4.2 Free Modules

Nov. 13, 2008

Definition 4.2.1. Let R be a ring and M be a R-module.

(1) $x_1, x_2, \cdots, x_n \in M$ are linear independent if for any $c_1, c_2, \cdots, c_n \in R$,

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = 0 \Rightarrow c_1 = c_2 = \cdots = c_n = 0$$

(2) $x_1, x_2, \cdots, x_n \in M$ span M if $(x_1, x_2, \cdots, x_n) = M$ (i.e. for any $m \in M$, there exists $c_1, c_2, \cdots, c_n \in R$ such that $m = c_1x_1 + c_2x_2 + \cdots + c_nx_n$).

(3) The set $\{x_1, x_2, \cdots, x_n\} \subseteq M$ is a basis if its elements are linear independent and span M.

(4) M is free if M has a basis.

Example 4.2.2. $M = R = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

Since $\overline{1}$ is a basis, $\mathbb{Z}_6$ is free. In fact, if $M = R$ and M has 1, then 1 is a basis.

Example 4.2.3. $R = \mathbb{Z}_6$. $M = \{\overline{0}, \overline{2}, \overline{4}\}$.

$\overline{3} \cdot \overline{2} = \overline{0} \Rightarrow \overline{2}$ is not linear independent.

$\overline{3} \cdot \overline{4} = \overline{0} \Rightarrow \overline{4}$ is not linear independent.

Hence, there is no basis in M and M is not free.

Theorem 4.2.4. *Let M be a free R-module, where R is a division ring. Suppose M has 2 bases of cardinalities n, m, respectively. Then, $n = m$.*

Proof. Let $\{e_i\}_{i=1}^n$ and $\{f_i\}_{i=1}^m$ be two bases of M. Suppose $n \neq m$. W.L.O.G, we assume $m < n$.

Since $f_1 \in \text{span}_R(e_1, e_2, \cdots, e_n)$, we have $f_1 = c_1e_1 + c_2e_2 + \cdots + c_ne_n$ for some $c_i \in R$ but not all 0. Say $c_k \neq 0$. Then, $e_k = c_k^{-1}(f_1 - c_1e_1 - c_2e_2 - \cdots - c_{k-1}e_{k-1} - c_{k+1}e_{k+1} - \cdots - c_ne_n)$ (c_k^{-1} exists for R is a division ring).

It is routine to check $\{e_i\}_{i=1}^n \setminus \{e_k\} \cup \{f_1\}$ is a basis.

Similarly, $\{e_i\}_{i=1}^n \setminus \{e_k, e_{k'}\} \cup \{f_1, f_2\}$ is a basis, where $k \neq k'$ (the coefficient of f_1 is not the only one nonzero element; otherwise, $f_2 = c'f_1$, $c' \in R$ and this contradicts to the fact that $\{f_i\}_{i=1}^m$ is a basis).

After m steps, we have a basis containing $f_1, f_2, \cdots, f_m$ and some e_i. Since $f_1, f_2, \cdots, f_m, e_i$ are not linear independent for $\{f_j\}_{j=1}^m$, we have a contradiction. $\square$

Definition 4.2.5. If all the bases of a free module M have the same cardinality n, n is called the rand or dimension of M.

Theorem 4.2.6. *Let M be a free module over a commutative ring R. Suppose M has 2 bases of cardinalities n, m, respectively. Then, $n = m$.*

Proof. Suppose $m \leq n$ and let $\{e_i\}_{i=1}^n$ and $\{f_i\}_{i=1}^m$ be two bases. Then

$$\begin{aligned} f_i &= \sum_{j=1}^n a_{ij} e_j \\ e_k &= \sum_{j=1}^m b_{kj} f_j \end{aligned}$$

where $1 \leq i \leq m$, $1 \leq k \leq n$, and a_{ij}, $b_{kj} \in R$. In matrix form,

$$\begin{aligned} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{pmatrix} &= A \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} \\ \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} &= B \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{pmatrix} \end{aligned}$$

for some $m \times n$ matrix A and $n \times m$ matrix B over R. Since $\{e_i\}_{i=1}^n$ is a basis, $BA = I_n$. Set $B' = \begin{array}{|c|c|}\hline \text{B} & 0 \\ \hline \end{array}_{n \times n}$ and $A' = \begin{array}{|c|}\hline \text{A} \\ \hline 0 \\ \hline \end{array}_{n \times n}$. Then, $B'A" = I_n$. Note: $\det(B'A') = \det(B')\det(A') = 0 \times 0 = 0$, a contradiction to $\det(I_n) = 1$. $\square$

Question: why $\det(B'A') = \det(B')\det(A')$ over any commutative ring?

Example 4.2.7. $\mathbb{Z}_2 = \{0, 1\}$. $R = M = \mathbb{Z}_2[x]$. Hence, $M = R$ is a R-module and 1 is a basis.

Let $f_1, f_2 \in M$ such that $f_1(x^{2i}) = x^i$, $f_1(x^{2i-1}) = 0$, $f_2(x^{2i}) = 0$, and $f_2(x^{2i-1}) = x^i$, for $i \in \mathbb{N} \bigcup \{0\}$.

Claim: $f_1, f_2 \in M$ are linear independent.

Suppose $g_1 f_1 + g_2 f_2 = 0$, for $g_1, g_2 \in R$. Then

$$\begin{aligned} 0 &= (g_1 f_1 + g_2 f_2)(x^{2i}) = g_1 f_1(x^{2i}) = g_1(x^i) \\ 0 &= (g_1 f_1 + g_2 f_2)(x^{2i-1}) = g_2 f_2(x^{2i-1}) = g_2(x^i) \end{aligned}$$

for $i \in \mathbb{N} \bigcup \{0\}$. Hence, $g_1 = g_2 = 0$.

Claim: f_1, f_2 span M.

Pick any $g \in M$ and $g_1, g_2 \in R$ such that $g_1(x^i) = g(x^{2i})$ and $g_2(x^i) = g(x^{2i-1})$ for $i \in \mathbb{N} \bigcup \{0\}$. Then,

$$\begin{aligned} (g_1 f_1 + g_2 f_2)(x^{2i}) &= g_1 f_1(x^{2i}) = g_1(x^i) = g(x^{2i}) \\ (g_1 f_1 + g_2 f_2)(x^{2i-1}) &= g_2 f_2(x^{2i-1}) = g_2(x^i) = g(x^{2i-1}) \end{aligned}$$

Hence, $g = g_1 f_1 + g_2 f_2$.

We have shown that $M \cong R \cong R^2 \cong R^3 \cdots$.

Definition 4.2.8. Let M, N be R-modules.

Let $M \oplus N = \{(m, n) | m \in M, n \in N\}$ and $+$ and scalar multiplication are defined componentwise. Then $M \oplus N$ is a R-module, called the direct sum of M and N.

Note 4.2.9. *$M \oplus N \oplus T$ can be defined similarly for R-modules M, N, T.*