Uniqueness of expression.
For $M_1, \dots, M_n \le M$,

$$M_1 + \dots + M_n = \{m_1 + \dots + m_n \ : \ m_i \in M_i \text{ for } 1 \le i \le n\}$$

is a submodule of M.

Question. When do elements in $M_1 + \dots + M_n$ have a unique decomposition?

Definition. $M_1 \times \dots \times M_n$ with $+$ and R acting componentwise is the *direct product* of R-modules $M_1, \dots, M_n$.

Lemma. *For $M_1, \dots, M_n \le M$ TFAE:*

(1) $\varphi \colon M_1 \times \dots \times M_n \to M_1 + \dots + M_n,\ (m_1, \dots, m_n) \mapsto m_1 + \dots + m_n$ *is an R-module isomorphism.*
(2) $M_i \cap (M_1 + \dots + M_{i-1} + M_{i+1} + \dots M_n) = \{0\}$ *for all* $1 \le i \le n$. $\ast$
(3) *For every $m \in M_1 + \dots + M_n$ there exist unique $m_1 \in M_1, \dots, m_n \in M_n$ such that $m = m_1 + \dots + m_n$.*

Note: $M_i \cap M_j = 0$ is not sufficient for $n \ge 3$.

Proof.

1) $\Rightarrow$ 2) Let $a_1 \in M_1, \dots, a_n \in M_n$ such that

$$a_i = a_1 + \dots + a_{i-1} + a_{i+1} + \dots + a_n$$

Then $\varphi(a_1, \dots, a_{i-1}, -a_i, a_{i+1}, \dots, a_n) = 0$

If φ is iso, then $a_i = 0$.

2) $\Rightarrow$ 3), (3) $\Rightarrow$ 1) easy, in book. $\square$

Definition. If $M = M_1 + \dots + M_n$ satisfies the equivalent conditions of the Lemma above, then M is the *(internal) direct sum* of $M_1, \dots, M_n$, denoted

$$M = M_1 \oplus \dots \oplus M_n.$$

Example.

$M_n(R)$-modules

$$M_i := \left\{ \begin{array}{c} \begin{bmatrix} 0 & \cdots & 0 & * & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & * & 0 & \cdots & 0 \end{bmatrix} \\ \hphantom{0 \cdots 0\,} i \hphantom{\,0 \cdots 0} \end{array} \right\} \le M_n(R)$$

$M_i \cong R^n$.

$M_n(R) = M_1 \oplus \dots \oplus M_n \cong (R^n)^n$

Freeness.

Definition. An R-module M is *free* over $A \subseteq M$ if $\forall m \in M \setminus \{0\}\ \exists! n \in \mathbb{N}$ $\exists! r_1, \dots, r_n \in R \setminus \{0\}\ \exists! a_1, \dots, a_n \in A\colon m = r_1 a_1 + \cdots + r_n a_n$.

Then we call A *free generators* (a *basis*) for M.

Example.

R-mod R^n is free over $\left\{ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \right\}$

$M_n(R)$-mod R^n is not free over $\left\{ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right\}$.

Universal property of modules.

Theorem. *For each set A there is a free R-module $F(A)$ on A.*
$F(A)$ satisfies the **universal property***: for any R-module M and any $\varphi\colon A \to M$ there exists a unique $\Phi \in \operatorname{Hom}_R(F(A), M)$ such that $\Phi|_A = \varphi$.*

$$\begin{tikzcd} A \arrow[d, "\varphi"'] & \subseteq & F(A) \arrow[dll, dotted, "\Phi"] \\ M & & \end{tikzcd}$$

Proof.

$$F(A) := \begin{cases} 0 & \text{if } A = \emptyset, \\ \{ f\colon A \to R \mid f(a) = 0 \text{ for all but finitely many elements } a \in A \} & \text{else.} \end{cases}$$

Then $F(A) \subseteq R^A$ is an R-module under pointwise $+$ and scaling by R.

$(f+g)(x) := f(x) + g(x)$ for $x \in A$

$(rf)(x) := r f(x)$ $\quad r \in R,\ x \in A$

Then $A \hookrightarrow F(A)$
$a \mapsto f_a$ where $f_a\colon A \to R,\ x \mapsto \begin{cases} 1 & \text{if } x = a \\ 0 & \text{else} \end{cases}$

Then $F(A) = R\{ f_a \mid a \in A \}$

$= \{ r_1 a_1 + \dots + r_n a_n \mid n \in \mathbb{N},\ r_1, \dots, r_n \in R,\ a_1, \dots, a_n \in A \}$

"formal R-linear combinations" identifying a and f_a

Claim: $F(A)$ is free on A because each $f \in F(A)$ has a unique decomposition as formal sum.

For $\varphi: A \to M$, define

$$\Phi: F(A) \to M \quad \text{by} \quad \Phi\left(\sum r_i a_i\right) := \sum r_i \varphi(a)$$

welldefined since decomposition is unique.

Then $\Phi \in \mathrm{Hom}_R(F(A), M)$

$\Phi|_A = \varphi$

Φ is the <u>unique</u> hom extending φ because every hom is uniquely determined by its images on the generators A. $\square$

Note.

(1) For $A = \{a_1, \ldots, a_n\}$ finite,

$$F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$$

(2) The free $\mathbb{Z}$-module over A is the free ab group over A.

Corollary. *Any free R-module over A is isomorphic to $F(A)$.*

Proof. Exercise. using universal property. $\square$