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.

In the second portion of the course, we moved to characterizing types of rings and modules, as well as how to work with them. This allowed us to construct complicated modules from simpler constituent parts, as well as to draw conclusions about the behavior of these larger modules through the properties of their constituent submodules. We also touched on new types of operators and groups, including tensor products and Lie groups. These concepts broadened the scope of examples within the class and demonstrated a variety of settings in which algebraic concepts are applicable. In particular, Lie groups and Lie algebras provided a beautiful way to connect many of the concepts that we have learned over the past two semesters to concepts in analysis, integrating the knowledge gained over the past two semesters into a broader mathematical framework.

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 $\mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by

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

for all $m \in M$. Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ 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 $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this action of the commutative ring R the abelian group $Hom_R(M, N)$ is an R-module

(3) If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi \circ \varphi \in Hom_R(L, N)$

(4) With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is a ring with 1. When R is commutative $\mathrm{Hom}_R(M, M)$ 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 and Direct Sums.* 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:

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

The direct product of a collection of R-modules is again an R-module. We can also refer to this direct product as an *(external) direct sum* [1, §10.3, p. 353]. We can characterize some equivalent notions of direct products of R-modules as follows [1, §10.3, p. 353]:

Proposition 5. Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent:

(1) The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots N_k$ defined by

$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \ldots + a_k$$

is an isomorphism (of R-modules): $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots N_k$

(2) $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j_1} + \cdots + N_k) = 0$ for all $j \in \{1, 2, \ldots, k\}$

(3) Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

If an R-module $M = N_1 + N_2 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of M satisfying the equivalent conditions of the proposition above, then M is said to be the *(internal) direct sum* of $N_1, N_2, \ldots, N_k$, written

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k$$

We also have an additional way to show that an A-module is decomposible into a direct sum of A-module through the following proposition [2, Lec 11, p. 2]:

Proposition: Let M be an A-module. Suppose that there exist A-module homomorphisms $\varphi_i : M \to M$ for $i = 1, \ldots, n$ such that

$$\sum_{i=1}^{n} \varphi_i = \mathrm{id} \quad \text{and} \quad \varphi_i \circ \varphi_j = 0 \text{ for } i \neq j$$

Then $\varphi_i^2 = \varphi_i$ for all i. Further, if $X_i = \varphi_i(M)$, then

$$\varphi : M \to \bigoplus_{i=1}^{n} X_i \text{ defined by } \varphi = \varphi_1 \oplus \cdot\varphi_n$$

is an A-module

2.1.4. *Decomposition of* $\mathbb{C}S_3$. Let $A = \mathbb{C}S_3$. Then if we define,

$$z_1 = \frac{1}{6}(1 + (12) + (13) + (23) + (123) + (132)),$$
$$z_2 = \frac{1}{6}(1 - (12) - (13) - (23) + (123) + (132)),$$
$$\text{and } z_3 = \frac{1}{3}(2 - (123) - (132)),$$

we showed that the maps,

$$\varphi_1 : M \to M, m \mapsto z_1 m, \;\; \varphi_2 : M \to M, m \mapsto z_2 m, \;\; \varphi_3 : M \to M, m \mapsto z_3 m$$

satisfy,

$$\varphi_1 + \varphi_2 + \varphi_3 = \mathrm{id}_M \quad \text{and} \quad \varphi_i \varphi_j = 0 \text{ for all } i \neq j$$

By the proposition presented above, we thus have that for any A-module M, we have

$$M \cong \varphi_1(M) \oplus \varphi_2(M) \oplus \varphi_3(M)$$

2.1.5. *Free Modules.* We can now introduce the definition for a free module in order to expand on this notion [1, §10.3, p. 354]:

Definition. An R-module F is said to be *free* on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$, for some $n \in \mathbb{Z}^+$. In this situation we say A is a *basis* or *set of free generators* for F. If R is a commutative ring, the cardinality of A is called the *rank* of F.

