L18: Abstract linear algebra

Definition 18.1

A subset A of an R-module M is said to be **linearly independent** if for $a_1, \dots, a_n \in R$ and $m_1, \dots, m_n \in A$ such that

$$a_1 \bullet m_1 + \cdots + a_n \bullet m_n = 0$$

Then $a_1 = a_2 = \cdots = a_n = 0$.
If A is *not* linearly independent then we say it is **linearly dependent**

Example 18.1. A basis B for a free R-module is linarly independent i.e

$$B = \{1, X, X^2, X^3, \dots\}$$

is linearly independent in $\mathbb{R}[X]$(when viewed as an R-module).

Definition 18.2

A **basis** of a free R-module is a linearly independent spanning set

Example 18.2. $\{0\} \subset M$ is not linearly independent (assumign $R \neq 0$) e.g $1 \bullet 0 = 0 = 0 \bullet 0$

Example 18.3. $\mathbb{Z}/2\mathbb{Z}$ as a $(\mathbb{Z}/4\mathbb{Z})$-module.
The only possible linearly independent subset is $\{\overline{1}\}$

$$\overline{2} \in \mathbb{Z}/4\mathbb{Z} \implies \overline{2}_r \bullet \overline{1}_2 = \overline{0}_2 \in \mathbb{Z}/2\mathbb{Z}$$

Theorem 18.3

If V is a finitely generated vector space over a field F, then V is a free F-vector space

Proof. Let $A = \{v_1, \dots, v_n\}$ be a finite spanning set of V.
We may suppose no proper subset of A is spanning. We show that A is linearly independent:
Suppose otherwise, then let $\alpha_1, \dots, \alpha_n \in F$ such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

such that $\alpha_1, \dots, \alpha_n$ not all zero.
After possibly rearraning, we may assume $\alpha_1 \neq 0$. Since F is a field, $\frac{1}{\alpha_1} \in F$ which implies

$$\begin{aligned} v_1 =& \frac{1}{\alpha_1} \bullet (-\alpha_2 v_2 - \alpha_3 v_3 - \cdots - \alpha_n v_n) \\ =& \left(\frac{-\alpha_2}{\alpha_1}\right) \bullet v_2 + \left(\frac{-\alpha_3}{\alpha_1}\right) \bullet v_2 + \cdots + \left(\frac{-\alpha_n}{\alpha_1}\right) \bullet v_2 \end{aligned}$$

and hence $v_1 \in \mathrm{Span}\{v_2, \dots, v_n\}$. But if any vector can be written by this span, then we have

$$\mathrm{Span}\{v_2, \dots, v_n\} = V$$

contradicting the fact that A is minimal. Hence A is linearly independent.
It remains to show that V is a free F-vector space. Suppose $v \in V$ and $a_i, b_i \in F$ with

$$\begin{aligned} v =& a_1 \bullet v_2 + a_2 \bullet v_2 + \cdots + a_n \bullet v_n \\ =& b_1 \bullet v_1 + b_2 \bullet v_2 + \cdots + b_n \bullet v_n \end{aligned}$$

Then we have

$$(a_1 - b_1) \bullet v_1 + (a_2 - b_2) \bullet v_2 + \cdots + (a_n - b_n) \bullet v_n = 0$$

Since A is linearly independent then for all i

$$a_i - b_i = 0 \implies a_i = b_i$$

Therefore, V is free on A. ■

Corollary 18.4

If V is a finitely generated F-vector space and A is a minimal spannig set, then V is a free F-vector space on A and A is a basis for V.

Corollary 18.5

If V is an F-vector space with finite spanning set A, then A contains a basis B for V.

Proof. Take a minimal spanning subset of A. ■

Theorem 18.6

Suppose V is an F-vector space with basis $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ is a linearly independent set.
After possibly rearranging A, the sets

$$C_k \coloneqq \{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\} \quad \forall 0 \leq k \leq m$$

are bases for V. In particular $n \geq m$.

Proof. Prove this by induction:
When $k = 0$, $C_0 = A = \{a_1, \ldots, a_n\}$ this is already true.
Now suppose C_k is a basis for V, we will show C_{k+1} is a basis for V.

$$\begin{aligned} & C_k = \{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\} \text{ spans } V \\ \implies & b_{k+1} = \alpha_1 \bullet b_1 + \alpha_2 \bullet b_2 + \cdots + \alpha_k \bullet b_k + \alpha_{k+1} \bullet a_{k+1} + \cdots + \alpha_n \bullet a_n \end{aligned}$$

Now B is linearly independent and so there exists $a_{k+i} \neq 0$ for some $i \geq 1$.

