Spanning sets and free modules

Defn: Let M be an R-module

An <u>R-linear combination</u> of elements $m_1, \ldots, m_n \in M$ is an element of the form

$$a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_n \cdot m_n \qquad a_1, a_2, \ldots, a_n \in R$$

We say a subset $A \subset M$ <u>spans</u> or <u>generates</u> the module if every element of M is an R-linear combination of elements in A.

More generally, if $B \subset M$, <u>the submodule spanned/generated by</u> B is

$$RB := \{ a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_n \cdot m_n \mid n \in \mathbb{Z}^+,\ a_1, \ldots, a_n \in R,\ m_1, \ldots, m_n \in B \}$$

Exercise: RB is an R-module

Example: For any ring R w/ $1 \neq 0$

every element is a "linear combination" of $\{1\}$

i.e. if $r \in R$, then $r = r \cdot 1$

So $R = R\{1\}$ is spanned by a single element as an R-module.

Example: The polynomial ring $R[x]$ has a natural R-module structure:

If $a \in R$, $p(x) = a_0 + a_1 X + \cdots + a_n X^n \in R[x]$

then
$$a \cdot (a_0 + a_1 X + \cdots + a_n X^n) := (a \cdot a_0) + (a \cdot a_1) \cdot X + \cdots + (a \cdot a_n) X^n$$

$R[x]$ is spanned by $\{1, x, x^2, x^3, x^4, \ldots\}$

Obs.: $R[x]$ has no finite spanning set!

To see this, suppose $R[x]$ is spanned by

$$p_1(X), p_2(X), \_\_\_, p_n(X) \in R[X]$$

Let $d = \max\{\deg p_1(X), \_\_\_, \deg p_n(X)\}$

Then $d < \infty \Longrightarrow \forall a_1, \_\_\_, a_n \in R$

$$\deg\left[a_1 \cdot p_1(X) + a_2 \cdot p_2(X) + \_\_\_ + a_n \cdot p_n(X)\right] \leq d.$$

$$\Longrightarrow X^{d+1} \notin \operatorname{Span}\{p_1(X), \_\_\_, p_n(X)\}$$

Defn.: We say an R-module M is

finitely generated

if it has a finite spanning set.

We say M is cyclic if it is spanned by a single element.

Example: If R is a ring, $A \subset R$

Then $RA = (A)$

(the module generated by A is the ideal generated by A)

A cyclic submodule of R is just a principal ideal.

Example: R a ring, $F = R^n$ is the free R-module of rank n.

F has a natural spanning set:

$$\mathcal{E}_n := \left\{ \begin{array}{l} e_1 = (1,0,0,\ldots,0) \\ e_2 = (0,1,0,\ldots,0) \\ e_3 = (0,0,1,\ldots,0) \\ \quad \vdots \\ e_n = (0,0,0,\ldots,0,1) \end{array} \right\}$$

Any element $(a_1, a_2, \ldots, a_n) \in R^n$ can be written as

$$(a_1, a_2, \ldots, a_n) = a_1 \cdot (1,0,0,\ldots,0) + a_2 \cdot (0,1,0,\ldots,0) + \ldots + a_n \cdot (0,0,0,\ldots,0,1)$$

$$= a_1 \cdot e_1 + a_2 \cdot e_2 + \ldots + a_n \cdot e_n$$

Re contextualizing the free R-module of rank n:

Consider the set $\{1, 2, 3, \ldots, n\}$

A function $a : \{1, 2, 3, \ldots, n\} \to R$

$$\begin{array}{lcl} 1 & \longmapsto & a(1) = a_1 \\ 2 & \longmapsto & a(2) = a_2 \\ \vdots & & \quad\vdots \\ n & \longmapsto & a(n) = a_n \end{array}$$

we can think of an ordered n-tuple of elements in R

as a function

$$a : \{1, 2, \ldots, n\} \longrightarrow R$$

i.e. we can think of R^n as

$$R^n = \{ a : \{1, 2, \ldots, n\} \longrightarrow R \}$$

The obvious addition is

$$\begin{aligned} a+b : \{1,2,\ldots,n\} &\longrightarrow R \\ 1 &\longmapsto a(1)+b(1) \\ 2 &\longmapsto a(2)+b(2) \\ &\vdots \\ n &\longmapsto a(n)+b(n) \end{aligned}$$

The obvious scalar multiplication is

$$\begin{aligned} r \cdot a : \{1,2,\ldots,n\} &\longrightarrow R \\ 1 &\longmapsto r \cdot a(1) \\ 2 &\longmapsto r \cdot a(2) \\ &\vdots \\ n &\longmapsto r \cdot a(n) \end{aligned}$$

<u>Defn</u>: Fix a ring R

An R-module F is <u>free</u> on a set A

if $\forall m \in F$

there are <u>unique</u> elements $m_1, m_2, \ldots, m_n \in A$

$a_1, a_2, \ldots, a_n \in R$

s.t. $m = a_1 \cdot m_1 + a_2 \cdot m_2 + \ldots + a_n \cdot m_n$

we call A set of <u>free generators</u> of F

or a <u>basis</u> of F

<u>Note</u>: usually, we ask that the basis is <u>ordered</u> in some way.

Example: The set $\mathcal{E}_n = \{e_1, e_2, \ldots, e_n\}$ is a basis for the free module of rank n.

Non-example: $\mathbb{Z}/2\mathbb{Z}$ is a non-free $\mathbb{Z}$-module.

$$\bar{1} = 1 \cdot \bar{1} = 3 \cdot \bar{1}$$

not unique!

Non-example: Is every submodule of a free module free?