These free generators satisfy an interesting property [1, §10.3, p. 354]:

Theorem. For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following *universal property*: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(A) = \varphi(a)$ for all $a \in A$.

When A is the finite set $\{a_1, a_2, \ldots, a_n\}$, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

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 $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ 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 $V^* = \mathrm{Hom}_F(V, F)$ 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

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

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 [4, §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. **Continuing with Modules.** Using the above notions from exact sequences, we can now define some more general classes of modules.

2.5.1. *Projective Modules.* Projective modules generalize the notion of free modules defined in Section 2.1.5 (recall that free modules are modules with basis vectors). We will see that every free module is a projective module, but the converse fails to hold true in some cases.

The following proposition fully characterizes projective modules [1, §10.5, p. 389]:

Proposition. Let P be an R-module. Then the following are equivalent:

(1) For any R-modules L, M, and N, if

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

is a short exact sequence, then

$$0 \to \mathrm{Hom}_R(P, L) \xrightarrow{\psi'} \mathrm{Hom}_R(P, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(P, N) \to 0$$

is also a short exact sequence.

(2) For any R-modules M and N, if $M \xrightarrow{\varphi} N \to 0$ is exact, then every R-module homomorphism from P into N lifts to an R-module homomorphism into M

(3) If P is a quotient of the R-module M then P is isomorphic to a direct summand of M, i.e., every short exact sequence $0 \to L \to M \to P \to 0$ splits.

(4) P is a direct summand of a free R-module

An R-module P is called *projective* if it satisfies any of the above conditions.

2.5.2. *Injective Modules.* Injective modules form the dual of projective modules. Generally, it is a module that shares some properties with the $\mathbb{Z}$ module $\mathbb{Q}$ of all rational numbers. Similarly to projective modules, we will present the proposition which characterizes injective modules [1, §10.5, p. 394]:

Proposition. Let Q be an R-module. Then the following are equivalent:

(1) For any R-modules L, M, and N, if

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

is a short exact sequence, then

$$0 \to \mathrm{Hom}_R(N, Q) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, Q) \xrightarrow{\psi'} \mathrm{Hom}_R(L, Q) \to 0$$

is also a short exact sequence.

(2) For any R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is exact, then every R-module homomorphism from L into Q lifts to an R-module homomorphism of M into Q

(3) If Q is a submodule of the R-module M, then Q is a direct summand of M, i.e., every short exact sequence $0 \to Q \to M \to N \to 0$ splits

An R-module Q is called *injective* if it satisfies any of the above equivalent conditions. For example, the rational numbers $\mathbb{Q}$ are an injective $\mathbb{Z}$-module. However, since $\mathbb{Z}$ is not divisible, $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module.

We now also have an important theorem which characterizes the containment of modules in injective modules [1, §10.5, p. 398]:

Theorem. Let R be a ring with 1 and let M be an R-module. Then M is contained in an injective R-module.

2.5.3. *Schur's Lemma.* Below is the statement of Schur's Lemma [2, Lec. 15, p. 1]:

Theorem. (Schur's Lemma) If U and V are simple A-modules and $\varphi : U \to V$ is an A-module homomorphism, then φ is either the 0 map, or it is an isomorphism.

Some consequences of this lemma are presented below:

(1) if V is simple, then
$$\mathrm{End}_A(V) = \{A - \text{module homomorphisms } \varphi : V \to V\}$$
is a division ring, i.e. $\mathrm{End}_A(V) = \mathrm{Aut}_A(V) \cup \{0\}$

(2) If U is a simple submodule of an A-module V and $\varphi : V \to W$ is an A-module homomorphism, then $U \subset \ker(\varphi)$ or W contains a submodule isomorphic to U.

(3) If $V \cong V_1 \oplus V_2$ where V_1 and V_2 are simple nonisomorphic modules, then the only submodules of V are $0, V_1, V_2$, and V. Further,
$$\mathrm{End}_A(V) = \mathrm{End}_A(V_1) \times \mathrm{End}_A(V_2)$$
and, again, $\mathrm{End}_A(V_i)$ are division rings.

