Chris Hayduk
Math B4900
Course Summary
05/25/2021

1. Introduction

Building upon last semester's topics, we begin this semester by extending many of the same notions of group actions to ring theory. Modules allow us to study the behavior of rings acting on an abelian group, similarly to groups acting on sets. Modules provide us with a generalization of the notion of vector spaces, which we can recover by restricting ourselves to only considering fields acting on abelian groups. This gives us a nice link between the more abstract topics of module theory and the more foundational topics which we have studied in linear algebra. In fact, we discuss several of these topics, such as determinants and trace of matrices, while using the more advanced machinery developed throughout our study of abstract algebra. Lastly, moving into Lang's *Algebra*, we make many of the ideas surrounding modules even more rigorous. In addition, we introduce the idea of exact sequences and short exact sequences, which provide us with theorems to discuss relations between modules.

2. Topics

2.1. **Introduction to Module Theory.**

2.1.1. *Basic Definitions and Examples.* Modules allow us to extend our notion of group actions to rings. We can think of modules as the algebraic objects which rings act on, which can be seen in the following definition [1, §10.1, p. 337]:

Definition. Let R be a ring (not necessarily commutative nor with 1). A left R-module or a left module over R is a set M together with

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies

   a) $(r+s)m = rm + sm$ for all $r, s \in R, m \in M$

   b) $(rs)m = r(sm)$ for all $r, s \in R, m \in M$

   c) $r(m+n) = rm + rn$ for all $r \in R, m, n \in M$

   If the ring R has a 1 we impose the additional axiom

   d) $1m = m$ for all $m \in M$

Now that we have our definition of modules, it is natural to consider an analogy to "subsets" in the context of modules [1, §10.1, p. 337]:

Definition. Let R be a ring and let M be an R-module. An R-submodule of M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$, for all $r \in R, n \in N$

Hence, a submodule of M is a subset of M which is itself a module under the operations. Similar to the subgroup criterion, we can condense this definition for submodules into two easily verifiable conditions [1, §10.1, p. 342]:

Proposition. Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

(1) $N \neq \varnothing$

(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$

2.1.2. *Quotient Modules and Module Homomorphisms.* Now that we have discussed modules and submodules, we can also extend the notion of quotient groups and quotient rings to modules. We begin with the following definition [1, §10.2, p. 345]:

Definition. Let R be a ring and let M and N be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism if its respects the R-module structures of M and N, i.e.

   a) $\varphi(x+y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$ and

   b) $\varphi(rx) = r\varphi(x)$ for all $r \in R, x \in M$

(2) An R-module homomorphism is an isomorphism (of R-modules) if it is both injective and surjective. The modules M and N are said to be isomorphic, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$

(3) If $\varphi : M \to N$ is an R-module homomorphism, let $\ker \varphi = \{m \in M \mid \varphi(m) = 0\}$ (the kernel of φ) and let $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$ (the image of φ, as usual)

(4) Let M and N be R-modules and define $\mathrm{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M to N

The above definition allows us to extend our vocabulary regarding homomorphisms and isomorphisms from groups and rings to modules as well. This will be an important building block for constructing quotient modules, as we recall from last semester that quotient groups had a very strong connection with the kernels of homomorphisms between groups.

Now similarly, to the submodule criterion, let us state a proposition that makes it much easier to verify if a map is an R-module homomorphism [1, §10.2, p. 346]:

Proposition. Let M, N and L be R-modules

(1) A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and all $r \in R$

(2) Let φ, ψ be elements of $Hom_R(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$

for all $m \in M$. Then $\varphi + \psi \in Hom_R(M, N)$ and with this operation $Hom_R(M, N)$ is an abelian group. If R is a commutative ring than for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m))$$

for all $m \in M$. Then $r\varphi \in Hom_R(M, N)$ and with this action of the commutative ring R the abelian group $Hom_R(M, N)$ is an R-module

(3) If $\varphi \in Hom_R(L, M)$ and $\psi \in Hom_R(M, N)$ then $\psi \circ \varphi \in Hom_R(L, N)$

(4) With addition as above and multiplication defined as function composition, $Hom_R(M, M)$ is a ring with 1. When R is commutative $Hom_R(M, M)$ is an R-algebra.

Now with the definition and machinery in place to work the R-module homomorphisms, we can discuss quotient modules [1, §10.2, p. 348]:

Proposition. Let R be a ring, let M be an R-module and let N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by

$$r(x + N) = (rx) + N \text{ for all } r \in R, x + N \in M/N$$

The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x+N$ is an R-module homomorphism with kernel N.

Now we will also present equivalents of the isomorphism theorems for modules [1, §10.2, p. 345]:

Theorem. Isomorphism Theorems

(1) (*The First Isomorphism Theorem for Modules*) Let M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$

(2) (*The Second Isomorphism Theorem*) Let A, B be submodules of the R-module M. Then $(A + B)/B \cong A/(A \cap B)$

(3) (*The Third Isomorphism Theorem*) Let M be an R-module, and let A and B be submodules of M with $A \subset B$. Then $(M/A)/(B/A) \cong M/B$

(4) (*The Fourth Isomorphism Theorem*) Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \longleftrightarrow A/N$, for all $A \supset N$. This correspondence commutes with the process of taking sums and intersections (i.e., there is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M which contain N).

