2008

Studies in free module and it's basis

Hsu-chia Chen

Studies In Free Module And Its Basis

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

by

Hsu-chia Chen

March 2008

Studies In Free Module And Its Basis

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Hsu-chia Chen

March 2008

Approved by:

[redacted]

3-17-08

Jim Okon, Committee Chair

Date

[redacted]

Zahid Hasan, Committee Member

[redacted]

Wenxiang Wang, Committee Member

[redacted]

Peter Williams, Chair,
Department of Mathematics

[redacted]

Joseph Chavez
Graduate Coordinator,
Department of Mathematics

Abstract

In this paper, we study some basic properties of free modules over a ring. A module with a basis is called a free module and a free module over a division ring (or field) is called a vector space. We show every vector space has a basis and any two bases of a vector space have same cardinality. However, a free module over an arbitrary ring (with identity) does not have this property. An example is given of a free R-module with the property that $\forall n > 0$, there exists a basis of cardinality n. That is, as an R-module, $R \cong R^n = R \oplus R \oplus ... \oplus R$ for any finite number of summands.

Acknowledgements

I would like to express my gratitude to everyone in helping the writing of this project either directly or indirectly. My first thanks go to Dr. James Okon for all his help and support. I also want to show my appreciation to Dr. Zahid Hasan and Dr. Wenxiang Wang for their comments on the paper. Special thanks will be extended to Dr. Charles Stanton for his helps on the formation of this paper. Last but not the least, I sincerely thank my friend Lu for his inspiration and encouragement.

Table of Contents

Chapter 1

Introduction

1.1 History and Importance

The vector concept is first introduced by Bolzano in the 19th century. In the book, published in 1804, he considers points, lines, and planes as undefined elements and defined operations on them. This is an important step for the linear space to arise. After several years, Möbius starts to consider directed quantities, which is an early appearance of vectors. Then, Bellavitis defines the equipollent sum of line segments and obtains an equipollent calculus, which is essentially a vector space. Many years after, Peano defines dimension; proves finite dimensional spaces have a basis and gives examples of infinite dimensional linear spaces. [OR96]

The notion of vector spaces has wide applications in mathematics, the sciences, and engineering. It is used to prove theorems in plane geometry and to analyze the equilibrium of two-dimensional rigid bodies. [RA77] Euclidean spaces are the most familiar vector spaces. In studying the properties and structure of a vector space, we can study many other important vector spaces.

1.2 Overview

In Chapter 2, we define modules and linearly independent sets. Then we introduce submodules, homomorphisms, cartesian products, sums of modules, and products of modules. Theorem 2.16 and 2.17 characterize when a module is an internal or external direct sum of modules. Finally, Theorem 2.21 shows that for an R-module A, $Hom_R(A, A)$

is a ring.

In Chapter 3, we study the notion of a free module. Theorem 3.1 shows that a module is free if and only if it has a basis. We then show in Theorem 3.5 that every module over a division ring has a basis. We use Zorm's Lemma to handle the case when a module has an infinite basis.

Several results in Chapter 5 require some knowledge of cardinal numbers. In Chapter 4, we define cardinal number and develop some of their basic properties. In particular, we prove the Schroeder-Bernstein theorem and some properties of addition and multiplication of cardinal numbers.

For a vector space, all bases have the same cardinality and their number is called the dimension of the vector space. If a module has a basis of infinite cardinality, all bases have the same cardinality. However, for modules with finite basis, this is not necessarily true. We give an example of a module that has a basis of cardinality n for each $n \in \mathbf{N}$.

Chapter 2

Vector Spaces and Modules

We begin this chapter with the definition of a module and linearly independent sets. Then, in Section 2.1, we introduce submodules, homomorphisms, and cartesian products. In Section 2.2, we introduce sums and products of modules. Theorems 2.16 and 2.17 characterize when a module is an external or internal direct sum of modules. Finally, Theorem 2.21 shows that for an R-module A, $Hom_R(A, A)$ is a ring.

Since the notion of a module is closely related to the concept of a vector space, we will present a short overview of the general properties of vector spaces that carry over to modules in this section.

Definition 2.1. [Gal02] Let R be a ring. Then an *R-module* is a set together with two binary operations of vector addition and scalar multiplication, satisfying the following properties: Under Addition

1. Closure: $u + v \in V$, for all $u, v \in V$.

2. Associativity: $u + (v + w) = (u + v) + w$, for all $u, v, w \in V$.

3. Commutativity: $u + v = v + u$, for all $u, v \in V$.

4. Identity: There exists $0 \in V$ such that $u + 0 = 0 + u = u$, for all $u \in V$.

5. Inverse: For each $u \in V$, there is an element $-u \in V$ such that $u + (-u) = 0$.

Under Scalar Multiplication

1. Closure: $cu \in V$, for all $c \in F$ and all $u \in V$.

2. Distributivity for multiplication over addition: Let c be any element of F. Then, $c(u+v) = (cu) + (cv)$, for all $u, v \in V$.

3. Distributivity for multiplication over addition: Let c, $d \in F$, $u \in V$, then $(c+d)u = (cu) + (du)$.

4. Associativity: $c(du) = (cd)u$ for all c, $d \in F$ and all $u \in V$.

5. Identity: $1 \cdot u = u$, for all $u \in V$.

One of the most important ideas in the study of modules is that of linear independence.

Definition 2.2. The vectors $v_1, v_2, ..., v_n$ in an R-module M are said to be *linearly independent* if whenever $c_1v_1 + c_2v_2 + ... + c_nv_n = 0$, for some scalars $c_1, \ldots, c_n \in R$, we must have $c_1 = c_2 = ... = c_n = 0$.

The next theorem gives a characterization of linear independence for vector spaces.

Theorem 2.3. *[KH01] The set of nonzero vectors $v_1, v_2, ..., v_n$ in a vector space V is linearly dependent if and only if one of the vectors v_k, $k \geq 2$, is a linear combination of the preceding vectors $v_1, v_2, ..., v_{k-1}$.*

Proof. Suppose $v_1, v_2, ..., v_n$ are linearly dependent. Then, $c_1v_1 + c_2v_2 + ... + c_nv_n = 0$ such that at least one scalar c_i is not zero. Now, let k be the largest subscript such that $c_k \neq 0$. If $k > 0$, then $v_k = -(\frac{c_1}{c_k})v_1 - (\frac{c_2}{c_k})v_2 - ... - (\frac{c_{k-1}}{c_k})v_{k-1}$. If $k = 1$, the $c_1v_1 = 0$, which implies that $v_1 = 0$, a contradiction to hypothesis that none of the vectors are the zero vector. Thus one of the vectors v_k is a linear combination of the preceding vectors $v_1, v_2, ..., v_{k-1}$. Conversely, if $v_k = c_1v_1 + c_2v_2 + ... + c_{k-1}v_{k-1}$, then $c_1v_1 + c_2v_2 + ... + c_{k-1}v_{k-1} + (-1)v_k + 0v_{k+1} + ... + 0v_n = 0$. Since there is at least one non-zero coefficient, -1, the set of vectors $v_1, v_2, ..., v_n$ are linear dependent. □

If R is a commutative ring, then everything will work as well for (unitary) right R-modules, i.e., we can similarly define a function $g : A \times R \to A$ satisfying the analogues of Definition 2.1 for a right R-module. Since every theorem of left R-modules has a right analogue, throughout this chapter, an R-module means a left R-module.

Example 2.4. Every abelian group A with additive operation is a Z-module, where for all $n \in Z$, $a \in A$, $na = a + a + \cdots + a \in A$.

2.1 Submodules, and Homomorphisms

Definition 2.5. If A is an R-module over a ring R, then a nonempty subset B of A is a *submodule* if and only if it is an additive subgroup of A, which is closed under multiplication by elements of R. That is, for all $r \in R$, $b \in B$, $rb \in B$.

If A is a module over a division ring, then a submodule of A is called a subspace.

Note that a submodule B of an R-module A is an additive subgroup with $rB \subseteq B$ for all $r \in R$.

Example 2.6. The trivial submodule of an R-module is zero module, denoted by (0).

Example 2.7. If $\{B_i \mid i \in I\}$ is a family of submodules of a module A, then the intersection of B_i, in notation $\cap_{i \in I} B_i$, is a submodule of A.

Definition 2.8. If A, B are modules over a ring R, then for all $r \in R$ and $a, c \in A$, the map $f : A \longrightarrow B$ is an *R-module homomorphism* if

1. $f(a + c) = f(a) + f(c)$
2. $f(ra) = rf(a)$

Equivalently, for all $x, y \in A$, $r, s \in R$, if $f(rx + sy) = rf(x) + sf(y)$, then f is an R-module homomorphism as well. If R is a division ring, then an R-module homomorphism is called a linear transformation. Indeed, an R-module homomorphism $f : A \longrightarrow B$ is an abelian group homomorphism under addition.

