JIMMY BROOMFIELD

MODULES OVER A PRINCIPAL IDEAL DOMAIN

THE UNIVERSITY OF MINNESOTA
Contents

Introduction 5

Basics of Module Theory 7
  Linear Algebra Review 7
  Endomorphisms and Cayley’s Theorem 9
  Fundamental Concepts 10
  Free Modules 13

The Structure of Modules 15

Bibliography 17

Index 19
Introduction

The theory of modules is a rich subject that is very much a generalization of abelian groups.

To begin this discussion, let us give a definition of a module.

**Definition 1.0.1.** Let R be a ring. A **left R-module** is an abelian group, $(M, +, 0)$, together with a function $\eta : R \times M \rightarrow M$ denoted $\eta(r, a) = ra$, such that for all $r, s \in R$ and $a, b \in M$:

1. $r(a + b) = ra + rb$.
2. $(r + s)a = ra + sa$
3. $r(sa) = (rs)(a)$
4. $1_R a = a$ for all $a \in M$

*Note that if R is a division ring, then M is called a left vector space.*

A right R-module can be defined in a similar way, however unless otherwise noted, we will take the term module to mean left module.

Before seeing a few examples of modules, we will work through some basic properties.

**Proposition 1.0.2.** Let M be an R-module, $0_R$ be the additive identity in R, $0_M$ be the additive identity in M, and $-(\cdot)$ represent the additive inverse of an element. Then to following hold.

1. $r0_M = 0_M$ for all $r \in R$.
2. $0_R m = 0_M$ for all $m \in M$.
3. $(−r)m = -(rm) = r(−m)$ for all $r \in R$ and $m \in M$.
4. $n(rm) = r(nm)$ if R is a commutative ring.

Now let us consider some examples of modules that will play important roles later.

**Example 1.0.3.** **Z-modules:** Every additive abelian group G is a Z-module under the map $(n, a) \mapsto na$ where $n \in \mathbb{Z}$, and $a \in G$. 

See Jacobson’s "Basic Algebra I" pages 157 and 158 for more of the history of this development.
Example 1.0.4. **Subring modules**: If $S$ is a subring of $R$, then $R$ is an $S$-module with $\eta$ being multiplication in $R$, i.e. $(s, r) \mapsto sr$.*

Example 1.0.5. **Translation modules**: If $R$ is a ring, then define $R_L$ is the set of all maps of the form $a_L : x \mapsto ax$, where $a \in R$. If we let $M = (R, +, 0)$, then $R_L$ is an

Example 1.0.6. **Ideal modules**: If $I$ is a left ideal of a ring $R$, then $I$ is a left $R$-module with $ra$ being the ordinary product in $R$. Further $I$ is an additive subgroup of $R$, therefore $R/I$ is an abelian group (with respect to addition). Hence $R/I$ is an $R$-module with multiplication given by $r(r_1 + I) = rr_1 + I$.*

Example 1.0.7. **Annihilating modules**: If $M$ is an $R$-module, $I$ is a 2-sided ideal of $R$, and $am = 0$ for all $a \in I, m \in M$, then we say that $I$ annihilates $M$. If this is the case, then $M$ is an $R/I$-module.

Example 1.0.8. **Cyclic modules**: If $M$ is an $R$-module and there exists an $x$ in $M$ such that $M = Rx = \{ax \mid a \in R\}$, then $M$ is said to be a cyclic module. Also, by the fundamental theorem of homomorphisms the map $\mu_x = r \mapsto rx$ gives rise to the isomorphism $M \cong R/\ker(\mu_x)$.

The example above leads to an important definition that will be used later in the structure theorems for finitely generated modules over a principle ideal domain.

**Definition 1.0.9.** Let $M$ be a cyclic $R$-module with $M = Rx$ for some $x \in M$. Then the kernel of the homomorphism $\mu_x = r \mapsto R$ is denoted by $\text{ann}(x)$. This is referred to as the **annihilator** of $x$ in $R$. Check to see that $\text{ann} x$ is an ideal in $R$.

