Modules, Splitting Sequences, and Direct Sums

Maria Ross

Department of Mathematics and Computer Science
University of Puget Sound

Abstract

This report studies modules, structures which are a generalization of vector spaces over any ring rather than a field. We examine basic properties of modules, including those similar to properties of vector spaces, groups, rings, and other familiar algebraic structures. We will focus on the direct sum of modules, and what properties are necessary for a module to be isomorphic to the direct sum of modules, and thus have a direct decomposition. This involves free modules and torsion modules, along with the study of sequences of module homomorphisms, and properties of sequences such as exactness and whether sequences split.

1 Introduction

We begin with a ring and consider a structure which has the properties of a vector space with the exception of being over a ring rather than a field. We call this structure a *module,* or an *R-module* over a ring R. If the base ring R is not commutative, we differentiate between left and right modules.

Definition 1.1. A *left R-module* M over a ring R is an abelian additive group together with a map $R \times M \to M$, denoted by $(r, m) \mapsto rm$ that satisfies the following properties for $r, s \in R$ and $m, n \in M$:

(i) $(r + s)m = rm + sm$

(ii) $r(m + n) = rm + rn$

(iii) $(rs)m = r(sm)$

(iv) if $1 \in R$, then $1m = m$.

Note that rings act on modules similarly to how groups act on sets with group actions.

Example 1.2. [1] Consider a ring R and the set of $n \times n$ matrices over R, $M_n(R)$. Define the action of R on $M_n(R)$ as $r \mapsto rA$ for $r \in R$ and $A \in M_n(R)$, where rA denotes scalar multiplication by r. Then $M_n(R)$ is an $R-$module under matrix addition, since $M_n(R)$ is an abelian additive group, and scalar multiplication satisfies the necessary module axioms.

Some familiar algebraic structures are examples of modules. Vector spaces are modules over fields, ideals of a ring R are $R-$modules, and abelian groups are modules over the ring of integers. Additionally, rings are always modules over themselves.

2 Some Properties of Modules

Modules exhibit many familiar properties that we have seen from vector spaces and other algebraic structures.

Definition 2.1. A non-empty subset N of an $R-$module M is a *submodule* if for every $r, s \in R$ and $n, l \in N$, we have that $rn + sl \in N$.

Example 2.2. Consider the ring of integers, and the ideal $6\mathbb{Z}$. Then $6\mathbb{Z}$ is a $\mathbb{Z}$-module, and $12\mathbb{Z}$ is a subgroup of $6\mathbb{Z}$. We only need to show that $ax + by \in 12\mathbb{Z}$ for $x, y \in 12\mathbb{Z}$ and $a, b \in \mathbb{Z}$. If $x, y \in 12\mathbb{Z}$, then $x = 12q$ for some integer q, and $y = 12r$ for some integer r. Then $ax + by = a(12q) + b(12r) = 12(aq) + 12(br) = 12(aq + br) \in 12\mathbb{Z}$ since $a, b, q, r \in \mathbb{Z}$. Thus $12\mathbb{Z}$ is a submodule of $6\mathbb{Z}$.

Proposition 2.3. *Consider a ring R and an R-module M. Then, for $r \in R$ and $m \in M$,*

(i) $(r)0_M = 0_M$

(ii) $(0_R)m = 0_M$

(iii) $(-r)m = -(rm) = r(-m)$

(iv) $(nr)m = n(rm) = r(nm)$ for all $n \in \mathbb{Z}$.

We want to work with functions between modules. This gives rise to the study of module homomorphisms, which behave exactly as one would expect them to.