Theorem 2.9. *If B is a subset of an R-module A, $\{B_i \mid i \in I\}$ is a family of submodules of A, $a \in A$, and $Ra = \{ra \mid r \in R\}$. Then*

1. *Ra is a submodule of A and $f : R \longrightarrow Ra$ given by $r \mapsto ra$ is an R-module epimorphism.*
2. *$D = RX =< X >= \{\sum_{i=1}^{s} r_i a_i \mid a_i \in X; r_i \in R\}$ is the submodule generated by X.*

3. *The sum of the family $\{B_i \mid i \in I\}$ consisting of all finite sums $b_{i_1} + b_{i_2} + ... + b_{i_n}$ where $b_{i_k} \in B_{i_k}$ is a submodule of A.*

Proof.

1. Let ra, $sa \in Ra$. Then, $ra + sa = (r+s)a \in Ra$. So Ra is closed under addition. Also, $s(ra) = (sr)a \in Ra$, for all r, $s \in R$, $a \in A$. Thus, Ra is closed under scalar multiplication. Therefore, Ra is a submodule of A. Now, define $f : R \to Ra$ by $f(r) = ra$. Let $r_1, r_2 \in R$. Then, $f(r_1+r_2) = (r_1+r_2)a = r_1a+r_2a = f(r_1)+f(r_2)$. Thus, f preserves addition. Let c, $r \in R$. Then, $f(cr) = (cr)a = c(ra) = cf(r)$. Clearly, $f(r) = ra \in Ra$, so f is onto. Therefore, $f : R \to Ra$ is an R-module epimorphism.

2. Let $\sum_{i=1}^{s} r_i a_i$, $\sum_{j=1}^{s} m_j a_j \in RX$. Then, $(r_1a_1 + \cdots + r_s a_s) + (m_1 a_1 + \cdots + m_s a_s) = (r_1 a_1 + m_1 a_1) + \cdots + (r_s a_s + m_s a_s) = (r_1 + m_1)a_1 + \cdots + (r_s + m_s)a_s \in RX$. Thus, Rx is closed under addition. To see it is closed under multiplication, we let r_i, $t \in R$, $\sum_{i=1}^{s} r_i a_i \in RX$. Then, $t(r_1 a_1 + \cdots + r_s a_s) = (tr_1 a_1 + \cdots + tr_s a_s) \in RX$. Therefore, RX is a submodule of A.

3. The sum of $\{B_i \mid i \in I\}$ is $< \cup_{i \in I} B_i >= \{b_{i_1} + \cdots + b_{i_n} \mid b_{i_j} \in B_{i_j}\}$. Let $b_{i_1} + \cdots + b_{i_n}$, $c_{i_1} + \cdots + c_{i_n} \in < \cup_{i \in I} B_i >$, where b_{i_k}, $c_{i_k} \in B_{i_k}$. Then, $(b_{i_1} + \cdots + b_{i_n}) + (c_{i_1} + \cdots + c_{i_n}) = (b_{i_1} + c_{i_1}) + \cdots + (b_{i_n} + c_{i_n}) \in < \cup_{i \in I} B_i$. So, $< \cup_{i \in I} B_i >$ is closed under addition. Now, for each $r \in R$, $r(b_{i_1} + \cdots + b_{i_n}) = rb_{i_1} + \cdots + rb_{i_n} \in < \cup_{i \in I} B_i >$. Hence, $< \cup_{i \in I} B_i >$ is closed under scalar multiplication. Thus, the sum of the family $\{B_i \mid i \in I\}$ is a submodule of A.

□

Next, we define Cartesian product and Canonical projection.

Definition 2.10. Let a nonempty set I be an index set and $\{A_i \mid i \in I\}$ be a family of sets. The set of all functions $f : I \to \cup_{i \in I} A_i$ is said to be the *Cartesian product* provided that for all $i \in I$, $f(i) \in A_i$. It is denoted $\prod_{i \in I} A_i$.

Definition 2.11. If $\prod_{i \in I} A_i$ is a cartesian product, then for each $k \in I$, a map $\pi_k : \prod_{i \in I} A_i \to A_k$ defined by $f \mapsto f(k)$ is called the *Canonical projection* of the product onto its kth component.

Theorem 2.12. *Let $\{A_i \mid i \in I\}$ be a family of sets indexed by a set I. If there is a set C, together with a family of maps $\{f_i : C \to A_i \mid i \in I\}$, then for any set B and family of maps $\{g_i : B \to A_i \mid i \in I\}$, there exists a unique map $g : B \to C$ such that $f_i g = g_i$ for all $i \in I$.*

2.2 Direct Sums and Basis

This section, we begin with the definition of **direct sums** and **direct products** in the category of groups.

Definition 2.13. Let G be a group and $\{N_i \mid i \in I\}$ be a family of normal subgroups of G. If $G =< \cup_{i \in I} N_i >$ and $N_j \cap < \cup_{i \neq j} N_i >=< e >$ for all $j \in I$, then G is said to be the *internal direct sum* of the family $\{N_i \mid i \in I\}$.

Definition 2.14. Let $\{G_i \mid i \in I\}$ be a family of groups. The *external direct product* of $\{G_i \mid i \in I\}$ is the set of all $f : I \to \cup_{i \in I} G_i$ such that $f(i) = e_i$, the identity in G_i. It is denoted $\prod_{i \in I} G_i$.

The next theorem shows that the direct sum and direct product of modules is again a module.

Theorem 2.15. *Let R be a ring and $\{A_i \mid i \in I\}$ a nonempty family of R-modules. If $\prod_{i \in I} A_i$ is the direct product of the abelian groups A_i and $\sum_{i \in I} A_i$ is the direct sum of the abelian groups A_i, then*

1. *$\prod_{i \in I} A_i$ is an R-module with the action of R given by $r\{a_i\} = \{ra_i\}$.*

2. *$\sum_{i \in I} A_i$ is a submodule of $\prod_{i \in I} A_i$.*

3. *The canonical projection $\alpha_k : \prod A_i \to A_k$ is an R-module epimorphism for each $k \in I$.*

4. *The canonical projection $\beta_k : A_k \to \sum A_k$ is an R-module monomorphism for each $k \in I$.*

Proof.

1. Let $\{a_i\}$, $\{b_i\} \in \prod_{i \in I} A_i$. Then, $\{a_i\} + \{b_i\} = \{a_i + b_i\} \in \prod_{i\in I} A_i$. Now, $r\{a_i\} = \{ra_i\} \in \prod_{i \in I} A_i$, where $r \in R$. Therefore, $\prod_{i\in I} A_i$ is closed under addition and scalar multiplication. The other modules properties are proven similarly. Thus, $\prod_{i \in I} A_i$ is an R-module.

2. Let $\sum_{i\in I} A_i = \{\{a_i\} \mid a_i \in A_i, a_i = 0 \text{ for almost all } i\}$. To see $\sum_{i \in I} A_i$ is a submodule of $\prod_{i\in I} A_i$, we need to check if $\sum_{i\in I} A_i$ is closed under the operations of $\prod_{i\in I} A_i$. Let $\{a_i\}$, $\{b_i\} \in \sum_{i\in I} A_i$, for some finite a_i, $b_i \neq 0$. Then, $\{a_i\} + \{b_i\} = \{a_i + b_i\} \in \sum_{i\in I} A_i$. So, $\sum_{i\in I} A_i$ is closed under addition. Now, $r\{a_i\} = \{ra_i\} \in \sum_{i\in I} A_i$. Hence, $\sum_{i\in I} A_i$ is closed under multiplication. Thus, $\sum_{i\in I} A_i$ is a submodule of $\prod_{i\in I} A_i$.

3. Define $\alpha_k : \prod A_i \to A_k$ by $\alpha_k(\{a_i\}) = a_k$, where $a_k \in A_k$. Let $\{a_i\}$, $\{b_i\} \in \prod_{i\in I} A_i$, then $\alpha_k(\{a_i\} + \{b_i\}) = (a_k + b_k) = \alpha_k(\{a_i\}) + \alpha_k(\{b_i\})$. Also, $\alpha_k(r\{a_i\}) = \alpha_k(\{ra_i\}) = ra_k = r\alpha_k(\{a_i\})$. If $a_k \in A_k$, let $x = \{a_i\}$, where $a_i = 0$ for $i \neq k$. Then, $\alpha_k(x) = a_k$. So, α_k is an R-module epimorphism.

4. To see $\beta_k : A_k \to \sum A_k$ is an R-module monomorphism, we let $a_k \in ker(\beta_k)$. Then, $\beta_k(a_k) = \{a_i\}$, where $a_i = 0$ for $i \neq k$. Since $\beta_k(\alpha_k) = 0$, $a_k = 0$. Hence, $ker(\beta_k) = \{0\}$ and β_k is one-to-one.

□

Theorem 2.16 gives a characterization of when a module is an external direct sum of modules.

