.

In general, call a subset $S \subseteq M$ R-linearly independent if $\sum_{i=1}^{k} r_i b_i = 0 \Rightarrow r_i = 0$ where $r_i \in R$, $b_i \in S$.

Def: A basis for an R-module M is an R-linearly independent subset of M such that $M = R\langle B \rangle$.

Thm 2.7: If R is a ring with 1, then a unitary R-module is free if and only if it has a basis.

Pf: ($\Rightarrow$) Immediate from the construction of a free module (see Prop 2.6).

($\Leftarrow$) Let B be a basis. If $B = \emptyset$, then $M = 0$ is free.

Suppose then that $B \neq \emptyset$, and let $\phi : B \hookrightarrow M$ be the inclusion map.

Set $M_b = Rb$ for each $b \in B$.

Then, $r \longmapsto rb$ is an isomorphism $R \cong M_b$

Since B is a basis, Thm 2.3 $\Rightarrow M = \bigoplus_{b \in B} M_b \cong \bigoplus_{b \in B} R$.

But $\bigoplus_{b \in B} R$ is a free R-module based on B, unique up to isomorphism. Thus M is free. $\square$

Examples:

1. A free $\mathbb{Z}$-module (i.e., free abelian group) based on B direct sum of $|B|$ copies of $\mathbb{Z}$.
2. An F-vector space is a free F-module.

Remark: It is not true that any two bases have the same cardinality.

Example: let $F = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$, and $R = \mathrm{End}(F)$.

The set $B_1 = \{1_R\}$ is a basis for R (as a free R-module).

Also, if $\{a_1, a_2, \ldots\}$ is a basis for F, then $B_2 = \{\phi_1, \phi_2\}$

where $\phi_1 : \begin{array}{l} a_{2n} \longmapsto a_n \\ a_{2n+1} \longmapsto 0 \end{array}$ and $\phi_2 : \begin{array}{l} a_{2n} \longmapsto 0 \\ a_{2n+1} \longmapsto a_n \end{array}$

is also a basis (check!)

However, there are conditions on R that ensure that any two bases have the same cardinality. This depends on the well-known fact that any two bases for a vector space have the same cardinality. We will review this here.

Thm 2.8: If V is a vector space over a division ring D, then V has a basis.

Pf: Let $\mathcal{S} = \{S \subseteq V : S \text{ is linearly independent}\}$.

Clearly, $\mathcal{S} \neq \phi$. Partially order $\mathcal{S}$ by set inclusion.

If $\mathcal{C}$ is a chain in $\mathfrak{S}$, define $B = \bigcup_{A \in \mathcal{C}} A$

<u>Claim</u>: $B \in \mathfrak{S}$. (This will be the upper bound of $\mathcal{C}$).

If not, then $\exists$ distinct $v_1, \dots, v_n \in B$, $a_1, \dots, a_n \in D$ (not all zero) such that $a_1 v_1 + \dots + a_n v_n = 0$

But each v_i is in some $A_i \in \mathcal{C}$, so one of $A_1, \dots, A_n$ contains all the others.

But then $v_1, \dots, v_n \in A_n$ which is linearly independent $\lightning$

Thus, $B \in \mathfrak{S}$ is an upper bound for $\mathcal{C}$.

By Zorns lemma, $\exists$ maximal element $M \in \mathfrak{S}$.

<u>Claim</u>: M is a basis for V. (Suffices to show it spans V).

Let $W = \mathrm{span}(M)$. If $W \subsetneq V$, then pick $v \in V \setminus W$ and set $M_1 = M \cup \{v\}$.

Then M_1 is linearly independent, contradicting maximality of M. $\lightning$. $\square$

<u>Thm 2.9</u>: Any two bases for a vector space V over a division ring D have the same cardinality.

<u>Pf</u>: If V is finite-dimensional, the result is a standard fact of elementary linear algebra.

Suppose B_1 & B_2 are infinite bases for V.

Each $v \in B_1$ is a linear combination of a unique finite subset of B_2; denote this by $B_2(v)$.

<u>Claim</u>: $B_2 = \bigcup_{v \in B_1} B_2(v)$.

If not, then $B_1 \subseteq \text{Span}(B_2 \setminus \{x\}) \Rightarrow V = \text{Span}(B_2 \setminus \{x\})$.

$\Rightarrow B_2$ is linearly dependent. $\lightning$

Thus, $|B_2| = \left| \bigcup_{v \in B_1} B_2(v) \right| \leq \sum_{v \in B_1} |B_2(v)| \leq \aleph_0 |B_1| = |B_1|$.

Similarly, $|B_1| \leq |B_2|$, and so $|B_1| = |B_2|$. $\square$

<u>Thm 2.10</u>: Suppose R is a ring with 1 having an ideal I such that R/I is a division ring, and F is a free R-module. Then any two bases of F have the same cardinality.

<u>Pf</u>: Set $E = IF = \{ \sum r_i x_i : r_i \in I, x_i \in F \}$, which is a submodule of F.

Then, F/E is a vector space over $K = R/I$, with scalar multiplication defined by $(r+I)(x+E) = rx + E$.

