L17: Spanning sets and free modules

Definition 17.1

Let M be an R-module.
An R**-linear combination** of elements $m_1, \dots, m_n \in M$ is an element of the form

$$a_1 \bullet m_1 + a_2 \bullet m_2 + \cdots + a_n \bullet m_n \quad a_i \in R$$

We say a subset $A \subset M$ **spans** or **generates** the module if every element of M is an R-linear combination of elements in A.
More generally, if $B \subset M$, the **submodule spanned/generated by** B is

$$RB \coloneqq \{a_1 \bullet m_1 + a_2 \bullet m_2 + \cdots + a_n \bullet m_n \mid n \in \mathbb{Z}^+,\, a_i \in R,\, m_i \in B\}$$

Exercise: Show that RB is an R-module

Example 17.1. For any ring R with $1 \neq 0$ every element is a "linear combination" of $\{1\}$ i.e. if $r \in R$, then $r = r \bullet 1$.
So $R = R\{1\}$ is spanned by a single element as an R-module

Example 17.2. 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

$$a \bullet (a_0 + a_1 X + \cdots + a_n X^n) \coloneqq (a \bullet a_0) + (a \bullet a_1) \bullet X + \cdots + (a \bullet a_m) X^n$$

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

Observe $R[X]$ has **no** finite spanning set! To see this, suppose $R[X]$ is spanned by

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

Let $d = \max\{\deg p_1(X), \dots, \deg p_n(X)\}$ Then $d < \infty \implies \forall a_1, \dots, a_n \in R$

$$\deg[a_1 \bullet p_1(X) + a_2 \bullet p_2(X) + \cdots + a_n \bullet p_n(X)] \leq d \implies X^{d+1} \notin \mathrm{Span}\{p_1(X), \dots, p_n(X)\}$$

Definition 17.2

We say an R-module M is **finitely generated** if it is has a finite spanning set. We say M is **cyclic** if it is spanned by a single element.

Example 17.3. 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 17.4. R a ring, $F = R^n$ is the free R-module of rank n. F has a natural spanning set:

$$E_n \coloneqq \left\{ \begin{array}{c} e_1 = (1, 0, 0, \dots, 0) \\ e_2 = (0, 1, 0, \dots, 0) \\ e_3 = (0, 0, 1, \dots, 0) \\ \dots \\ e_n = (0, 0, 0, \dots, 0, 1) \end{array} \right\}$$

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

$$\begin{aligned}(a_1, a_2, \dots, a_n) =& a_1 \cdot (1, 0, 0, \dots, 0) + a_2 \cdot (0, 1, 0, \dots, 0) + \cdots + a_n \cdot (0, 0, 0, \dots, 1)\\ =& a_1 \cdot e_1 + a_2 \cdot e_2 + \cdots + a_n \cdot e_n\end{aligned}$$

Recontextualizing the free R-module of rank n:

Consider the set $\{1, 2, 3, \dots, n\}$ A function

$$\begin{aligned}a\colon \{1, 2, 3, \dots, n\} &\to R\\ 1 &\mapsto a(1) = a_1\\ 2 &\mapsto a(2) = a_2\\ &\dots\\ n &\mapsto a(n) = a_n\end{aligned}$$

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

$$a\colon \{1, 2, \dots, n\} \to R$$

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

$$R^n = \{a\colon \{1, 2, \dots, n\} \to R$$

The obvious addition is

$$\begin{aligned}a + b\colon \{1, 2, \dots, n\} &\to R\\ 1 &\mapsto a(1) + b(1)\\ 2 &\mapsto a(2) + b(2)\\ &\dots\\ n &\mapsto a(n) + b(n)\end{aligned}$$

The obvious scalar multiplication is

$$\begin{aligned}r \cdot a\colon \{1, 2, \dots, n\} &\to R\\ 1 &\mapsto r \cdot a(1)\\ 2 &\mapsto r \cdot a(2)\\ &\dots\\ n &\mapsto r \cdot a(n)\end{aligned}$$

Definition 17.3

Fix a ring R. An R-module F is **free** on a set A if $\forall m \in F$ there are **unique** elements

$$m_1, m_2, \ldots, m_n \in A$$
$$a_1, a_2, \ldots, a_n \in R$$

s.t. $m = a_1 \cdot m_1 + a_2 \cdot m_2 + \cdots + a_n \cdot m_n$.
We call A set of **free generators** of F or a **basis** of F.
Note: Usually, we ask that the basis is **ordered** in some way.