Theorem 2.16. *(see p. 174 [Hun80]) Let A, A_1, A_2,..., A_n be R-modules over a ring R. Then $A \cong A_1 \oplus A_2 \oplus ... \oplus A_n$ if and only if there are R-module homomorphisms $\pi_i : A \to A_i$ and $\iota_i : A_i \to A$ such that, for each $i = 1, 2, ..., n$, we have*

1. $\pi_i \iota_i = 1_{A_i}$ for $i = 1, 2, ..., n$;

2. $\pi_j \iota_i = 0$ for $i \neq j$;

3. $\iota_1\pi_1 + \iota_2\pi_2 + ... + \iota_n\pi_n = 1_A$.

Proof.

($\Rightarrow$) Let the module $A = A_1 \oplus A_2 \oplus \cdots \oplus A_n$. Define $\pi_i : A \to A_i$ by $\pi_i(a_1, \ldots, a_n) = a_i$ and $\iota_i : A_i \to A$ by $\iota_i(a_i) = (0, \ldots, a_i, \ldots, 0)$. Then

1. $\pi_i\iota_i(a_i) = \pi_i(0, \ldots, a_i, \ldots, 0) = a_i$ for $i = 1, 2, \ldots, n$. So, $\pi_i \cdot \iota_i = 1_{A_i}$.

2. Let $i \neq j$. Then, $\pi_j\iota_i(a_i) = \pi_j(0, \ldots, a_i, \ldots, 0) = 0$ since only ith element is not 0.

3. Let $a \in A$. Then $a = (a_1, \ldots, a_n)$, $\exists a_i \in A_i$. Now, $\sum \iota_j\pi_j(a) = \sum \iota_j(a_j) = \sum(0, \ldots, a_j, \ldots, 0) = (a_1, \ldots, a_n) = a$. So, $\iota_1\pi_1 + \cdots + \iota_n\pi_n = I_A$.

($\Leftarrow$) Define $\varphi : A \to \prod_1^n A_i$ by $\varphi(a) = (\pi_1(a), \ldots, \pi_n(a))$, $\forall a \in A$. Then, for each $a, b \in A$, $r \in R$

$$\begin{aligned}
&\varphi(a + b) \\
&= (\pi_1(a + b), \ldots, \pi_n(a + b)) \\
&= (\pi_1(a) + \pi_1(b), \ldots, \pi_n(a) + \pi_n(b)) \\
&= (\pi_1(a) + \ldots + \pi_n(a)) + (\pi_1(b) + \ldots + \pi_n(b)) \\
&= \varphi(a) + \varphi(b).
\end{aligned}$$

Now

$$\begin{aligned}
&\varphi(ra) \\
&= (\pi_1(ra), \ldots, \pi_n(ra)) \\
&= (r\pi_1(a), \ldots, r\pi_n(a)) \\
&= r(\pi_i(a), \ldots, \pi_n(a)) \\
&= r\varphi(a).
\end{aligned}$$

If $a \in ker\varphi$, then $\varphi(a) = 0$. So, $(\pi_1(a), \ldots, \pi_n(a)) = 0$. Therefore, $\pi_i(a) = 0$ for $i = 1, \ldots, n$. Now, $a = \sum \iota_i\pi_i(a) = \sum \iota_i(0) = 0$. So, $ker\varphi = 0$ and φ is one-to-one. Let $(a_1, \cdots, a_n) \in \prod_1^n A_i$. Let $a = \sum_1^n \iota_i(a_i)$. Now

$$\begin{aligned}
&\varphi(a) \\
&= (\pi_1(\sum_1^n \iota_i(a_i)), \ldots, \pi_n(\sum_1^n \iota_i(a_i)) \\
&= (\pi_1\iota_1(a_1), \ldots, \pi_n\iota_n(a_n)) \\
&= (a_1, \ldots, a_n)
\end{aligned}$$

Thus, φ is onto. Therefore, $A \cong \prod_1^n A_i$. □

Theorem 2.17 shows when a module is an internal direct sum of submodules.

Theorem 2.17. *If A is an R-module over a ring R and $\{A_i \mid i \in I\}$ is a collection of submodules of A, then there is an isomorphism $A \cong \sum_{i\in I} A_i$ if*

1. *The R-module A is the sum of the collection of submodules $\{A_i \mid i \in I\}$, in notation, $A =< \cup_{i\in I} A_i >$.*

2. *For each $k \in I$, $A_k \cap < \cup_{i\in I} A_i >= 0$.*

Proof. Let $A =< \cup_{i\in I} A_i >$ and $A_k \cap < \cup_{i\neq k} A_i >= 0$. For each $a \in A$, $a = \sum_1^n a_{i_k}$, $a_{i_k} \in A_{i_k}$. Define $f : A \to \sum_{i\in I} A_i$ by $f(a) = \{c_j\}_{j\in I}$ where

$$c_j = \begin{cases} a_{i_k}, & j = i_k, \exists k \\ 0, & j \notin \{i_1, \ldots, i_n\} \end{cases}$$

By property 2, f is well defined. Now $f(a+b) = \{c_j + d_j\}_{j\in I} = \{c_j\} + \{d_j\} = f(a) + f(b)$ and similarly, $f(ra) = \{rc_j\} = r\{c_j\} = rf(a)$. So, f is a preserve addition and scalar multiplication. Let $a \in ker(f)$. Then, $0 = f(a) = \{c_j\}$. So, $a = \sum 0 = 0$. Thus, $ker(f) = 0$ and f is one-to-one. Clearly, $f(a) = a_{i_1} + \cdots + a_{i_n}$, so f is onto. Therefore, f is a bijection and $A \cong \sum_{i\in I} A_i$. □

Definition 2.18. The subset $S = \{v_1, v_2, \ldots, v_n\}$ of a vector space V is said to be a *basis* of V provided that

1. S is linearly independent.

2. S spans V.

Theorem 2.19. *If $S = \{v_1, v_2, \ldots, v_n\}$ is a basis of a vector space V, then every element of V can be written as a linear combination of the vectors in S in a unique way.*

Proof. Let $v \in V$. Suppose $v = c_1v_1 + c_2v_2 + \cdots + c_nv_n$ and $v = d_1v_1 + d_2v_2 + \cdots + d_nv_n$. Now, subtracting the two equations above, we obtain $0 = (c_1 - d_1)v_1 + (c_2 - d_2)v_2 + \cdots + (c_n - d_n)v_n$. Since S is linearly independent, it follows that $(c_i - d_i) = 0$ for $1 \leq i \leq n$. So, $c_i = d_i$ and we conclude that there is only one way to express every element of V as a linear combination of the vectors in S. □

Definition 2.20. Let R be a ring and A be a module. A set of all R-module homomorphisms $A \to A$ is denoted by $Hom_R(A, A)$.

The set $Hom_R(A, A)$ will provide an example to show that, in general, the idea of dimension does not carry over to modules.

Theorem 2.21. *Let R be a ring with identity and A a free R-module with an infinite denumerable basis $\{e_1, e_2, \dots, e_n\}$. Then, $K = Hom_R(A, A)$ is a ring under the operations of pointwise addition and composition.*

Proof. To see K is a ring, we need to show that the following properties hold in K. Let f, g, $h \in K$. Then

1. $(f+g)(a+b) = (f+g)(a) + (f+g)(b) = f(a) + g(a) + f(b) + g(b) = f(a) + g(a) + f(b) + g(b) = (f+g)(a) + (f+g)(b)$. Now, $(f+g)(ra) = f(ra) + g(ra) = rf(a) + rg(a) = r(f(a) + g(a)) = r(f+g)(a)$. So, K is closed under addition.

2. $((f+g)+h)(a) = (f+g)(a) + h(a) = f(a) + g(a) + h(a) = f(a) + (g(a) + h(a)) = (f + (g+h))(a)$. Thus, associative property holds in K for addition.

3. The map $0(a) = 0$ for $a \in A$ is the additive identity of K since $(0+f)(a) = 0(a) + f(a) = f(a)$, for all $f \in K$, $a \in A$.

4. The additive inverse of f is $-f$ where $(-f)(a) = -f(a)$ for all $a \in A$.

5. For all a, $b \in A$, $f(g(a+b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b))$. Also, $f(g(ra)) = f(rg(a)) = rf(g(a))$. Hence, K is closed under multiplication.

6. Since composition of functions is associative, K is associative under multiplication.

7. The identity map I_A is the multiplicative identity for K.

8. Distributive law holds in K since $f(g(a) + h(a)) = fg(a) + fh(a)$.

Therefore, $K = Hom_R(A, A)$ is a ring. □

Chapter 3

Free Modules

In this chapter we will study the notion of free modules, including a discussion of the rank of a free module. Generally speaking, any R-module that has a basis is called a free R-module. That is, an R-module A is the free R-module on the subset B if and only if B is a basis of A. A subset B of a module A over a ring R is said to be a basis of A provided that B is linearly independent and B spans (generates) A. Let $b_n \in B$ where any $b_i \neq b_j$ and $r_i \in R$. If $\sum_{i \in I} r_i b_i = 0$ implies $r_i = 0$ for every i, then B is linearly independent. If every element $a \in A$ can be written as a linear combination of elements in B by coefficients in R, then we say B spans A. In particular, B spans A if and only if $a = r_1 b_1 + r_2 b_2 + \ldots + r_n b_n$ for all $a \in A$, $r_i \in R$, $b_i \in B$.