As we progress through this material, we will see additional modules that will play a significant role our discussion of the structure theorems.

*Note that $S$ is not an $R$-module because the multiplication is not closed.

**$R/I$ need not be a ring, unless $I$ is a 2-sided ideal.**
Basics of Module Theory

Linear Algebra Review

Linear algebra plays an important role in modern mathematics. As we shall soon see, modules have a very similar structure to that of vector spaces. This follows from our definition of a module. With this in mind, we will study the generalizations of the following concepts in the setting of module theory: vectors, linear independence, bases, linear transformations, eigenvalues, eigenvectors, matrix representation of transformations, change of basis matrices, determinants, matrix similarity, characteristic polynomials, minimum polynomials, and canonical matrix forms.

Notation and Special Matrices

We begin this section with a discussion of notation and special matrices that are convenient for calculations. We begin with some basic notation for working with matrices:

**Notation 1.0.10.** Let $A$ be an $m \times n$ matrix with entries $a_{ij}$ in a ring $R$. Then we have the following notation:

1. $C_j(A) = c_j = [a_{1j} \ldots a_{mj}]^T$ is the $j^{th}$ column of $A$.
2. $R_i(A) = r_j = [a_{i1} \ldots a_{in}]$ is the $i^{th}$ row of $A$.
3. $r_i(A) = r_j = [a_{1i} \ldots a_{in}]^T$ is the column representation of $R_i(A)$.
4. $e_j$ is the $n \times 1$ vector whose $j^{th}$ entry is $1_R$ and whose remaining entries are $0_R$, for each $n \in \mathbb{N}$, and $j \in \{1, \ldots, n\}$.

Using this notation, we can now state some convenient results relating the columns, rows, and entries of a matrix to the canonical base.

**Proposition 1.0.11.** Let $A \in M_{m \times n}(R)$, $B \in M_{n \times p}$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, $x \in R^n$. Then we have the following:

1. $Ae_j = C_j(A) = c_j$.
2. $e_i^T A = R_i(A) = r_i^T$.
3. $e_i^T A e_j = [a_{ij}]_{1 \times 1} = a_{ij}$.
4. \( Ax = x_1C_1(A) + \ldots + x_nC_n(A) \)
5. \( C_i(AB) = AC_i(B) \)
6. \( R_i(AB) = R_i(A)B \)

**Proof.** This is left as an exercise to the reader. \( \square \)

**Exercise 1.0.12.** If \( T \) is a linear transformation from \( M_n(R) \to M_n(R) \) where \( R \) is a commutative ring, let \( A \) be the matrix representation of \( T \).

(a) For any \( U \in GL_n(R) \) show that \( UA \) applied to a vector \( x \) is a linear combination of \( A \) applied to \( x \) (Hint: represent \( x \) as a sum of terms that look like \( x_i e_i \)).

Now we will focus our attention on some of the special matrices that will help us in calculations later.

**Definition 1.0.13.** The elementary matrices of type-0 are denoted \( e_{ij} \) and have all entries equal to zero except in the \( ij \) position, where it takes the value of \( 1_R \).

\[
e_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}
\]

**Definition 1.0.14.** The elementary matrices of type-1 are denoted \( T_{ij}(a) \) (where \( i \neq j \)) and are given by \( T_{ij}(a) = I + ae_{ij} \).

**Definition 1.0.15.** The elementary matrices of type-2 are matrices are denoted \( D_i(a) \), and are given by \( D_i(a) = I + (a - 1_R)e_{ii} \).

**Definition 1.0.16.** The elementary matrices of type-3 are matrices are permutation matrices denoted by \( P_{ij} \), and are given by

\[
P_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}
\]

The following proposition shows how left and right multiplication by an elementary matrix will affect an arbitrary matrix \( A \in M_n(R) \).