Example 17.5. The set $E_n = \{e_1, e_2, \ldots, e_n\}$ is a basis for the free module of rank n.

Example 17.6. $\mathbb{Z}/2\mathbb{Z}$ is a non-free Z-module.

$$\begin{aligned} \overline{1} &= 1 \cdot \overline{1} \\ &= 3 \cdot \overline{1} \end{aligned}$$

Example 17.7. Is every submodule of a free module free?
$\mathbb{Z}/4\mathbb{Z}$ is a free module over $\mathbb{Z}/4\mathbb{Z}$
Exercise: Check that $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}\{\overline{1}\}$ is free.
$2\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{2}\} \subset \mathbb{Z}/4\mathbb{Z}$ is a submodule.
BUT:

$$\overline{2} \cdot \overline{2} = \overline{0}$$
$$\overline{0} \cdot \overline{2} = \overline{0}$$

There is no unique way of writing $\overline{0}$ as a $(\mathbb{Z}/4\mathbb{Z})$-linear combination of $\{\overline{2}\}$. This implies $2 \cdot \mathbb{Z}/4\mathbb{Z} = (\overline{2})$ is **not** free

Example 17.8. Fix a ring R. Let A be **any** set

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

Proposition 17.4

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

Proof. Let $\phi, \psi \colon A \to R$ then addition

$$\begin{aligned} \phi + \psi \colon A &\to R \\ a &\mapsto \phi(a) + \psi(a) \end{aligned} \qquad\qquad \begin{aligned} r \cdot \phi \colon A &\to R \\ a &\mapsto r \cdot \phi(a) \end{aligned}$$

Consider the inclusion map

$$\begin{aligned} \iota \colon A &\to F_R(A) \\ a &\mapsto \phi_a \colon A \to R \\ & \qquad x \mapsto \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases} \end{aligned}$$

Obviously this map is injective. If $\phi_a = \phi_b$ then $\phi_a(a) = 1 = \phi_b(a) \implies a = b$.
We call $\iota(A) = E_A$ and we see that
(1) E_A spans $F_R(A)$

Proof. $(\phi\colon A \to R) \in F_R(A)$
Let $\{a_1, \dots, a_n\} \subset A$ such that $\phi(a_i) \neq 0$. Then

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

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

$$\implies \phi \in \operatorname{Span} E_a$$

■

(2) $F_R(A)$ is free on E_A

Proof. Suppose

$$\phi = r_1 \cdot \phi_{a_1} + r_2 \cdot \phi_{a_2} + \cdots + r_n \cdot \phi_{a_n}$$
$$= s_1 \cdot \phi_{a_1} + s_2 \cdot \phi_{a_2} + \cdots + s_n \cdot \phi_{a_n}$$

Then

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

$$\implies (r_1 - s_1) \cdot \underbrace{\phi_{a_1}(a_1)}_{=1} + (r_2 - s_2) \cdot \cancelto{0}{\phi_{a_2}(a_1)} + \cdots + (r_n - s_n) \cdot \cancelto{0}{\phi_{a_n}(a_1)} = 0$$

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

Similarly $r_i = s_i \, \forall i$ ■

■

Theorem 17.5

Let R be a ring, A is any set, M is an R-module such that there exists $f\colon A \to M$.
There is a unique R-module homomorphism

$$\Phi_A\colon F(A) \to A$$

such that

TIKZ

Proof.

$$\Phi_A\colon F(A) \to M$$
$$(\phi\colon A \to R) \mapsto \sum_{a \in A} \underbrace{\phi(a)}_{\in R} \cdot \underbrace{f(a)}_{\in M}$$

■

Corollary 17.6

If R is a ring and F is any free module on a set A, then $F \cong F(A)$

Proof. $A \subset F$ that generates F freely over R, $j\colon A \to F$

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

There is an obvious map

$$\Psi_A\colon F \to F(A)$$
$$r_1a_1 + \cdots + r_na_n \mapsto r_1\phi_{a_1} + r_2\phi_{a_2} + \cdots + r_n\phi_{a_n}$$

Clearly this map

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

By uniqueness $\Psi_A \circ \Phi_A = \mathrm{Id}_{F(A)}$ and hence $\Phi_A\colon F(A) \to F$ is an R-module isomorphism ■