In Theorem 3.1, we give several characterizations of a free module. Theorem 3.5 shows every module over a division ring is free. Finally, in Theorem 3.6, we show every spanning set in a vector space contains a basis.

3.1 Characterizations of a Free Module

Theorem 3.1. *(see p. 181 [Hun80]) Let A be a module over a ring R with identity. The following conditions on R-module A are equivalent:*

1. *The R-module A has a nonempty finite basis X.*

2. *A is the internal direct sum of a finite family of cyclic R-modules. Each of the cyclic R-modules is isomorphic to R.*

3. *A is R-module isomorphic to an external direct sum of a finite number of copies of the R-module R.*

4. *There exists a nonempty set X and a function $\alpha : X \longrightarrow A$ with the following property: given any R-module B and function $\beta : X \longrightarrow B$, there exists a unique R-module homomorphism $\gamma : A \longrightarrow B$ such that $\gamma \circ \alpha = \beta$.*

Proof.

$1 \Rightarrow 2$ Let X be a nonempty basis of A and $x \in X$. Let $C_i = \{Rx_i \mid x_i \in X\}$ be a family of cyclic R-modules. Then the map $f : R \longrightarrow Rx_i$ given by $f(r) = rx_i$ is an R-module epimorphism by Theorem 2.10. If $rx_i = 0$, then $r = 0$ since X is a basis. So, f is a monomorphism and $R \cong Rx_i = C_i$. Now, we need to verify that $A = \sum_{i=1}^{n} Rx_i$ is an internal direct sum of $\{C_i\}_{i=1}^{n}$. Let $a \in A$. Then $a = \sum r_i x_i$, $r_i \in R$, $x_i \in X$. However, $r_i x_i \in C_i$, $\forall i$, so $a \in < \cup C_i >_{i \in I}$. Thus, $A =< \cup_{i=1}^{n} C_i >$. Let $x \in C_j \cap < \cup_{i \neq j} C_i >$. Then, $x = r_j x_j = \sum_{i \neq j} r_i x_i$. Hence, $r_j x_j - \sum_{i \neq j} r_i x_i = 0$. Since X is linearly independent, $r_i = 0$, $\forall i$. So $x = 0$. Thus, $C_j \cap < \cup_{i \neq j} C_i >= 0$. Therefore, A is the internal direct sum of the family C_i.

$2 \Rightarrow 3$ Let A be the internal direct sum of C_i and $C_i = Rx_i \cong R$. For each $a \in A$, $a = \sum r_i x_i$ for unique $r_1, \ldots, r_n \in R$. Define a map $g : A \rightarrow \sum Rx_i$ by $g(a) = (r_1 x_1, \ldots, r_n x_n)$. Let $a = \sum r_i x_i \in A$, $b = \sum s_i x_i \in A$ and $r \in R$. Then

$$\begin{aligned}
&g(a+b)\\
&= g(\sum s_i x_i + \sum r_i x_i)\\
&= g(\sum (s_i + r_i) x_i)\\
&= ((s_1 + r_1)x_1, \ldots, (s_n + r_n)x_n)\\
&= (s_1 x_1, \ldots, s_n x_n) + (r_1 x_1, \ldots, r_n x_n)\\
&= g(a) + g(b)
\end{aligned}$$

Similarly, $g(ra) = rg(a)$. So, g is an R=module homomorphism. If $a \in kerg$, then $g(a) = (r_1 x_1, \ldots, r_n x_n) = 0$. So, $r_i x_i = 0$ for each i. Thus, $a = 0$. So, g is one-to-one. Clearly, g is onto. Therefore, $A \cong \sum Rx_i$.

$3 \Rightarrow 1$ Let $A \cong \sum_1^n R$ and let $e_i = (0, 0, \ldots, 1_R, \ldots, 0) \in \sum_1^n R$. Clearly, $\{e_i\}_{i=1}^{n}$ is a basis for $\sum_{i=1}^{n} R$. Since $(r_1, r_2, \ldots, r_n) = \sum_1^n r_i e_i$ and $\sum_1^n r_i e_i = 0$, then $(r_1, r_2, \ldots, r_n) = 0$. So, $r_i = 0$, $\forall i$. Let $f : A \rightarrow \sum_1^n R$ be the isomorphism. Let

$X = \{f^{-1}(e_i)\}_{i=1}^{n}$ and $x_i = f^{-1}(e_i)$. Let $a \in A$. Then, $\exists a' \in \sum_1^n R$, such that $f^{-1}(a') = a$. Since $a' = \sum r_i e_i$, $a = f^{-1}(a') = \sum r_i f^{-1}(e_i) = \sum r_i x_i$. Hence, X spans A. If $\sum r_i x_i = 0$, then $\sum r_i e_i \in ker f^{-1} = \{0\}$. So, $\sum r_i e_i = 0$. Thus, $r_i = 0$, $\forall i$ and X is linearly independent. Therefore, X is a basis of A.

$1 \to 4$ Let X be a non-empty finite basis of A and let $\alpha : X \to A$ be the inclusion map. Let $X = \{x_1, \ldots, x_n\}$. If $a \in A$, then $\exists r_1, \ldots, r_n \in R$, such that $a = \sum r_i x_i$ since X spans A. Suppose we are given a map $\beta : X \to B$. Now define $\gamma : A \to B$ by $\gamma(a) = \gamma(\sum_{i=1}^n r_i x_i) = \sum_{i=1}^n r_i \beta(x_i)$. So, $\gamma \circ \alpha(x_i) = \gamma(x_i) = 1 \circ \beta(x_i) = \beta(x_i)$ for each i. To see it's uniqueness, let $\gamma' : A \to B$ be a map such that $\gamma' \circ \alpha = \beta$. Now, if $a = \sum_{i=1}^n r_i x_i \in A$. Then $\gamma'(a) = \sum_{i=1}^n r_i \gamma'(x_i) = \sum_{i=1}^n r_i \gamma' \circ \alpha(x_i) = \sum_{i=1}^n r_i \beta(x_i) = \gamma(a)$. Thus, $\gamma' = \gamma$. To see $\gamma : A \to B$ is an R-module homomorphism, we let a_1, $a_2 \in A$. Then $\exists r_i$, $s_i \in R$ such that $a_1 = \sum r_i x_i$ and $a_2 = \sum s_i x_i$.

Now, $\gamma(a_1 + a_2) = \gamma(\sum (r_i + s_i) x_i) = \sum (r_i + s_i)\beta(x_i) = \sum r_i \beta(x_i) + \sum s_i \beta(x_i) = \gamma(a_1) + \gamma(a_2)$. Let $r \in R$, then $\gamma(r a_1) = \gamma(r \sum r_i x_i) = \gamma(\sum r r_i x_i) = \sum r r_i \beta(x_i) = r \sum r_i \beta(x_i) = r\gamma(a_1)$. So, γ is an R-module homomorphism.

$4 \to 1$ Let $X = \{x_1, \ldots, x_n\}$ and consider $B = \sum_1^n R$. By the proof of $3 \to 1$, $X' = \{e_1, \ldots, e_n\}$ has the property that $\exists \alpha' : X' \to B$ (by $\alpha'(e_i) = e_i$) and, given an R-module C and a function $\beta' : X' \to C$, then $\exists \gamma' : B \to C$ such that $\gamma' \circ \alpha'(e_i) = \beta'(e_i)$, $\forall i$. See diagram (3.1):

$$\begin{tikzcd} X' \arrow[r, "\alpha'"] \arrow[dr, "\beta'"'] & B \arrow[d, "\gamma'"] \\ & C \end{tikzcd} \tag{3.1}$$

Now, define a bijection $f : X' \to X$ by $f(e_i) = x_i$ for $i = 1, \ldots, n$.

Now, $\alpha \circ f : X' \to A$. So, $\exists \gamma' : B \to A$ such that $\gamma' \circ \alpha'(e_i) = \alpha \circ f(e_i) = \alpha(x_i)$, $\forall i$. Also $\alpha' \circ f^{-1} : X \to B$ by $\alpha' \circ f^{-1}(x_i) = e_i$ for each i. So, there exists $\gamma : A \to B$ such that $\gamma \circ \alpha(x_i) = \alpha' \circ f^{-1}(x_i)$ for each i. Then the diagram (3.2) commutes:

$$\begin{tikzcd} X \arrow[r, "\alpha"] \arrow[dr, "\alpha' \circ f^{-1}"'] & A \arrow[d, "\gamma"] \\ & B \end{tikzcd} \tag{3.2}$$

Note that $\gamma \circ \gamma'(e_i) = \gamma(\alpha \circ f(e_i)) = \gamma(\alpha(x_i)) = e_i$ and $\gamma' \circ \gamma(\alpha(x_i)) = \gamma'(e_i) =$

$\alpha(x_i)$. Thus, the diagram (3.3) commutes:

$$\begin{tikzcd}
X' \arrow[r, "\alpha'"] \arrow[d, "f"'] & B \arrow[d, "\gamma\circ\gamma'"] \\
X \arrow[r, "\gamma\circ\alpha"'] & B'
\end{tikzcd} \tag{3.3}$$

Now, given an identity map $I_B : B \to B'$ with $I_B(e_i) = e_i$ and $\gamma \circ \gamma'(e_i) = e_i$. So, by uniqueness, $\gamma \circ \gamma' = I_B$. Similarly, $\gamma' \circ \gamma = I_A$. Then, $A \cong B$ and, by $3 \to 1$, $\alpha(X)$ is a basis of B. □

An R-module A that satisfies the equivalent conditions of the Theorem above is called a free R-module.