**Proposition 1.0.17.** Let \( A \in M_n(R) \), for a ring \( R \). Then:

1. \( e_{ij}A \) is the operation where each \( k \)th row of \( A \) is replaced by \( \delta_{ik}R_j(A) \) i.e. the \( k \)th row is zero except when \( k = i \) in which case it replaced by the \( j \)th row.

2. \( Ae_{ij} \) is the operation where each \( k \)th column of \( A \) is replaced by \( \delta_{kj}C_i(A) \).

This is similar to the case above.

3. \( T_{ij}(b)(A) \) is the operation for which \( R_i(A) \) is replaced by \( R_i(A) + bR_j(A) \).

4. \( AT_{ij}(b) \) is the operation for which \( C_j(A) \) is replaced by \( C_j(A) + bC_i(A) \).
5. $D_i(b)A$ is the operation where the $i$th row is replaced by $bR_i(A)$.

6. $AD_j(b)$ is the operation where the $j$th column is replaced by $bC_j(A)$.

7. $P_{ij}A$ swaps the $i$th and $j$th rows of $A$.

8. $AP_{ij}$ swaps the $i$th and $j$th columns of $A$.

We will conclude this section with an example of a module constructed with respect to a linear transformation $T$.

**Example 1.0.18.** Let $F$ be a field, $x$ be an indeterminate, and let $F[x]$ be the polynomial ring over $F$. Now suppose that $V$ is a vector space over $F$ and $T$ is a linear transformation from $V$ to itself. An $F[x]$-module with respect to a linear transformation $T$ is the set $V$ along with the map $\eta : F[x] \times V \to V$ given by

$$[a_nx^n + \ldots + a_1x + a_0](v) \mapsto a_nT^nv + \ldots + a_1Tv + a_0v$$

**Endomorphisms and Cayley’s Theorem**

This section will be brief, and the proofs will be omitted since they are easily produced. To begin, let us consider the structure of the set of endomorphisms of an abelian group.

**Theorem 1.0.19.** Let $M$ be an abelian group and let $\text{End}M$ be the set of endomorphism of $M$. Then for all $\eta, \mu \in \text{End}M$ we define $\eta\mu$ by $(\eta\mu)(x) = \eta(\mu(x))$ and $\eta + \mu$ by $(\eta + \mu)(x) = \eta(x) + \mu(x)$. Finally if we define the maps $1$ and $0$ by $1x = x$ and $0x = 0_M$, then under these operations, $(\text{End}M, +, \cdot, 0, 1)$ is a ring.

Now consider the example below.

**Example 1.0.20.** $M = (\mathbb{Z}^2, +, 0)$, where $\mathbb{Z}^2 = \{(x, y) : x, y \in \mathbb{Z}\}$. Notice that $e_1 = (1, 0)$ and $e_2 = (0, 1)$ generate $\mathbb{Z}^2$, since

$$(x, y) = x \cdot (1, 0) + y \cdot (0, 1)$$

for all $x, y \in \mathbb{Z}$. Therefore any endomorphism, $\eta$, of $M$ is determined by where $\eta$ maps $(1, 0)$ and $(0, 1)$. We now claim that there is a one-to-one correspondence between $\text{End}M$ and $\mathbb{Z}^2 \times \mathbb{Z}^2$. To see this, let $(x, y) \in \mathbb{Z}^2 \times \mathbb{Z}^2$, then the map

$$\eta = [(x, y) \mapsto xe_1 + ye_2]$$

is an endomorphism since

$$\eta((x_1, y_1) + (x_2, y_2)) = \eta((x_1 + x_2, y_1 + y_2))$$

$$= u(x_1 + x_2) + v(y_1 + y_2) = ux_1 + vy_1 + ux_2 + vy_2$$

$$= \eta((x_1, y_1)) + \eta((x_2, y_2))$$
Now since \( \eta \) is an endomorphism, and all endomorphisms are of this form, the map

\[ \eta : \mathbb{Z}^2 \to \text{End}M \]

\[ (u, v) \mapsto \eta \]

\[ (u, v) \mapsto [(1, 1) \mapsto (u, v)] \]

gives a one-to-one correspondence between \( \mathbb{Z}^2 \times \mathbb{Z}^2 \) and \( \text{End}M \). Now if \( \eta(e_1) = (a, b) \), and \( \eta(e_2) = (c, d) \) then we have the following bijection from \( \text{End}M \) to \( M_2(\mathbb{Z}) \).