(4) If V is simple and U is a nonzero proper submodule of $V \oplus V$, then $V \cong U$ (but is not necessarily equal to $V \oplus 0$ or $0 \oplus V$)

2.5.4. *Maschke's Theorem.* We have that a ring A is *semisimple* if every A module is isomorphic to the direct sum of simple modules [2, Lec. 11, p. 1]. We will now state Maschke's Theorem, which states that "group algebras are often semisimple" [2, Lec. 11, p. 2]:

Theorem. Let G be a finite group and let F be a field with $\mathrm{char}(F) \nmid |G|$. Let V be an FG-module and U be a submodule. Then there's a submodule W in V satisfying $U \cap W = 0$ and $U + W = V$ so that $V \cong U \oplus W$, i.e. V contains a direct sum complement to U.

2.5.5. *Artin-Wedderburn.* Artin-Wedderburn assists in classifying semisimple rings and semisimple algebras. The theorem statement is as follows [2, Lec. 16, p. 6]:

Theorem. Let $A \neq 0$ be a ring with 1. The following are equivalent:

(1) Every A-module is projective

(2) Every A-module is injective

(3) Every A-module is completely reducible

(4) The left regular module decomposes as $A \cong \bigoplus_{\lambda \in \Lambda} A^\lambda$, where each A^λ is a simple A-module. More specifically, $A^\lambda = Ae_\lambda$ for some idempotent $e_\lambda \in A$, and the idempotents $\{e_\lambda \mid \lambda \in \Lambda\}$ satisfy
$$e_\lambda e_\mu = \delta_{\lambda_\mu} e_\lambda \quad \text{and} \quad \sum_{\lambda \in \Lambda} e_\lambda = 1$$

(5) As rings,
$$A \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_\ell}(\Delta_\ell)$$
where Δ_i is a division ring for each i. Moreover, up to permutation and isomorphism, the n_i and δ_i are unique.

Any ring A satisfying these conditions is called *semisimple*.

Example: If G is a finite group and F is a field of characteristic not dividing $|G|$, then FG is semisimple [2, Lec. 16, p. 6].

2.5.6. *Noetherian Modules.* Noetherian modules are modules which satisfy the ascending chain condition on its submodules, defined formally as follows [4, §10.1, p. 413]:

Definition. Let A be a ring and M a module (i.e., a left A-module). We shall say that M is *Noetherian* if it satisfies any of the following three conditions:

(1) Every submodule of M is finitely generated

(2) Every ascending sequence of submodules of M,
$$M_1 \subset M_2 \subset M_3 \subset \cdots$$
such that $M_i \neq M_{i+1}$ is finite.

(3) Every non-empty set S of submodules of M has a maximal element (i.e., a submodule M_0 such that for any element N of S which contains M_0 we have $N = M_0$).

All three of the above conditions are equivalent. We can also characterize the submodules of a Noetherian module as follows [2, Lec. 17, p. 4]:

Proposition. If M is Noetherian, then so is N and M/N for every submodule $N \subset M$.

Moreover, we can go in the reverse direction, and show that a Noetherian submodule can imply that the greater module is also Noetherian [2, Lec. 17, p. 4]:

Proposition. For a submodule $N \subset M$, if N and M/N are Noetherian, then so is M.

2.5.7. *Artinian Modules.* Artinian modules are modules which satisfy the descending chain condition on its submodules, defined formally as follows [4, §10.7, p. 439]:

Definition. Let A be a ring, not necessarily commutative, and E an A-module. We say that E is *Artinian* if E satisfies the descending chain condition on submodules, that is a sequence
$$E_1 \supset E_2 \supset E_3 \supset \cdots$$
must stabilize: there exists an integer N such that if $n \geqslant N$ then $E_n = E_{n+1}$.