Corollary 3.2. *Let R be a ring with identity. Then, every finitely generated R-module A is the homomorphic image of a free R-module F.*

Proof: Let $X = \{a_1, \ldots, a_n\}$ be a set of generators of A and F the free R-module on the set X. Let $\alpha : X \to F$ and define $\gamma : X \to A$ by $\gamma(a_i) = a_i$ for each i. Then, there exists a unique $\beta : F \to A$ such that $\beta\alpha(x) = \gamma(x)$ by Theorem 3.1. Now $Im(\beta) =< \beta(\alpha(X)) >=< \gamma(X) >= A$. So, β is onto. □

Lemma 3.3. *Let V be a vector space over a field F. Then X is a basis of V if X is a maximal linearly independent subset of V.*

Proof. Let $X = \{x_1, \ldots, x_n\}$ be a maximal linearly independent subset of V. Let S be the subspace of V spanned by the set X. Since X is linearly independent and spans S, X is a basis of S. If $S = V$, we are done. If $S \neq V$, then there exists an element $x \in V$ with $x \neq S$. Consider $X \cup \{x\}$. If $r \neq 0$, then $rx + r_1x_1 + \cdots + r_nx_n = 0$ can be written as $x = -r^{-1}r_1x_1 - \cdots - r^{-1}r_nx_n$, which shows that $x \in V$. It is contradicts to the choice of x. So, $r = 0$. Then, $r_i = 0$ for all i since X is linearly independent. It follows that the set $X \cup \{x\}$ is a linearly independent subset of V. It contradicts to the fact that X is a maximal subset of V. Therefore, $S = V$ and X is a basis of V. □

3.2 Free Module over a Division Ring

Our next theorem shows that every vector space has a basis. To handle infinite basis we need Zorm's Lemma.

Definition 3.4. A non-empty set A and a relation $\leq$ is said to be *partially ordered* if for each a, b, $c \in A$

1. $a \leq a$
2. If $a \leq b$ and $b \leq c$ then $a \leq c$
3. If $a \leq b$ and $b \leq a$ then $a = b$.

   We say $(A, \leq)$ is linearly ordered if, in addition,

4. for each a, $b \in A$, $a \leq b$ or $b \leq a$

Definition 3.5. Let $(A, \leq)$ be a partially ordered set and $a \in A$. If every $c \in A$ which is comparable to a is such that $c \leq a$, then a is maximal in A. An upper bound of a nonempty subset B of A is an element $d \in A$ such that $b \leq d$ for every $b \in B$. A nonempty subset B of A that is linearly ordered by $\leq$ is called a *chain* in A.

Lemma 3.6. *(Zorn's Lemma) Let A be a nonempty partially ordered set. If every chain in A has an upper bound in A, then A contains a maximal element.*

Theorem 3.7. *Every linearly independent subset X of a vector space V is contained in a basis of V. In particular, every vector space V has a basis.*

Proof. Since $\emptyset$ is linearly independent and is contained in every vector space, the second statement is an immediate consequence of the first. Let $S = \{Y \mid Y \subseteq V$, Y is linearly independent, $Y \supseteq X\}$ be the set of all linearly independent subsets of V containing X. Since $X \in S$, $S \neq \emptyset$. Now let $\{C_i\}_{i \in I}$ be a chain in S and let $C = \cup_{i \in I} C_i$. We will show $C \in S$. Let $x_1, \ldots, x_t \in C$ with $x_j \in C_{i_j}$. Suppose $\sum r_i x_i = 0$, $r_i \in R$. Let N be such that $x_1, \ldots, x_t \in C_N$. So, since C_N is linearly independent, $r_i = 0$, $\forall i$. Then, C is linearly independent and $C \in S$. Thus C is an upper bound for the chain $\{C_i\}_{i \in I}$ in S. By Zorn's Lemma, there exists a maximal element $B \in S$. Now B is a maximal linearly independent subset of V. By Lemma 3.3 B is a basis of V. □

Our final result in this section shows every spanning set in a vector space contains a basis.

Theorem 3.8. *Let X be a subset of a vector space V over a division ring D. If X spans V, then X contains a basis of V.*

Proof. Let X be a subset of V that spans V. If X is linearly independent, then X is a basis of V. If X is linearly dependent, then $\sum r_i x_i = 0$, where $r_i's$ are not all 0. By Theorem 2.3, some $x_j = r_1 x_1 + \cdots + r_{j-1} x_{j-1}$. Let $X_1 \subset X$, where $x_j \notin X_1$. Then, $X_1 = \{x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_t\}$ spans V. If X_1 is linearly independent, then $X_1 \in X$ is a basis of V. If X_1 is linearly dependent, then we delete one element $x_k \in X_1$ and get a new set X_2 that also spans V. Continuing this process, we will find a subset $X_l \in X$ that is linearly independent and spans V. Then, X_l is a basis of V. □

Chapter 4

Cardinality

In Chapter 5 we will show that if a module has an infinite basis, then all basis are infinite of the same cardinality. To do this, we need some results on cardinal numbers. We begin by defining a cardinal number of a set as its equivalence class under equipollence. We then introduce an order on cardinal numbers and show $|A| \leq |B|$ and $|B| \leq |A|$ implies $|A| = |B|$. We conclude with a theorem on the arithmetic properties of cardinal numbers.

4.1 Cardinal Number

Definition 4.1. Let A, B be two sets. If there exists a bijective map $f : A \rightarrow B$, then we say A and B are *equipollent*. We use $A \sim B$ to denote that A and B are equipollent.

Theorem 4.2. *Given a class C of sets, equipollence is an equivalence relation on C.*

Definition 4.3. The *cardinal number* (or *cardinality)* of a set A is the representative of an equivalence class of the set A under the equivalence relation of equipollence, denoted $|A|$.

If a set A is finite, then $|A|$ is finite; A is infinite, $|A|$ is infinite. Precisely, the cardinal number of a finite set is the number of elements in the set. Cardinal numbers possess the following properties:

1. The cardinal number of every set is unique.

2. Two sets A and B are said to have the same cardinal number provided that they are equipollent, written $|A| = |B| \Leftrightarrow A \sim B$.

3. The cardinal number of a finite set is the number of elements in the set.

We can also use lower case Greek letters such as α, β, γ, etc to denote cardinal numbers.

Definition 4.4. Let A, B be disjoint sets, where $|A| = \alpha$ and $|B| = \beta$. Then the sum $\alpha + \beta$ is defined to be the cardinal number $|A \cup B|$; the product $\alpha\beta$ is defined to be the cardinal number $|A \times B|$.

Definition 4.5. Let A, B be sets and α, β be cardinal numbers, such that $|A| = \alpha$ and $|B| = \beta$. If $B \subset A$ and $A \sim B$ (that is, there is a one-to-one map $A \to B$), then we say α is less than or equal to β, denoted $\alpha \leq \beta$ or $\beta \geq \alpha$. Moreover, if $\alpha \leq \beta$ and $\alpha \neq \beta$, then we say α is strictly less than β and denoted $\alpha < \beta$.

4.2 Order of Cardinal Number

The next theorem shows that if α, β are cardinal numbers with $\alpha \leq \beta$ and $\beta \leq \alpha$, then $\alpha = \beta$.