\[ \eta \mapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix} \]

It can also be checked that this map is an isomorphism. This shows an isomorphism from \( \text{End}M \) to \( M_2(\mathbb{Z}) \), showing that \( (\text{End}M, +, \cdot, 0, 1) \) is a ring.

We will soon have a theorem that is nearly the converse to theorem 1.0.19. Before our next result we need the following definition.

**Definition 1.0.21.** A ring of endomorphisms is a subring of \( \text{End}M \) for some abelian group \( M \).

Now we have

**Theorem 1.0.22.** (Cayley's Theorem for Rings) Any ring is isomorphic to a ring of endomorphisms of an abelian group.

In the proof of Cayley’s theorem for rings, if \( R \) is a ring we let \( M = (R, +, 0) \) be the additive abelian group structure of a ring \( R \). Then the left translation module \( R_L \) is isomorphic to \( R \).

**Fundamental Concepts**

In this section, we will define several concepts and results that are basic to module theory. Before starting our list of definition, we shall make a note about our way of speaking of modules. We defined a left-module over a ring \( R \) to be an abelian group \( M \) along with a map, \( \eta \), satisfying the properties in definition 1.0.1. From now on we will call the application of the map, \( \eta \), as the action of \( R \) on \( M \).

Further we will now refer to a left modules simply as a module, an \( R \)-module, or a module over \( R \). Now we will start our list of list of definitions.
Definition 1.0.23. Let $M$ be a module over $R$. A submodule $N$ of $M$ is a subgroup of the additive group $(M, +, 0)$ that is closed under the action of $R$.

Now let us consider a few examples of submodules.

Example 1.0.24. Let $M$ be a $\mathbb{Z}$-module. If $N$ is a subgroup of $(M, +, 0)$, then $N$ is a $\mathbb{Z}$-submodule of $M$. Conversely if $N'$ is a $\mathbb{Z}$-submodule of $M$, then $N'$ is a subgroup of $(M, +, 0)$.

Example 1.0.25. Let $V$ be a vector space over a field $F$, $T : V \to V$ be a linear transformation. Then $V$ is an $F[x]$-module with respect to $T$. If $W$ is a subspace of $V$ and stabilized by $T$, i.e. $T(W) \subseteq W$, then $W$ is a submodule of $V$ over $F[x]$.

Example 1.0.26. Let $R$ be a ring, then $M = (R, +, 0)$ is a module over $R$. In this case, the submodules of $M$ are the left ideals of $R$.

Example 1.0.27. If $M$ is a module and $\{N_{\alpha}\}_{\alpha \in A}$ is a set of submodules of $M$, then $\bigcap_{\alpha \in A} N_{\alpha}$ is also a submodule of $M$.

We will now define a few special submodules.

Definition 1.0.28. If $M$ is a module and $S$ is a nonempty subset, then we denote the intersection of all submodules of $M$ containing $S$ by $\langle S \rangle$. We call this the submodule generated by the set $S$.

Definition 1.0.29. If $M$ is a module and $\{N_{\alpha}\}_{\alpha \in A}$, then we define the submodule generated by the submodules $\{N_{\alpha}\}_{\alpha \in A}$ to be $\langle \bigcup_{\alpha \in A} N_{\alpha} \rangle$. This set consists of all finite sums of the form $\sum_{i=0}^{d} x_{i}$ where each $x_{i} \in N_{\alpha_{i}}$. We denote this submodule by

$$\sum_{\alpha \in A} N_{\alpha}$$

Definition 1.0.30. Suppose $M$ is a module over a ring $R$ and let $N$ be a submodule. Then the factor group $M/N$ forms an $R$-module where $a(x + N) = ax + N$ for all $a \in R$ and $x \in M$. We call this module the quotient module of $M$ with respect to $N$.