2.1.3. *Generation of Modules, Direct Sums, and Free Modules.* Now we introduce some definitions regarding submodules generated by subsets as well as finite sums of submodules [1, §10.3, p. 351]:

Definition. Let M be an R-module and let $N_1, \ldots, N_n$ be submodules of M.

(1) The *sum* of $N_1, \ldots, N_n$ is the set of all finite sums of elements from the sets $N_i : \{a_1 + a_2 + \cdots + a_n \mid a_i \in N_i \text{ for all } i\}$. Denote this sum by $N_1 + \cdots + N_n$

(2) For any subset A of M let

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m \mid r_1, \ldots, r_m \in R, a_1, \ldots, a_m \in A, m \in \mathbb{Z}^+\}$$

If A is the finite set $\{a_1, a_2, \ldots, a_n\}$ we shall write $Ra_1 + Ra_2 + \cdots + Ra_n$ for RA. Call RA the *submodule of M generated by A*. If N is a submodule of M (possibly $N = M$) and $N = RA$, for some subset A of M, we call A a *set of generators* or *generating set* for N, and we say N is *generated by A*

(3) A submodule N of M (possibly $N = M$) is *finitely generated* if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset

(4) A submodule N of M (possibly $N = M$) is *cyclic* if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element:

$$N = Ra = \{ra \mid r \in R\}$$

2.2. **Vector Spaces.**

2.2.1. *Definitions and Basic Theory.* Vector spaces follow very nicely from our above discussion of modules, as the definition of each vector space property is the same as the module-theoretic definition with the added assumption that R is a field. Hence, in the definitions above, we can replace "module" with "vector space" to get the equivalent definitions. Now we will discuss some notions distinct from modules [1, §11.1, p. 409]:

Definition.

(1) A subset S of V is called a set of *linearly independent* vectors if an equation $\alpha_1v_1 + \alpha_2v_2 + \cdots + \alpha_nv_n = 0$ with $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ and $v_1, v_2, \ldots, v_n \in S$ implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$

(2) A *basis* of a vector space V is an ordered set of linearly independent vectors which span V. In particular two bases will be considered different even if one is simply a rearrangement of the other. This is sometimes referred to as an *ordered basis*.

Proposition. Assume the set $\mathcal{A} = \{v_1, v_2, \ldots, v_n\}$ spans the vector space V but no proper subset of $\mathcal{A}$ spans V. Then $\mathcal{A}$ is a basis of V. In particular, any finitely generated (i.e., finitely spanned) vector space over F is a free F-module

Corollary. Assume the finite set $\mathcal{A}$ spans the vector space V. Then $\mathcal{A}$ contains a basis of V.

2.2.2. *The Matrix of a Linear Transformation.* We have that $M_{\mathcal{B}}^{\mathcal{E}}(\varphi) = (a_{ij})$ is the $m \times n$ matrix whose i, j entry is α_{ij}. Then for $v \in V$, we can write v in terms of the basis $\mathcal{B}$ as follows

$$v = \sum_{i=1}^{n} \alpha_i v_i, \ \alpha_i \in F$$

Then the image of v under φ is given by

$$\varphi(v) = \sum_{i=1}^{m} \beta_i w_i$$

Thus we have the following definition [1, §11.2, p. 415]:

Definition. The $m \times n$ matrix $A = (a_{ij})$ associated to the linear transformation φ above is said to *represent* the linear transformation φ with respect to the bases $\mathcal{B}, \mathcal{E}$. Similarly φ is the linear transformation represented by A with respect to the bases $\mathcal{B}, \mathcal{E}$.

2.2.3. *Dual Vector Spaces.* We will begin with the definition of dual spaces [1, §11.3, p. 431]:

Definition.

(1) For V any vector space over F let $V^* = Hom_F(V, F)$ be the space of linear transformation from V to F, called the *dual space* of V. Elements of V^* are called *linear functionals*.

(2) If $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ is a basis of the finite dimensional space V, define $v_1^8 \in V^*$ for each $i \in \{1, 2, \ldots, n\}$ by its action on the basis $\mathcal{B}$:

$$v_i^*(v_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

We can now use the notation we've just introduced in order to discuss some properties of V^* [1, §11.3, p. 432]:

Proposition. With notation as above, $\{v_1^*, v_2^*, \ldots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional then V^* has the same dimension as V.

Definition. The basis $\{v_1^*, v_2^*, \ldots, v_n^*\}$ of V^* is called the *dual basis* to $\{v_1, v_2, \ldots, v_n\}$

Definition. The dual of V^*, namely V^{**}, is called the *double dual* or *second dual* of V.

The dual space to V^*, V^{**}, can be related back to V through a linear transformation which is reflected in the following theorem [1, §11.3, p. 433]:

Theorem. There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional then this linear transformation is an isomorphism.

Hence, we can relate V both to its dual space and the dual of its dual space.