A ring is Artinian if its left-regular module is Artinian.

2.5.8. *Semisimple Modules.* Put succinctly, a semisimple module is a module that, in some sense, are modules which can be easily understood by their constituent parts. We will define it formally as follow [2, Lec 18, p. 1]:

Definition. Let M be an A-module. We say M is semisimple if every submodule of M is a direct summand of M (i.e. every submodule of M has a direct sum complement).

Some examples include: the 0 module, simple modules, and completely decomposable modules

We can define some similar notions of semisimple modules through the following theorem [3, §1.2, p. 26]:

Theorem. For an A-module M, the following three properties are equivalent:

(1) M is semisimple.

(2) M is the direct sum of a family of simple submodules.

(3) M is the sum of a family of simple submodules.

Moreover, we can state a theorem which characterizes equivalent notions of *semisimple rings* [3, §1.2, p. 27]:

Theorem. For a ring A, the following are equivalent:

(1) Every SES of A-modules splits.

(2) Every A-module is semisimple.

(3) Every finitely generated A-module is semisimple.

(4) Every cyclic A-module is semisimple.

(5) The left-regular A-module is semisimple

Moreover, if A satisfies these conditions, then the left-regular module is isomorphic to a finite direct sum of simple modules.

We can now connect semisimplicity to projective and injective modules as follows [2, Lec. 18, p. 4]:

Theorem. Let A be a ring with 1. The following are equivalent:

(1) A is semisimple.

(2) All A-modules are projective.

(3) All finitely-generated A-modules are porjective.

(4) All cyclic A-modules are projective.

Corollary. A is semisimple if and only if every A-module is injective.

2.6. **Matrix Rings.** A matrix ring over a ring A is, generally, a set of matrices with entries in a ring A that itself forms a ring under matrix addition and multiplication. In this section, we develop some notions which relate matrix rings to properties of the underlying ring that forms the entries of these matrices. For example, we can make the following statement about the ideals of a matrix ring [2, Lec. 19, p. 1]:

Theorem. The ideals of $A = M_n(R)$ are in bijection with the ideals of R; namely, the ideals of A are precisely those of the form $M_n(S)$ where S is an ideal of R. In particular, if R is simple, then so is $M_n(R)$.

Hence, we can now simply compute the ideals for R in order to retrieve the ideals for $M_n(R)$. In addition, matrix rings formed over division rings have several interesting properties [2, Lec. 19, p. 3]:

Theorem. Let Δ be a division ring, and let $A = M_n(\Delta)$. Then,

(1) A is a simple ring, and is semisimple, Artinian, and Noetherian;

(2) the natural A-module $V = \Delta^n$ is the unique simple A-module (up to isomorphism);

(3) the left-regular A-module is isomorphic to V^n; and

(4) the endomorphism ring $\mathrm{End}(V)$ is isomorphic to Δ

We can now examine the products of matrix rings. The following theorem provides us with tools for describing and operating with them [2, Lec 20, p. 1]:

Theorem. Let $A = A_1 \times \cdots \times A_\ell$, where $A_i = M_{n_i}(\Delta_i)$ for some integers n_i and division rings Δ_i.

(1) Let z_i be the identity of the ith component, so that

$$A \to \hat{A}_i \text{ defined by } a \mapsto z_i a$$

is the projection onto the ith component. Then $z_1, \ldots, z_\ell$ are pairwise orthogonal idempotents that sum to 1.

(2) For any A-module N, we have

$$N \cong z_1 N \oplus \cdots \oplus z_\ell N.$$

In particular, each $z_i N$ is an $\hat{A}_i$ module on which $\hat{A}_j$ acts trivially for every $i \neq j$.

(3) Up to isomorphism $\{\Delta_i^{n_i} \mid i = 1, \ldots, \ell\}$ forms a complete list of simple A-modules with action on $\Delta_i^{n_i}$ given by

$$\hat{A}_i \cong A_i \text{ acts naturally, and } \hat{A}_j \text{ acts by 0 for } j \neq i$$

(4) Every A-module is completely decomposable, i.e. A is semisimple.