Now we will turn our attention to homomorphisms of modules.

Definition 1.0.31. Let $M$ and $N$ be modules over a ring $R$. Then $\eta : M \to N$ is called a module homomorphism (also referred to as an $R$-homomorphism or homomorphism over $R$) if $\eta$ is a group homomorphism of $M$ and $N$ which satisfies $\eta(ax) = a\eta(x)$ for all $a \in R$ and $x \in M$.

Notice that if $N$ is a submodule of $M$, then the natural map $\nu : M \to M/N$ given by $x \mapsto x + N$ is a module homomorphism from $M$ to $M/N$. 

**Theorem 1.0.32. (First Isomorphism Theorem of Modules)**

Let $M$ and $N$ be modules and $\phi : M \to N$ be a module homomorphism. Then

1. The kernel of $\phi$ is a submodule of $M$.
2. The image of $\phi$ is a submodule of $N$.
3. The image of $\phi$ is isomorphic to $M/ \ker(\phi)$.

If $\phi$ is an epimorphism, then $N$ is isomorphic to $M/ \ker(\phi)$.

**Theorem 1.0.33. (Second Isomorphism Theorem of Modules)**

Let $M$ be a module, and let $S$ and $T$ be submodules of $M$. Then:

1. The sum $S + T = \{s + t|s \in S, t \in T\}$ is a submodule of $M$.
2. The intersection $S \cap T$ is a submodule of $M$.
3. The quotient modules $(S + T)/T$ and $S/(S \cap T)$ are isomorphic.

The following example shows the

**Example 1.0.34.** Let $M$ be a cyclic module over $\mathbb{Z}$. Then $M = \mathbb{Z}x$ for some $x \in M$, but by the first isomorphism theorem, the epimorphism $\eta : \mathbb{Z} \to \mathbb{Z}x$ given by $a \mapsto ax$ leads to the isomorphism

$$M \cong \mathbb{Z}/\text{ann } x$$

But this gives rise to two possibilities.

1. If we have $\text{ann } x = \{0\}$, then $M \cong \mathbb{Z}$.
2. Otherwise $\text{ann } x = (n)$, in which case $M \cong \mathbb{Z}/(n)$.

Further, since $\text{ann } x$ is the ideal $(n)$ and the order of $x$ is $n$, we refer to $\text{ann } x$ as the **order ideal of** $x$.

We will conclude this section by defining the $\text{Hom}$ space between two modules and giving a result on the $\text{Hom}$ space of a module with itself.

**Definition 1.0.35.** Let $M$ and $N$ be modules over a ring $R$, then $\text{Hom}_R(M, N)$ is the set of homomorphisms of $M$ into $N$.

**Theorem 1.0.36.** Let $M$ and $N$ be modules over a ring $R$, then $\text{Hom}_R(M, N)$ is an abelian group under the binary operation $(\eta + \mu)(x) = \eta(x) + \mu(x)$, where $\eta, \mu \in \text{Hom}_R(M, N)$ and $x \in R$.

The statement above can be extended to the following result.

**Theorem 1.0.37.** Let $M$ be an $R$-module, and define $(\eta + \mu)(x) = \eta(x) + \mu(x)$ and $(\eta \cdot \mu)(x) = \eta(\mu(x))$. Then $(\text{Hom}_R(M, M), +, \cdot, 0, 1)$ is a ring, where $0$ and $1$ are defined in the obvious way.
Free Modules

To be continued...
The Structure of Modules


Morbi ut tellus ut pede tincidunt porta. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam congue neque id dolor.


Vestibulum sed nisl eu sapien cursus rutrum.


Bibliography
Index

license, 2