2.2.4. *Determinants.* We can start with the definition of what a determinant is, as well as how to compute it,

Definition. An $n \times n$ *determinant function* on R is any function

$$\det : M_{n \times n}(R) \to R$$

that satisfies the following two axioms:

(1) det is an n-multilinear alternating form on $R^n (= V)$, where the n-tuples are the n columns of the matrices in $M_{n \times n}(R)$

(2) $\det(I) = 1$ where I is the $n \times n$ identity matrix

Theorem. There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (α_{ij}) by the formula:

$$\det(\alpha_{ij}) = \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \alpha_{\sigma(2)2} \cdots \alpha_{\sigma(n)n}$$

2.3. **Modules over Principal Ideal Domains.**

2.3.1. *Jordan Canonical Form.* Jordan Canonical Form allows us to "simplify" matrices, putting them into a form that is as close to a diagonal matrix as possible [1, §11.3, p. 431]:

Definition.

(1) A matrix is said to be in *Jordan canonical form* if it is a block diagonal matrix with Jordan blocks along the diagonal

(2) A *Jordan canonical form* for a linear transformation T is a matrix representing T which is in Jordan canonical form

That is, a matrix J is in Jordan canonical form if it is constructed as follows,

$$J = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_p \end{bmatrix}$$

where each block J_i is a square matrix of the form,

$$J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}$$

Theorem. Let V be a finite dimensional vector space over the field F and let T be a linear transformation of V. Assume F contains all the eigenvalues of T:

(1) There is a basis for V with respect to which the matrix for T is in Jordan canonical form, i.e., is a block diagonal matrix whose diagonal blocks are the Jordan blocks for the elementary divisors of V

(2) The Jordan canonical form for T is unique up to a permutation of the Jordan blocks along the diagonal

2.4. **The Group of Homomorphisms.** We have that a pair of homomorphisms is said to be exact if

$$X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z$$

if $\text{img}(\varphi) = \ker(\psi)$. This definition may seem a bit esoteric, so we'll present an example here in order to illustrate things better:

$$\mathbb{Z} \xrightarrow{2x} \mathbb{Z} \xrightarrow{x \mod 2} \mathbb{Z}/2\mathbb{Z}$$

We see that the map $2x$ has the image $2\mathbb{Z}$. Moreover, the kernel of $x \mod 2$ is precisely $2\mathbb{Z}$ as well because every even integer modulo 2 is equal to 0. Hence, we have that this sequence is exact.

We can now define a special case of an exact sequence [1, §10.5, p.379]:

Definition: The exact sequence

$$0 \to A \xrightarrow{\psi} B \xrightarrow{\phi} \to C \to 0$$

is called a *short exact sequence*.

We can extend our exact sequence from above to a short exact sequence as follows,

$$0 \to \mathbb{Z} \xrightarrow{2x} \mathbb{Z} \xrightarrow{x \mod 2} \mathbb{Z}/2\mathbb{Z} \to 0$$

We can now present two similar relationships between exact sequences of modules and of the associated homomorphism groups [3, §2.2, p. 122]:

Proposition. A sequence

$$X' \xrightarrow{\lambda} X \to X'' \to 0$$

is exact if and only if the sequence

$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y) \leftarrow 0$$

is exact for all Y.

Similarly, we have,

Proposition. A sequence

$$0 \to Y' \to Y \to Y'',$$

is exact if and only if

$$0 \to \mathrm{Hom}_A(X, Y') \to \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X, Y'')$$

is exact for all X.

In addition, we have the notion of a split short exact sequence [2, Lec 10, p.6]:

Definition: An SES $0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$ of A-modules is said to be *split* if there is *some* $Z' \subset Y$ satisfying,

(1) $Y = f(X) + Z'$

(2) $f(X) \cap Z' = 0$, and

(3) $g|_{Z'}$ is an isomorphism.

So $Y \cong f(X) \oplus Z'$, and that isomorphism preserves the splitting.

From the same lecture, we have two examples demonstrating a difference between split and non-split short exact sequences, given by [2, Lec 10, p.7]:,

$$0 \to \mathbb{Z} \xrightarrow{x \mapsto (x,0)} \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \xrightarrow{(x,y) \mapsto y} \mathbb{Z}/n\mathbb{Z} \to 0 \tag{1}$$

and,

$$0 \to \mathbb{Z} \xrightarrow{x \mapsto nz} \mathbb{Z} \xrightarrow{x \mapsto x + n\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to 0 \tag{2}$$

are both exact, but (1) is split and (2) is not.

2.5. **Module Decompositions.**

2.5.1. *Finding Module Decompositions.*

2.5.2. *Decomposition of* $\mathbb{C}S_3$.

2.5.3. *Failing to Find Module Decompositions.*

References

[1] Dummit, David Steven., and Richard M. Foote. *Abstract Algebra*. 3rd ed., John Wiley & Sons, 2004.
[2] Daugherty, Zajj. *Math B4900: Modern Algebra II*, Lecture Notes, 2021.
[3] Lang, Serge. *Algebra*. Springer-Verlag New York Inc., 2012.