(5) If $\Delta_1 \cong \cdots \cong \Delta_\ell \cong F$ are all the same field, then A is a vector space over F of dimension $\sum_{i=1}^{\ell} n_i^2$ and $\dim(Z(A)) = \ell$.

2.7. **Categories.** Our brief foray into Category Theory provided us with a glimpse of an even more general theory of relationships between objects. In particular, categories consist of sets of objects, along with sets of morphisms between those objects. These can be defined as follows [2, Lec. 15, p. 5]:

A **category** $\mathcal{C}$ consists of $\mathrm{Obj}(\mathcal{C})$, a set of objects, and $\mathrm{Hom}(\mathcal{C}) = \bigsqcup_{X,Y \in \mathrm{Obj}(\mathcal{C})} \mathrm{Hom}_{\mathcal{C}}(X, Y)$, a set of morphisms between those objects. These morphisms are subject to several constraints:

(1) Composition of morphisms is defined:

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) &\to \mathrm{Hom}_{\mathcal{C}}(X, Z) \\ (f, g) &\mapsto g \circ f = gf \end{aligned}$$

(2) Composition of morphisms is associative: $h(gf) = (hg)f$.

(3) If $X \neq X'$ or $Y \neq Y'$, then $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cap \mathrm{Hom}_{\mathcal{C}}(X', Y') = \varnothing$.

(4) Identity morphisms exist, i.e. for all $Y \in \mathrm{Obj}(\mathcal{C})$, there is some $1_Y \in \mathrm{Hom}_{\mathcal{C}}(Y, Y)$ such that

$$1_Y f = f \text{ and } g 1_Y = g$$

for all $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$.

A **subcategory** $\mathcal{D} \subset \mathcal{C}$ satisfies $\mathrm{Obj}(\mathcal{D}) \subset \mathrm{Obj}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{D}}(X, Y) \subset \mathrm{Hom}_{\mathcal{C}}(X, Y)$ for all $X, Y \in \mathrm{Obj}(\mathcal{D})$.

We can now show a couple examples of categories [2, Lec. 15, p. 6]:

(1) $\mathcal{S}$et is the category whose objects are sets, and whose morphisms are set maps:

$$\mathrm{Obj}(\mathcal{S}et) = \{\text{sets}\}, \quad \mathrm{Hom}(X, Y) = \{\text{functions } f : X \to Y\}$$

The category $\mathcal{F}$inSet of finite sets is a subcategory.

(2) $\mathcal{G}$rp is the category whose objects are groups, and whose morphisms are group homomorphisms. One subcategory of $\mathcal{G}$rp is the category of abelian groups, $\mathcal{A}$b

2.8. **Tensor Products.** Tensor products allow us to define a new type of relation between vector spaces as follow [2, Lec. 21, p. 2]:

Let F be a field, and let U and V be vector space over F. Define the **tensor product** of U and V over F as the linear span of **simple tensors** $u \otimes v$ (where $u \in U, v \in V$),

$$U \otimes V = F\{u \otimes v | u \in U, v \in V\}$$

modulo "bilinear" relations:

$$(\alpha u) \otimes v = \alpha(u \otimes v) = u \otimes (\alpha v)$$
$$(u_1 + u_2) \otimes v = u_1 \otimes v + u_2 \otimes v$$
$$u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2$$

2.9. **Lie Groups and Lie Algebras.** A Lie group is group which is also a differentiable manifold. Hence, the group is continuous and the group multiplication is differentiable. Some important examples are the classical Lie groups [2, Lec 22, p. 1]:

(1) general linear group $\mathrm{GL}_n(F) = \{x \in M_n(F) \mid \det(x) \neq 0\}$