If B is a basis for F, set $\bar{b} = b + E$, and $\bar{B} = \{ \bar{b} : b \in B \}$.

Each $x \in F/E$ can be written as

$$x = \sum_{i=1}^{k} r_i b_i + E = \sum_{i=1}^{k} (r_i + I) \bar{b}_i, \quad r_i \in R, \ b_i \in B.$$

Thus, $\bar{B}$ spans F/E over K.

To show linear independence, suppose that

$$\sum_{i=1}^{k} (r_i + I) \bar{b}_i = \sum_{i=1}^{k} r_i b_i + E = E \qquad (\text{i.e., } \bar{0} \in F/E).$$

Then, $\sum_{i=1}^{k} r_i b_i \in E$, so there are $s_1, \dots, s_k \in I$ such that

$$\sum_{i=1}^{k} r_i b_i = \sum_{i=1}^{k} s_i b_i \Rightarrow \sum_{i=1}^{k} (r_i - s_i) b_i = 0 \Rightarrow r_i = s_i \quad \forall i.$$

$$\Rightarrow r_i + I = I.$$

Thus, $\overline{B}$ is a K-basis for K/E (in particular, $b \mapsto \overline{b}$ is 1-1), and F/E has K-dimension $|B|$.

Thus, all bases of F have the same K-dimension as an arbitrary basis for F/E, which is independent of choice of basis, by Prop 2.9.

$\square$

Cor: If R is a commutative ring with 1 and F is a free R-module, then any two bases of F have the same cardinality.

Pf. Take any maximal ideal $M \subseteq R$, and apply Thm 2.10 $\square$

Thm 2.11: If R is any ring with 1 and M is a unitary R-module, then M is a homomorphic image of a free R-module F.

Pf: Analogous to the proof of Prop 8.8 (Groups): If $G = \langle S \rangle$, then $\exists$ homom. $F_S \twoheadrightarrow G$, i.e., every group is a homomorphic image of a free group.

$\square$

Cor: If R is a commutative ring with 1 and M is a unitary R-module with $M = R\langle S\rangle$ for some $S \subseteq M$, then M is a homomorphic image of a free R-module F of rank $|S|$.

Example: The ring $R = \mathbb{Z}_4$ is a free R-module, but the ideal $M = 2R$ is not a free R-module, since it doesn't have a basis (the only non-zero element is a zero-divisor).

key idea: Submodule of free modules aren't necessarily free (in sharp contrast for the case of groups).

Thm 2.12: Suppose R is a PID, F is a free R-module, and E is a submodule of F. Then E is free, and $\operatorname{rank}(E) \leq \operatorname{rank}(F)$.

Pf: Assume $E \neq 0$. Let B be a basis for F.

For any $C \subseteq B$, set $F_C = R\langle C\rangle$ and $E_C = E \cap F_C$.

Let $\mathcal{S} = \{(C, C', f) : C' \subseteq C \subseteq B,\ E_C \text{ is free},\ f : C' \to E_C \text{ s.t. } f(C') \text{ is a basis for } E_C\}$.

Note: $(\emptyset, \emptyset, \emptyset) \in \mathcal{S} \Rightarrow \mathcal{S} \neq \emptyset$.

Partially order $\mathcal{S}$ s.t. $(C, C', f) \leq (D, D', g)$ iff $C \subseteq D$, $C' \subseteq D'$, and $g|_{C'} = f$.

By Zorn's lemma, $\exists$ maximal element (A, A', h) in $\mathcal{S}$.
It suffices to show that $A = B$, since $E = E_B$.
Suppose that $A \neq B$, and pick $b \in B \setminus A$ and let $D = A \cup \{b\}$.

- If $E_D = E_A$ then $(A, A', h) < (D, A', h)$ $\lightning$ (maximality of (A, A', h)).
- If $E_D \neq E_A$ then there are elts $y + rb \in E_D$, $y \in F_A$, $r \in R$.

Let $I = \{r \in R \text{ s.t. } y + rb \in E \text{ for some } y \in F_A\}$.
Then I is an ideal of R, say $I = (s)$, so $w = x + sb \in E$ for some $x \in F_A$ (note $s \neq 0$).
Set $D' = A' \cup \{b\}$ and extend $h' : D' \to E_D$, $h'(b) = w$.
If $z \in E_D$, then $z = y + rb$ for some $y \in F_A$, $r = r's \in I$,
so $z = (y - r'x) + r'w$, $\quad z - r'w = y - r'x \in E \cap F_A = E_A$.
Therefore, $R\langle h'(D')\rangle = E_D$, and so $h'(D')$ is a basis for E_D, thus $(A, A', h) < (D, D', h')$ $\lightning$ (maximality). $\square$

Cor: Suppose R is a PID, M is a finitely generated R-module, and N is a submodule of M. Then N is finitely generated.

Pf: By Prop 2.5, $\exists$ R-homom. $f : R^n \to M$ for some n.
Thus, $f^{-1}(N)$ is a submodule of R^n, so it is free of rank $m \leq n$ by Thm 2.12.
Therefore, $N = f(f^{-1}(N))$ has a set of $m < \infty$ generators. $\square$