$\mathbb{Z}/4\mathbb{Z}$ is a free module over $\mathbb{Z}/4\mathbb{Z}$

(Check: $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}\{\bar{1}\}$ is free)

$2 \cdot \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{2}\} \subset \mathbb{Z}/4\mathbb{Z}$ is a submodule

BUT: $\bar{2} \cdot \bar{2} = \bar{0}$, $\bar{0} \cdot \bar{2} = \bar{0}$ $\Longrightarrow$ There is no unique way of writing $\bar{0}$ as a $(\mathbb{Z}/4\mathbb{Z})$-linear combination of $\{\bar{2}\}$

$\Longrightarrow$ $2 \cdot \mathbb{Z}/4\mathbb{Z} = (\bar{2})$ is not free.

Example: Fix a ring R. Let A be any set

$$F_R(A) := \{ \phi : A \to R \mid \phi(a) = 0 \text{ for all but finitely many } a \in A \}$$

Claim: $F_R(A)$ is a free module over R on the set A.

Pf: Addition: $\phi, \psi : A \to R$

$$\begin{aligned} \phi + \psi : A &\longrightarrow R \\ a &\longmapsto \phi(a) + \psi(a) \end{aligned}$$

Scalars: $\phi : A \to R$, $r \in R$

$$\begin{aligned} r \cdot \phi : A &\longrightarrow R \\ a &\longmapsto r \cdot \phi(a) \end{aligned}$$

Consider the inclusion map

$$\begin{aligned} \iota : A &\longrightarrow F_R(A) \\ a &\longmapsto \left(\begin{aligned} \phi_a : A &\longrightarrow R \\ x &\longmapsto \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases} \end{aligned} \right) \end{aligned}$$

Obviously this map is injective: If $\phi_a = \phi_b$

then $\phi_a(a) = 1 = \phi_b(a)$

$\implies a = b$.

We call $\iota(A) = \mathcal{E}_A$ and we see that

① $\mathcal{E}_A$ spans $F_R(A)$

Pf: $(\phi : A \longrightarrow R) \in F_R(A)$

Let $\{a_1, \ldots, a_n\} \subset A$ s.t. $\phi(a_i) \neq 0$

$$\phi(a_i) = \phi(a_i) \cdot 1 = \phi(a_i) \cdot \phi_{a_i}(a_i)$$

$$\Longrightarrow \phi \equiv \underbrace{\phi(a_1)}_{\in R} \cdot \phi_{a_1} + \underbrace{\phi(a_2)}_{\in R} \cdot \phi_{a_2} + \cdots + \underbrace{\phi(a_n)}_{\in R} \cdot \phi_{a_n}$$

$$\Longrightarrow \phi \in \operatorname{Span} \mathcal{E}_A$$

$\square$

② $F_R(A)$ is free on $\mathcal{E}_A$

Pf: Suppose $\phi = r_1 \cdot \phi_{a_1} + r_2 \cdot \phi_{a_2} + \ldots + r_n \cdot \phi_{a_n}$

$= s_1 \cdot \phi_{a_1} + s_2 \cdot \phi_{a_2} + \ldots + s_n \phi_{a_n}$

$$\Longrightarrow (r_1 - s_1) \cdot \phi_{a_1} + (r_2 - s_2) \cdot \phi_{a_2} + \cdots + (r_n - s_n) \phi_{a_n} = 0$$

$$\Longrightarrow (r_1 - s_1) \underbrace{\phi_{a_1}(a_1)}_{=1} + (r_2 - s_2) \cancel{\phi_{a_2}(a_1)}^{0} + \ldots + (r_n - s_n) \cancel{\phi_{a_n}(a_1)}^{0} = 0$$

$$(r_1 - s_1) \cdot 1 = (r_1 - s_1) = 0$$

$$\Longrightarrow r_1 = s_1$$

Similarly, $r_i = s_i \quad \forall i$

$\square$

Thm: (The universal property of free R-modules)

R a ring, A is any set

M is an R-module s.t. $\exists\, f : A \longrightarrow M$.

There is a unique R-module homomorphism

$$\Phi_A : F(A) \longrightarrow M$$

s.t.

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "f"'] & F(A) \arrow[d, dashed, "\exists!\, \Phi_A"] \\ & M \end{tikzcd}$$

$$a \longmapsto \phi_a$$

Pf: $\Phi_A : F(A) \longrightarrow M$

$$(\phi : A \to R) \longmapsto \sum_{a \in A} \overbrace{\phi(a)}^{\in R} \cdot \overbrace{f(a)}^{\in M}$$

$\square$

Cor: If R is a ring, F is any free module on a set A

Then $F \cong F(A)$

Pf: $A \subset F$ that generates F freely over R

$j : A \longrightarrow F$

$$
\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[dr, "j"'] & F(A) \arrow[d, "\Phi_A"] \\
 & F
\end{tikzcd}
$$

Thee is an obvious map $\Psi_A : F \longrightarrow F(A)$

$$r_1 a_1 + \dots + r_n a_n \longmapsto r_1 \phi_{a_1} + r_2 \phi_{a_2} + \dots + r_n \phi_{a_n}$$

Clearly this map

$$
\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[dr, "j"'] \arrow[ddr, "\iota"'] & F(A) \arrow[d, "\Phi_A"] \arrow[dd, bend left=60, "Id_{F(A)}"] \\
 & F \arrow[d, "\Psi_A"] \\
 & F(A)
\end{tikzcd}
$$

By uniqueness $\Psi_A \circ \Phi_A = Id_{F(A)}$

$\Longrightarrow$ $\Phi_A : F(A) \longrightarrow F$ is an R-module isomorphism

∎