(2) special linear group $\mathrm{SL}_n(F) = \{x \in M_n(F) \mid \det(x) = 1\}$

(3) special orthogonal group $\mathrm{SO}_n(F) = \{x \in \mathrm{SL}_n(F) \mid x^{-1} = x^t\}$

(4) special unitary group $\mathrm{SU}_n(F) = \{x \in \mathrm{SL}_n(F) \mid x^{-1} = x^*\}$

We can now define a Lie algebra as well [2, Lec 22, p. 2]:

The tangent space to 1 in a Lie group G admits an algebraic structure, resulting in a Lie algebra: a vector space $\mathfrak{g}$ over F with a (bilinear) bracket $[,] : \mathfrak{g} \otimes \mathfrak{g} \to \mathfrak{g}$ satisfying

a) (skew symmetry) $[x, y] = -[y, x]$, and

b) (Jacobi identity $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$

for all $x, y, z \in \mathfrak{g}$ (not associative). Lie algebras can be thought of as infinitesimal symmetry motions.

2.10. **Characters.** We will define characters as follows [2, Lec 23, p. 1]:

Let G be a finite group and F a field. Let $\rho : FG \to \mathrm{End}(V)$ be a finite-dimensional representation (equivalently, let $V = F^n$ be an FG-module). The **character** of the representation ρ is

$$\chi_\rho : FG \to F \text{ defined by } a \mapsto \mathrm{tr}(\rho(a)).$$

Equivalently, χ_V is the character associated to the module V. We can now present some properties as characters [2, Lec 23, p. 2]:

Proposition. Let $\rho : FG \to \mathrm{End}(V)$ be a finite-dimensional representation of a finite group G, and let χ_ρ be the associated character.

(1) χ_ρ is linear, i.e. for all $a, b \in FG$ and $\alpha \in F$, we have,

$$\chi_\rho(a + b) = \chi_\rho(a) + \chi_\rho(b) \text{ and } \chi_\rho(\alpha a) = \alpha\chi_\rho(a)$$

(2) χ_ρ is a class function on G, meaning that it is uniform on conjugacy classes of G (i.e. for all $g, h \in G$, we have $\chi_\rho(ghg^{-1}) = \chi_\rho(h)$

(3) the degree of χ_ρ is $\deg(\chi_\rho) = \deg(\rho) = \chi_\rho(1)$.

In addition,

Proposition. The character of the (direct) sum is the sum of the characters:

$$\chi_{\rho_1 \oplus \cdots \oplus \rho_\ell} = \chi_1 + \cdots + \chi_\ell$$

3. Conclusion and Reflection

After two semesters of rigorous work in Algebra, I can say quite confidently that I have learned more about this field than I ever thought possible for myself. About 10 years ago, I received a C+ in high school Honors Algebra - my worst grade to date. Then, in college, I struggled to wrap my head around the concepts presented in my first Linear Algebra course and left it feeling like I did not fully grasp the material. I entered Algebra last semester excited to learn, but apprehensive due to my previous experiences with the much simpler iterations of this subject. In spite of this apprehension, over the ensuing 9 months, I have developed a deep appreciation for this beautiful area of mathematics and how it integrates into the broader mathematical fabric. In particular, as a fan of analysis, our brief study of Lie groups and Lie algebras was incredible for helping me to integrate and synthesize much of the work we have discussed about groups, algebras, and representation theory. At the same time, in my Stochastic Processes class, we began diving deep into random walks on groups, again drawing upon many of the concepts learned during these past two semesters. These two topics in particular helped me to appreciate not only how far my understanding of Algebra had come since the days of struggling with high school Algebra, but also to understand the power of applying algebraic techniques and concepts to other areas of math. I hope to continue to dive deep into Algebra over the coming years, exploring its applications to other areas of math, as well as to other subjects entirely.

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] Lam, Tsit-Yuen. *A First Course in Noncommutative Rings*. Springer, 2001.
[4] Lang, Serge. *Algebra*. Springer-Verlag New York Inc., 2012.