Theorem 4.6. *(Schroeder-Bernstein) Let A and B be sets. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. This means that if there are injective functions, say, $f : A \to B$ and $g : B \to A$ between the sets A and B, then there exists a bijective function $h : A \to B$.*

Proof. We first consider the case where $B \subset A$. Let

$$\begin{aligned} B' &= (A - B) \cup f(A - B) \cup f^2(A - B) \cup f^3(A - B) \cup \ldots \\ B^+ &= f(A - B) \cup f^2(A - B) \cup f^3(A - B) \cup f^4(A - B) \cup \ldots \\ C &= B - B^+ \end{aligned}$$

We know that $A = (A - B) \cup B = (A - B) \cup B^+ \cup C = B' \cup C$ and $B = B^+ \cup C$. Therefore, $f(B') = f((A - B) \cup B^+) \subseteq f(A - B) \cup f(B^+) \subseteq B^+$. Now, define a function $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in B' \\ x & \text{if } x \in C \end{cases}$$

Since $C \cap B' = \emptyset$, h is well-defined. Note that $h(B') = f(B') \subseteq B^+$ and $h(C) = C$. To see h is one-to-one, let $h(x) = h(y)$ where $x, y \in A$. If $x \in C$, then $h(y) = h(x) = x \in C$. Thus, $y \in C$ and $h(y) = y$. Hence, $x = y$. Similarly, if $y \in C$, then $x \in C$ and $x = y$. If $x, y \in B'$, then $f(x) = f(y)$. Thus, $x = y$. So, we have proven that h is an injective (one-to-one) function. To see h is onto, let $y \in B = B^+ \cup C$. If $y \in C$, then $h(y) = y$. If $y \in B^+ = \cup_{n=1}^{\infty} f^{(n)}(A - B)$, then $y \in f^n(A - B)$ for some $n > 0$. Thus, $y = f(x)$ where $x \in f^{(n-1)}(A - B)$. Therefore, h is a surjection (onto). Since h is one-to-one and onto, we conclude that h is a bijection. Therefore, if $f : A \to B$ and $g : B \to A$ are injective functions with $B \subseteq A$, then there exists a bijection $h : A \to B$.

In the general case, we have an injective function $f : A \to B$ and an injective function $g : B \to g(B) \subseteq A$. By the above argument, there exists a bijection $h : A \to g(B)$. Now, since $g : B \to g(B)$ is a bijection, $g^{-1} : g(B) \to B$ is also a bijection. Hence, $g^{-1} \circ h : A \to B$ is a bijection. Thus, $|A| = |B|$. □

Example 4.7. Let $A = \mathbf{Z}$, $B = 2\mathbf{Z} \subseteq \mathbf{Z}$. Then, the set $(A - B) = \{1, 3, 5, 7, 9, 11, \ldots\} = \{2n + 1 \mid n \geq 0\}$. Define a function $f : \mathbf{Z} \to 2\mathbf{Z}$ by $f(n) = 4n$. Then, $f(A - B) = \{4(2n + 1) \mid n \geq 0\} = \{4, 12, 20, 28, \ldots\}$, $f^2(A - B) = \{16(2n + 1) \mid n \geq 0\} = \{16, 48, 80, \ldots\}$ and so on. Thus, $B^+ = f(A - B) \cup f^2(A - B) \cup \ldots = \{2^k n \mid n, k \in \mathbf{N}, n$ is odd, k is even $\}$ and $C = (B - B^+) = \{2^k n \mid n, k \in \mathbf{N}, n$ is odd, k is odd $\}$. The function $h : A \to B$ defined by

$$h(x) = \begin{cases} f(x) & \text{if } x \in B' \\ x & \text{if } x \in C \end{cases}$$

sends x in B' to $4x$ and x outside B' to x. The following diagram shows the preimages of the first 10 elements of $B = 2\mathbf{Z}$.

n	2	4	6	8	10	12	14	16	18	20
$h^{-1}(n)$	2	1	6	8	10	3	14	4	18	5

The cardinal number of the natural numbers $\mathbf{N}$ is denoted $\aleph_0$. Any set A is said to have a cardinality $\aleph_0$ provided that it is equipollent to $\mathbf{N}$.

Theorem 4.8. *Let α, β be cardinal numbers where $\alpha \geq \beta \neq 0$ and α is infinite. Then, $\alpha\beta = \alpha$. Particularly, $\alpha\aleph_0 = \alpha$ and $\aleph_0\beta = \aleph_0$ if β is finite.*

Corollary 4.9. *If $F(S)$ is the set of all finite subsets of an infinite set S, then $|F(S)| = |S|$.*

Chapter 5

Free Modules Over An Arbitrary Ring

Recall that, the property of any two bases of a free module having same cardinality is based on a "well-behaved" ring such as a division ring or a field. In this chapter, let us consider the more complicated situation of a free module over an arbitrary ring. Theorem 5.6 shows that if a module has a basis of infinite cardinality, then all basis have the same cardinality. Proposition 5.8 shows that there exist modules having finite basis of different cardinalities. Thus, the idea of dimension cannot be extended to modules in general.

5.1 Modules with Infinite Bases

Definition 5.1. Given R-modules M_1, M_2, ... , M_n. Define a new module $M = M_1 \oplus M_2 \oplus ... \oplus M_n$ with the elements $(m_1, m_2, ..., m_n)$, where $m_i \in M_i$. Addition and scalar multiplication are defined as follows:

$$(m_1, m_2, \ldots, m_n) + (p_1, p_2, \ldots, p_n) = (m_1 + p_1, m_2 + p_2, ..., m_n + p_n),$$
$$r(m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n).$$

Then M is called the *external direct sum* of the R-modules M_i, $1 \leq i \leq n$.

The next proposition shows when an internal sum of modules is direct.

Proposition 5.2. *Let $M_1, M_2, \ldots, M_n$ be submodules of an R-module M such that for each i, $1 \leq i \leq n$, we have $M_i \cap (M_1 + M_2 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_n) = 0$. Let $N = M_1 + M_2 + \ldots + M_n$. Then, $N \cong M_1 \oplus \ldots \oplus M_n$.*

Proof. We define $f : M_1 \oplus M_2 \oplus \ldots \oplus M_n \to N$ by $f((m_1, m_2, \ldots, m_n)) = m_1 + m_2 + \ldots + m_n$. Let $(m_1, m_2, \ldots, m_n)$, $(p_1, p_2, \ldots, p_n) \in M_1 \oplus M_2 \oplus \ldots \oplus M_n$. Then

$$\begin{aligned}
&f((m_1, m_2, \ldots, m_n) + (p_1, p_2, \ldots, p_n)) \\
&= f((m_1 + p_1, m_2 + p_2, \ldots, m_n + p_n)) \\
&= (m_1 + p_1) + (m_2 + p_2) + \ldots + (m_n + p_n) \\
&= (m_1 + m_2 + \ldots + m_n) + (p_1 + p_2 + \ldots + p_n) \\
&= f((m_1, m_2, \ldots, m_n)) + f((p_1, p_2, \ldots, p_n))
\end{aligned}$$

Let $r \in R$, then $f(r(m_1, m_2, \ldots, m_n)) = f((rm_1, rm_2, \ldots, rm_n)) = rm_1 + rm_2 + \ldots + rm_n = r(m_1 + m_2 + \ldots + m_n) = rf((m_1, m_2, \ldots, m_n))$. So, f is a linear transformation. To see f is one-to-one, let $m = (m_1, m_2, \ldots, m_n) \in ker(f)$. Then $f(m) = m_1 + m_2 + \ldots + m_n = 0$. For each i, $m_i = -\sum_{j \neq i} m_j$, so $m_i \in M_i \cap (M_1 + M_2 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_n) = 0$. Thus, $m = 0$. Hence, $ker(f) = \{0\}$ and f is one-to-one. Clearly, $f((m_1, m_2, \ldots, m_n)) = m_1 + m_2 + \ldots + m_n$, so f is onto. Therefore, f is a bijection and $N \cong M_1 \oplus \ldots \oplus M_n$. □

If V is a vector space of dimension n over a field K, then $V \cong K^n$. The next result shows this holds for modules with a finite basis.

Lemma 5.3. *Let M be an R-module with a basis of n elements. Then $M \cong R^n \cong R \oplus R \oplus \ldots \oplus R$.*

Proof. Let $X = \{x_1, x_2, ..., x_n\}$ be a finite basis of M and $a \in M$. Then $a = r_1x_1 + r_2x_2 + ... + r_nx_n$, $r_i \in R$. The map $f : M \to R^n$ given by $f(\sum_{i=1}^n r_ix_i) = (r_1, r_2, ..., r_n)$ is well-defined since the coefficients r_i are uniquely determined by x. Further f is a module homomorphism since $f(\sum_{i=1}^n r_ix_i + \sum_{i=1}^n s_ix_i) = f(\sum_{i=1}^n (r_i + s_i)x_i) = (r_1 + s_1, r_2 + s_2, ..., r_n + s_n) = (r_1, r_2, ..., r_n) + (s_1, s_2, ..., s_n) = f(\sum_{i=1}^n r_ix_i) + f(\sum_{i=1}^n s_ix_i)$ and $f(\sum_{i=1}^n rr_ix_i) = (rr_1, rr_2, ..., rr_n) = r(r_1, r_2, ..., r_n) = rf(\sum_{i=1}^n r_ix_i)$. If $b = \sum_{i=1}^n c_ix_i \in kerf$, then $f(b) = f(\sum_{i=1}^n c_ix_i) = (c_1, c_2, ..., c_n) = (0, 0, ..., 0)$. Thus, $c_i = 0, \forall i$. Therefore, $kerf = \{0\}$. So, f is one-to-one. For $(r_1, r_2, \ldots, r_n) \in R$, $f(\sum_{i=1}^n r_ix_i) = (r_1, r_2, ..., r_n)$, so f is onto. Thus, f is a bijection and we conclude that $M \cong R^n \cong R \oplus R \oplus \ldots \oplus R$. □

Definition 5.4. Let X be a subset of an R-module A. Let $\{B_i | i \in I\}$ be the family of all submodules of A containing X. Then, $\cap_{i \in I} B_i$ is called *the submodule of A generated by the set X* and denoted $< X >$.