Definition 2.4. If M and N are $R-$modules, a *module homomorphism* from M to N is a mapping $f : M \to N$ so that

(i) $f(m + n) = f(m) + f(n)$

(ii) $f(rm) = rf(m)$

for $m, n \in M$ and $r \in R$. A homomorphism from a module to itself is a *module endomorphism*, and a bijective module homomorphism is a *module isomorphism.* A surjective homomorphism is an *epimorphism*, and an injective homomorphism is a *monomorphism.*

Example 2.5. Consider the $\mathbb{Z}$-modules $M = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ and $N = \{0, 2, 4, 6, 8\}$. Note that these are indeed modules, because all abelian groups are modules over the ring of integers. Then there is a module isomorphism $\phi : M \to N$ where $\phi(x) = 2x$ for $x \in M$, so $M \cong N$.

We will give an example of modules that are not isomorphic later, in the section on free modules.

Since modules are additive abelian groups, we understand module quotient structures.

Proposition 2.6. *Suppose R is a ring, M an $R-$module, and N a submodule of M. Then M/N, the quotient group of cosets of N, is an $R-$module.*

Proof. Since M and N are additive abelian groups, it follows that M/N is an additive abelian group. We define the action of R on M/N by $(r, m + N) \mapsto rm + N$, and use coset operations and the action of R on representatives from M to see that for $r, s \in R$ and $m + N, l + N \in M/N$,

(i) $(r + s)(m + N) = r(m + N) + s(m + N) = (rm + N) + (sm + N)$

(ii) $r((m + N) + (l + N)) = r(m + l + N) = rm + rl + N = (rm + N) + (rl + N)$

(iii) $(rs)(m + N) = (rsm + N) = r(sm + N)$

(iv) if $1 \in R$, then $1(m + N) = 1m + N = m + N$.

□

For the purposes of this report, we will be primarily concerned with modules over commutative rings. For reasons of simplicity, this report will typically refer to modules, rather than specifying left or right modules, and will assume rings are commutative unless stated otherwise.

3 Direct Sums, Free Modules, and Torsion

We begin with the notion of the direct product from group theory. Since modules are additive abelian groups, it is clear that we have a way of computing the direct product of modules. First, consider a set I of indices, either finite or infinite. A *family* $(x_i, i \in I)$ is a function on I whose value at i is x_i. Suppose R is a ring, and M_i (for $i \in I$) are R-modules. We define the *direct product* of modules M_i, denoted by $\prod_{i \in I} M_i$, to be all families $(x_i, i \in I)$ with $x_i \in M_i$. Addition is defined by $(x_i) + (y_i) = (x_i + y_i)$, and scalar multiplication is defined by $r(x_i) = (rx_i)$. Complications arise in the cast of the index set I being infinite, so in order to simplify things, we add a new definition.

Definition 3.1. The *external direct sum* of the modules M_i for $i \in I$ is $\bigoplus_{i \in I} M_i$, all families $(x_i, i \in I)$ with $x_i \in M_i$ such that $x_i = 0$ for all except finitely many i. That is, no x_i can take on nonzero values for infinite indices i. Addition and scalar multiplication are the same as for the direct product defined above, so for finite I, we have that $\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i$.

The notation for direct sums and direct products is fairly abstract, so a straightforward example can help to clarify these definitions.

Example 3.2. Suppose M and N are R-modules, and we want to find $M \oplus N$. Since we are finding the direct sum of only two modules, we do not have to worry about the distinction between the direct sum and the direct product, and $M \oplus N = \{(m, n) | m \in M, n \in N\}$. For an explicit example, let $M = \mathbb{Z}_2$ and $N = \mathbb{Z}_3$ be $\mathbb{Z}$-modules. Then $M \oplus N = \{(0,0), (0,1), (0,2), (1,0), (1,1)(1,2)\}$. Then, we see that $M \oplus N \cong \mathbb{Z}_6$.