After rearranging, we may assume $\alpha_{k+1} \neq 0$, and so

$$
\begin{aligned}
a_{k+1} &= \frac{1}{\alpha_{k+1}} \cdot (b_{k+1} - \alpha_1 \cdot b_1 - \cdots - \alpha_k \cdot b_k - \alpha_{k+2} \cdot a_{k+2} - \cdots - \alpha_n \cdot a_n) \\
&= \left(\frac{1}{\alpha_{k+1}}\right) \cdot b_{k+1} + \left(\frac{-\alpha_1}{\alpha_{k+1}}\right) \cdot b_1 + \cdots + \left(\frac{-\alpha_k}{\alpha_{k+1}}\right) \cdot b_k + \left(\frac{-\alpha_{k+2}}{\alpha_{k+1}}\right) \cdot a_{k+2} + \cdots + \left(\frac{-\alpha_n}{\alpha_{k+1}}\right) \cdot b_n
\end{aligned}
$$

This implies

$$
\begin{aligned}
&a_{k+1} \in \operatorname{Span}\{b_1, \ldots, b_{k+1}, a_{k+2}, \ldots, a_n\} = \operatorname{Span} C_{k+1} \\
\implies &\operatorname{Span} C_{k+1} \supset \operatorname{Span}\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\} = \operatorname{Span} C_k = v \\
\implies &\operatorname{Span} C_{k+1} = V
\end{aligned}
$$

It remains to show C_{k+1} is linearly independent.
Suppose

$$
\begin{aligned}
&\beta_1 \cdot b_1 + \cdots + \beta_k \cdot b_k + \beta_{k+1} \cdot b_{k+1} + \gamma_{k+2} \cdot a_2 + \cdots + \gamma_n a_n = 0 \\
&= \left(\sum_{i=1}^{k} \beta_i \cdot b_i\right) + \beta_{k+1} \cdot \left(\sum_{i=1}^{k} \alpha_i \cdot b_i + \sum_{j=k+1}^{n} \alpha_j \cdot a_j\right) + \left(\sum_{j=k+2}^{n} \gamma_j \cdot \alpha_j\right) \\
&= \left[\sum_{i=1}^{k} (\beta_i + \beta_{k+1}\alpha_i) \cdot b_i\right] + (\beta_{k+1}\alpha_{k+1}) \cdot a_{k+1} + \left[\sum_{j=k+2}^{n} (\beta_{k+1}\alpha_j + \gamma_j) \cdot a_j\right]
\end{aligned}
$$

Because C_k is linearly independent then

$$\beta_i + \beta_{k+1}\alpha_i = 0, \quad \beta_{k+1}\alpha_{k+1} = 0, \quad \beta_{k+1}\alpha_j + \gamma_j = 0$$

By assumption $a_{k+1} \neq 0$ and so since F is a field then $B_{k+1} = 0$ and hence $\beta_i = \gamma_j = 0$.
Therefore, C_{k+1} is linearly independent. ■

Corollary 18.7

If V is an F-vector space with basis $B = \{b_1, \ldots, b_n\}$, then any linearly independent set A has at most n elements and any spanning set C has at least n elements.

Corollary 18.8

Any two bases B, B' of a finitely generated F-vector space have the same cardinality.

Definition 18.9

If V is a finitely generated F-vector space, then the **dimension** of V is

$$\dim_F V := \dim V := \text{ cardinality of any basis of } V$$

We say V is finite dimensional
If V is not finitely generated, then we say it is **infinite dimensional** ($\dim V = \infty$)

Example 18.4.
- $\dim \mathbb{R}^2 = 2$
- $\dim\{\text{real polynomials of degree at most } 3\} = 4$
- $\dim \mathbb{R}[X] = \infty$

Corollary 18.10

If V is a finite dimensional F -vector space with $B = \{b_1, \dots, b_n\}$, then B defines an F-vector space isomorphism

$$\Phi_B \colon V \xrightarrow{\cong} F^n$$

Proof. First

$$\begin{aligned} \Phi_B \colon V &\to F^n \\ b_1 &\mapsto e_1(1, 0, 0, \dots, 0) \\ b_2 &\mapsto e_2(0, 1, 0, \dots, 0) \\ \dots& \\ b_n &\mapsto e_n(0, 0, \dots, 0, 1) \end{aligned}$$

extend this linearly i.e

$$\begin{aligned} \Phi_B(\alpha_1 \cdot b_1 + \alpha_2 \cdot b_2 + \cdots + \alpha_n b_n) =& \alpha_1 \cdot \Phi_B(b_1) + \alpha_\bullet \Phi_B(b_2) + \cdots + \alpha_\bullet \Phi_B(b_n) \\ =& \alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \cdots + \alpha_n \cdot e_n \end{aligned}$$

Check injectivity

$$\operatorname{Ker} \Phi_B = \{\alpha_1 \cdot b_1 + \cdots + \alpha_n \cdot b_n \mid \alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \cdots + \alpha_n \cdot e_n = 0\} = \{0\}$$

Check surjectivity, we have

$$v = \alpha_1 \cdot e_1 + \cdots + \alpha_n \cdot e_n \in F^n$$

then

$$\Phi_B(\alpha_1 \cdot b_1 + \cdots + \alpha_n \cdot b_n) = v$$

■