The following lemma shows that if a module has a basis of infinite cardinality, then all other bases have infinite cardinality.

Lemma 5.5. *Let F be a free R-module with an infinite basis X. If $Y \subseteq F$ spans F, then Y is also infinite.*

Proof. Suppose $Y = \{y_1, y_2, \ldots, y_n\}$ is finite. Then, for each i, $y_i = \sum_{j=1}^{m_j} r_j x_{i,j}$, where $x_{i,j} \in X$, for all i, j. Let $X_1 = \{x_{11}, \ldots, x_{nm_n}\}$. Then, $F \subseteq < Y > \subseteq < X_1 >$. Now, there exists $x \in X - X_1$ with $x \in < X_1 >$, contradicting the linear independence of X. Thus, Y is infinite. □

In the next theorem, we will strengthen the lemma above to show that if a module has a basis of infinite cardinality, then all other basis have the same cardinality.

Theorem 5.6. *If F is a free R-module over a ring R with identity and X is an infinite basis of F. Then, all of the bases of F has the same cardinality.*

Proof. If Y is another basis of F, then Y is infinite by Lemma 5.5.

Let $K(Y)$ be the set of all finite subsets of Y. Define $f : X \rightarrow K(Y)$ by $f(x) = \{y_1, y_2, \ldots, y_n\}$ where $x = \sum_1^n r_i y_i$. Since Y is a basis, f is well defined. Since $F \subseteq < X > \subseteq < Imf >$, Imf must be infinite by Lemma 5.5.

Next we show for all $T \in Im(f)$, $|f^{-1}(T)| < \infty$. If $x \in f^{-1}(T)$, then $x \in < T >$. So $f^{-1}(T) \subseteq < T >$. Let $T = \{y_1, y_2, \ldots, y_n\}$. For each i, $y_i \in < X_i >$ where $X_i \subseteq X$ is finite. Let $X_T = \cup_{i=1}^n X_i$. Now $f^{-1}(T) \subseteq < T > \subseteq < X_T > \cap X = X_T$. Since X_T is finite, $f^{-1}(T)$ is also finite.

For each $T \in Imf$, let $x_1, x_2, \cdots, x_n$ be the elements of $f^{-1}(T)$, and define an injective map $g_T : f^{-1}(T) \rightarrow Imf \times \mathbf{N}$ by $g_T(x_k) = (T, k)$. Since the sets $f^{-1}(T)$ form a partition of X, the map $X \rightarrow Imf \times \mathbf{N}$ defined by $g(x) = g_T(x)$ is well-defined. To see the function $g : X \rightarrow Imf \times \mathbf{N}$ is an injection, let $x, y \in X$ with $g(x) = g(y) = (T, k)$. Then, if $f^{-1}(T) = \{x_1, x_2, \ldots, x_n\}$, $x = y = x_k \in f^{-1}(T)$. Therefore, g is one-to-one. Hence, $|X| \leq |Imf \times \mathbf{N}|$. From Theorem 4.8 and Corollary 4.9, it follows that $|X| \leq |Imf \times \mathbf{N}| = |Imf| \aleph_0 = |Imf| \leq |K(Y)| = |Y|$. Similarly, we will have the result that $|Y| \leq |X|$. Therefore, we conclude $|X| = |Y|$ by the Schroeder-Bernstein Theorem. □

For vector spaces, Theorem 5.6 is true for basis of finite cardinality.

5.2 Modules with Finite Bases

Theorem 5.7. *If X and Y are both bases of a vector space V over a field D, then $|X| = |Y|$.*

Proof. If X is infinite, then Y is also infinite and $|X| = |Y|$ by Lemma 5.5 and Theorem 5.6. Suppose $X = \{x_1, x_2, \cdots, x_m\}$ and $Y = \{y_1, y_2, \cdots, y_n\}$ are finite with $m < n$. Since X and Y are bases, $0 \neq y_1 = r_1x_1 + r_2x_2 + \cdots + r_mx_m$ for some $r_i \in D$. Clearly, not all r_i's are 0, say r_1 is the first nonzero. Thus, $x_1 = r_1^{-1}y_1 - r_1^{-1}r_2x_2 - \cdots - r_1^{-1}r_mx_m$ and the set $X' = \{y_1, x_2, x_3, \ldots, x_m\}$ spans V because X spans V.

Now, consider the set $\{y_1, y_2, x_2, \ldots, x_m\}$. This time, let y_2 be the linear combination of $y_1, x_2, \ldots, x_m$, say, $y_2 = s_1y_1 + t_2x_2 + \cdots + t_mx_m$, where s_j, $t_k \in D$. Then, at least one of $t_2, \cdots, t_m$ is nonzero, for otherwise it will contradict the linear independence of the y_n's. If $t_2 \neq 0$, then $y_1, y_2, x_3, \cdots, x_m$ spans V since X' spans V. Repeating in this fashion, at the end we will see a set $\{y_1, y_2, y_3, \cdots, y_m\}$ that spans V. But then y_{m+1} is a linear combination of $y_1, y_2, \cdots, y_m$, which contradicts the linear independence of Y. Therefore, we must have $|Y| \leq |X|$. Similarly, we can show that $|X| \leq |Y|$ by reversing the roles of X and Y. Hence, $|X| = |Y|$. □

The common cardinality of the bases of a vector space is called the dimension of the vector space. The following two results show that such a notion is not possible for modules in general. Proposition 5.8 illustrates the technique of Theorem 5.9 by considering a few special cases.

Proposition 5.8. *Let K be a field and let V be a vector space with an infinite basis $\{e_1, e_2, e_3, \ldots\}$. Let $R = Hom_K(V, V)$, which is the set of all K-module homomorphisms $V \to V$. Then*

1. *$R \cong R$.*

2. *$R \cong R \oplus R$.*

3. $R \cong R \oplus R \oplus R$.

Proof.

1. $R \cong R$: Assume $B_1 = \{I_V\}$, where I_V is the identity element of R. In order to show that B_1 is a basis of R, we need to check that B_1 is linearly independent and B_1 spans R.

   B_1 is linearly independent: Let $a \in R$. If $aI_V = 0$ implies $a = 0$, then B_1 is linearly independent. Now, if $aI_V = 0$, then

   $$\begin{aligned} & aI_V(e_i) = 0(e_i) \quad \forall i. \\ & a(e_i) = 0(e_i) \quad \forall i \quad \text{(since } I_V \text{ is an identity element).} \\ & a(e_i) = 0 \quad \forall i \\ & a = 0 \quad \text{(since } \{e_i\}_{i=1}^{\infty} \text{ is a basis).} \end{aligned}$$

   Thus, B_1 is linearly independent.

   B_1 spans R: If every element of R can be written as a linear combination of B_1 over R, then B_1 spans R. Let $f \in R = Hom_K(V, V)$, then $f = f \cdot I_V$ since $f(x) = (f \cdot I_V)(x), \forall x \in V$. We conclude that B_1 spans R.

   Since B_1 is linearly independent and spans R, B_1 is a one-element basis of R. Thus, $R = Hom_K(V, V) \cong R$ is an R-module by Lemma 5.3.

2. $R \cong R \oplus R$: Define $f_1, f_2 \in R$ by

   $$f_1(e_n) = \begin{cases} e_{\frac{n+1}{2}} & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases}$$

   $$f_2(e_n) = \begin{cases} e_{\frac{n}{2}} & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

   We claim $B_2 = \{f_1, f_2\}$ is a two-element basis of R. If

   $$a_1 f_1 + a_2 f_2 = 0 \tag{5.1}$$

   then, for each $n \geq 1$,

   $$a_1 f_1(e_n) + a_2 f_2(e_n) = 0(e_n) \tag{5.2}$$

When n is odd, Equation (5.2) will be simplified to

$$\begin{aligned}
&a_1 f_1(e_n) = 0(e_n) \quad (\text{since } a_2 f_2(e_n) = 0)\\
&a_1 f_1(e_n) = 0\\
&a_1(e_{\frac{n+1}{2}}) = 0 \quad (\text{by definition } f_1(e_n) = e_{\frac{n+1}{2}})\\
&a_1 = 0, \quad \text{since } \{e_i\}_{i=1}^{\infty} \text{ is a basis}
\end{aligned}$$

Similarly, when n is even, we will get $a_2 = 0$. Therefore, B_2 is linearly independent. Now let $g \in R$ and define $g_1, g_2 \in R$ by $g_1(e_i) = g(e_{2i-1})$ and $g_2(e_i) = g(e_{2i})$ for each i. We will show $g = g_1 f_1 + g_2 f_2$. When n is odd, $(g_1 f_1 + g_2 f_2)(e_n) = g_1 f_1(e_n) = g_1(e_{\frac{n+1}{2}}) = g(e_{2(\frac{n+1}{2})-1}) = g(e_n)$. Similarly, when n is even, $(g_1 f_1 + g_2 f_2)(e_n) = g_2 f_2(e_n) = g(e_{2(\frac{n}{2})}) = g(e_n)$. Thus, $g = g_1 f_1 + g_2 f_2$ and B_2 spans R. We conclude that B_2 is a two-element basis of R and, by Lemma 5.3, $R \cong R \oplus R$.