Definition 3.3. [9] Suppose M is an R-module, and M_1, M_2 are submodules of M. M is the *internal direct sum* of M_1 and M_2 if $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$. In this case, every $m \in M$ can be written uniquely as $m = m_1 + m_2$ for $m_1 \in M_1$, $m_2 \in M_2$. If M is the internal direct sum of M_1 and M_2, then M is isomorphic to the external direct sum of M_1 and M_2. That is, $M \cong M_1 \oplus M_2$. Because interal direct sums are isomorphic to external direct sums, we typically will refer only to direct sums without specifying any further. If M is an R-module and $M \cong M_1 \oplus M_2$, then $M_1 \oplus M_2$ is called a *direct decomposition* of M. A module is *indecomposable* if it cannot be written as the direct sum of nonzero submodules. Then, we become interested in when modules are decomposable.

When R is a field, every R-module has a basis, since every R-module is a vector space. However, over a general ring, not every module has a basis. Modules that do have bases are called *free*.

Proposition 3.4. *A free R-module M is isomorphic to the direct sum of "copies" of R.*

Proof. [7] Let X be a basis of M. We consider the family of modules $\{R_x | x \in X\}$ where for each $x \in X$, R_x is R viewed as a module over itself. Let $S = \bigoplus_{x \in X} R_x$. Consider $z \in M$, written uniquely with respect to the basis X as $z = \sum a_x x$ for $x \in X$. Then, define the homomorphism $\phi : M \to S$ by $\phi(z) = (a_x)_{x \in X}$. By the definition of the direct sum, $a_x = 0$ for all but finitely many $x \in X$. Thus $\phi(x) \in S$. Define $\mu : S \to M$ by $\mu(a_x) = \sum a_x x$. Then, μ is a module homomorphism, and is the inverse of ϕ, so ϕ is an isomorphism. □

Given a finitely generated free module M over a commutative ring R, the number of elements in the basis of M is the *rank* of M. Note that when R is a field and M is a vector space, rank is dimension and every vector space of the same rank is isomorphic. This is not the case for general modules.

Example 3.5. Let M and N be free modules over $\mathbb{Z}$, with bases $B_M = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ and $B_N = \left\{ \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \end{bmatrix} \right\}$. Then, $M = \{\begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{Z}\}$, and $N = \{\begin{bmatrix} 2a \\ 2b \end{bmatrix} : a, b \in \mathbb{Z}\}$. If M and N were vector spaces, they would be isomorphic. However, because our scalar multiples are from a ring that does not have multiplicative inverses, N has no vectors with odd-parity entries. Thus, M and N are not isomorphic.

Definition 3.6. [4] A module M over a ring R is *cyclic* if there is an $a \in M$ so that $aR = M$.

The modules described in Example 2.2, $6\mathbb{Z}$ and $12\mathbb{Z}$, are examples of cyclic modules. Note that since we are working with commutative rings, it is not important whether we

express a cyclic module as $M = aR$ or $M = Ra$, but in the case of noncommutative rings, this would be an important distinction.

Modules over special types of rings tend to be particularly interesting. First, we look at modules over integral domains. A characterizing property of an integral domain is the lack of zero divisors, and this property extends to modules over integral domains by *torsion*. Let R be an integral domain and M be an R-module. Then $x \in M$ is a *torsion element* if $rx = 0$ for some nonzero $r \in R$.

Proposition 3.7. *Let M be a module. Then the set T of all torsion elements of M is a submodule of M.*

Proof. The four module axioms are inherited from M, so we need only prove that T is a closed additive abelian group. If $x, y \in T$, then there is some $r_1 \neq 0$ so that $r_1 x = 0$, and some $r_2 \neq 0$ so that $r_2 y = 0$. Then, for $x + y \in M$ and $r_1 r_2 \in R$,

$$\begin{aligned} r_1 r_2(x+y) &= r_1 r_2 x + r_1 r_2 y && \text{by the module axioms for } M \\ &= r_2(r_1 x) + r_1(r_2 y) && \text{by commutativity of } R \\ &= r_2(0) + r_1(0) && \text{by hypotheses} \\ &= 0 && \text{by properties of modules.} \end{aligned}$$

Additionally, we know that $r_1 r_2 \neq 0$, since an integral domain has no zero divisors, so we can conclude that $x + y \in T$. Therefore T is closed, and thus is a submodule of M. □

This submodule is called the *torsion submodule*. If $T = M$, then M is called a *torsion module*. If $T = \{0\}$, M is said to be *torsion free*. Note that free modules are torsion free, but the converse is only guaranteed for modules over principal ideal domains. In fact, there are many special properties of modules over PIDs, which will be explored throughout this report.