3. $R \cong R \oplus R \oplus R$: Define $f_1, f_2, f_3 \in R$ by

$$f_1(e_q) = \begin{cases} e_{k+1} & \text{if } q = 3k+1, k \in Z \\ 0 & \text{if } q \not\equiv 1 \bmod 3 \end{cases}$$

$$f_1(e_q) = \begin{cases} e_{k+1} & \text{if } q = 3k+2, k \in Z \\ 0 & \text{if } q \not\equiv 2 \bmod 3 \end{cases}$$

$$f_1(e_q) = \begin{cases} e_{k+1} & \text{if } q = 3k+3, k \in Z \\ 0 & \text{if } q \not\equiv 0 \bmod 3 \end{cases}$$

We claim $B_3 = \{f_1, f_2, f_3\}$ is a three-element basis of $R = Hom_k(V, V)$. If

$$a_1 f_1 + a_2 f_2 + a_3 f_3 = 0 \tag{5.3}$$

Then, for each $q \geq 1$,

$$a_1 f_1(e_q) + a_2 f_2(e_q) + a_3 f_3(e_q) = 0(e_q) \tag{5.4}$$

When $q = 1, a_2 f_2(e_q) = a_3 f_3(e_q) = 0$ and Equation(5.4) above will become

$$\begin{aligned} a_1 f_1(e_1) &= 0(e_1) \\ a_1 f_1(e_1) &= 0 \\ a_1(e_2) &= 0 \\ a_1 &= 0 \quad \text{since } \{e_i\}_{i=1}^{\infty} \text{ is a basis} \end{aligned}$$

Similarly, when $q = 2$, we will have $a_2 = 0$; when $q = 3$, we will have $a_3 = 0$. Therefore, B_3 is linearly independent.

Let $g \in R$ and define $g_1, g_2, g_3 \in R$ by

$$g_1(e_i) = g(e_{3i-2}) \tag{5.5}$$

$$g_2(e_i) = g(e_{3i-1}) \tag{5.6}$$

$$g_3(e_i) = (e_{3i}) \tag{5.7}$$

for each $i \geq 1$. We will show $g = g_1 f_1 + g_2 f_2 + g_3 f_3$. Let $q \geq 1$. In the case of $q = 3k + 1$, for some $k \in N, g_2 f_2(e_q) = g_3 f_3(e_q) = 0$, then

$$\begin{aligned} & g_1 f_1(e_q) + g_2 f_2(e_q) + g_3 f_3(e_q) \\ &= g_1 f_1(e_q) \\ &= g_1(e_{k+1}) \\ &= g(e_{3(k+1)-2}) \\ &= g(e_{3k+1}) \\ &= g(e_q) \end{aligned}$$

Similarly, when $q = 3k + 2$ and $q = 3k + 3$, we will also get the result that $(g_1 f_1 + g_2 f_2 + g_3 f_3)(e_q) = g(e_q)$. Therefore, $g = g_1 f_1 + g_2 f_2 + g_3 f_3$ and B_3 spans R. Therefore, B_3 is a basis of R with three elements. By Lemma 5.3, $R \cong R \oplus R \oplus R$.

□

In Proposition 5.8, we proved several special cases to illustrate the ideas of the proof of Theorem 5.9. We now prove our main result.

Theorem 5.9. *Let K be a field and V a vector space with an infinite denumerable basis $\{e_1, e_2, e_3, ...\}$. If n is any positive number, then $R = Hom_K(V, V)$ has a basis of n elements. In particular, $R \cong R^n$ for each $n \in \mathbb{N}$.*

Proof. We will show $R \cong R^n = R \oplus R \oplus \cdots \oplus R$ as R-modules. Let $q \in N$. Define $f_1, f_2, \ldots, f_n \in R$ by

$$f_1(e_q) = \begin{cases} e_{k+1} & \text{if } q = nk+1 \\ 0 & \text{if } q \not\equiv 1 \bmod n \end{cases}$$

$$f_2(e_q) = \begin{cases} e_{k+1} & \text{if } q = nk+2 \\ 0 & \text{if } q \not\equiv 2 \bmod n \end{cases}$$

$$\vdots$$

$$f_i(e_q) = \begin{cases} e_{k+1} & \text{if } q = nk+i \\ 0 & \text{if } q \not\equiv i \bmod n \end{cases}$$

$$\vdots$$

$$f_n(e_q) = \begin{cases} e_{k+1} & \text{if } q = nk+n \\ 0 & \text{if } q \not\equiv 0 \bmod n \end{cases}$$

We claim $B_n = \{f_1, f_2, \ldots, f_i, \ldots, f_n\}$ is an n-element basis of R. If $a_1 f_1 + a_2 f_2 + \cdots + a_i f_i + \cdots + a_n f_n = 0$ and $q \equiv i \bmod n$. Let $q = nk + i$ for $k \geq 0$, $1 \leq i \leq n$. Then

$$a_1 f_1(e_q) + a_2 f_2(e_q) + \cdots + a_i f_i(e_q) + \cdots + a_n f_n(e_q) = 0(e_q) \tag{5.8}$$

Since $f_j(e_q) = 0$ for $j \neq i$, Equation (5.8) above will become

$$\begin{aligned} & a_i f_i(e_q) = 0 \\ & a_i(e_{\frac{q-i}{3}+1}) = 0 \\ & a_i(e_{k+1}) = 0 \quad \text{for all } k \geq 0 \\ & a_i = 0 \quad \text{since } \{e_j\}_{j=1}^{\infty} \text{ is a basis.} \end{aligned}$$

Thus, when $q = nk + i$, we will have $a_i = 0$, $1 \leq i \leq n$. Therefore, B_n is linearly independent.

Let $g \in R$. Define $g_1, g_2, \dots, g_n \in R$ by

$$\begin{aligned} g_1(e_j) =& g(e_{nj-(n-1)}) \\ g_2(e_j) =& g(e_{nj-(n-2)}) \\ &\vdots \\ g_i(e_j) =& g(e_{nj-(n-i)}) \\ &\vdots \\ g_n(e_j) =& g(e_{nj}) \end{aligned}$$

. for each $j \geq 1$. We will show $g = g_1 f_1 + g_2 f_2 + ... + g_i f_i + ... + g_n f_n$. When $q = nk + 1$, for some $k \in N, g_2 f_2(e_q) = g_3 f_3(e_q) = \cdots = g_i f_i = \cdots = g_n f_n = 0$, then

$$\begin{aligned} &(g_1 f_1 + g_2 f_2 + \cdots + g_i f_i + \cdots + g_n f_n)(e_q) \\ &= g_1 f_1(e_q) \\ &= g_1 f_1(e_{nk+1}) \\ &= g_1(e_{k+1}) \\ &= g(e_{n(k+1)-(n-1)}) \\ &= g(e_{nk+n-n+1)}) \\ &= g(e_{nk+1}) \\ &= g(e_q) \end{aligned}$$

Now, when $q = nk + i, k, i \in N$ with $1 \leq i \leq n$, we have $(g_1 f_1 + g_2 f_2 + ... + g_i f_i + ... + g_n f_n)(e_q) = g_i f_i(e_q) = g_i f_i(e_{nk+i}) = g_i(e_{k+1}) = g(e_{n(k+1)-(n-i)}) = g(e_{nk+n-n+i}) = g(e_{nk+i}) = g(e_q)$. Hence, $g = \sum_1^n f_i g_i$ and B_n spans R. Therefore, B_n is an n-element basis of $R = Hom_k(V, V)$. By Lemma 5.3, $R \cong R^n \cong R \oplus R \oplus R \oplus \dots \oplus R$. □

Bibliography

[Gal02] Joseph A. Gallian. *Contemporary Abstract Algebra.* Houghton Mifflin Company, Boston, 2002.

[Hun80] Thomas W. Hungerford. *Algebra,* volume 73 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[KH01] B. Kolman and David R. Hill. *Introductory Linear Algebra with Applications.* Prentice Hall, New Jersey, 2001.

[OR96] J. J. O'Connor and E. F. Robertson. Abstract linear spaces, 1996. Online; accessed 8-June-2007.

[RA77] C. Rorres and H. Anton. *Applications of Linear Algebra.* John Wiley and Sons, Inc., New York, 1977.