Proposition 3.8. *A cyclic torsion R-module T over a PID is isomorphic to a quotient of R:*

$$T \cong R/(r)$$

where r is the order of the element a that satisfies $T = aR$.

Theorem 3.9. [5] Let T be a finitely generated torsion module over a PID R. Then T is isomorphic to the direct sum of cyclic torsion R-modules; that is,

$$T \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$$

for some m with nonzero a_i.

Theorem 3.10. [5] If R is a PID, then every finitely generated R-module M is isomorphic to $F \oplus T$ where F is a finite free R-module and T is a finitely generated torsion R-module, which is of the form $T \cong \bigoplus_{j=i}^{m} R/(a_j)$.

Proof. [5] Let $x_1, \ldots, x_n$ be generators for M. Define a function $f : R^n \to M$ by $f(e_i) = x_i$. Then there is a surjective map $g : R^n \to M$ so that $M \cong R^n/N$. There is also an isomorphism so that $R^n/N \cong \bigoplus_{j=1}^{m} R/(a_j) \oplus R^{n-m}$ for some $m \leq n$ and all $a_j \neq 0$. Then, $\bigoplus_{j=1}^{m} R/(a_j)$ is a torsion module T, and R^{n-m} is a finite free module F, so we conclude that $M \cong F \oplus T$. □

4 Exact Sequences and Splitting Sequences

For the remainder of this report, it will be beneficial for the reader to be familiar with commutative diagrams and diagram chasing. A *commutative diagram* is a directed graph of vertices (which in our case will be modules and groups) and edges (which in our case are homomorphisms), where all directed paths with the same start point and end point yield the same result through function composition. *Diagram chasing* is a proof method that relies on the commutativity and exactness of these diagrams, and the injectiveness or surjectiveness of the functions in diagrams.

Suppose R is a ring, M_1, and M_2, M_3 are R-modules. Then a sequence of module homomorphisms

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$$

is *exact* if $\text{im}(f_1) = \ker(f_2)$. For the remainder of this section, we assume R is a ring and that all sequences are sequences of $R-$module homomorphisms.

A sequence of n module homomorphisms $f_1, \ldots, f_n$ is exact if $\text{im}(f_i) = \ker(f_{i+1})$ for all $1 \leq i \leq n$. An exact sequence of the form

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

is called a *short exact sequence*. Exactness at M_1 implies that $\ker(f_1) = 0$, so f_1 is injective. Exactness at M_2 implies $\text{im}(f_1) = \ker(f_2)$, and exactness at M_3 implies $\text{im}(f_2) = M_3$, so f_2 is surjective.

Following are some fundamental examples of short exact sequences. First, for any R-module M and submodule N, there is a short exact sequence

$$0 \longrightarrow N \xrightarrow{f_1} M \xrightarrow{f_2} M/N \longrightarrow 0$$

where the injective function $f_1 : N \to M$ is defined by $f_1(n) = n$ for $n \in N$, and all elements of M not contained in N have empty pre-images. The surjective mapping $f_2 : M \to M/N$ is defined by $f_2(m) = m + N$, the coset of N with representative m for $m \in M$. Then, it is clear that $\text{im}(f_1) = \ker(f_2)$, since $\text{im}(f_1) = N$, and $n + N = N = 0 + N$ for $n \in N$.

For ideals I and J of a ring R such that $I + J = R$, there is a short exact sequence

$$0 \longrightarrow I \cap J \xrightarrow{f_1} I \oplus J \xrightarrow{f_2} R \longrightarrow 0$$

where $f_1 : I \cap J \to I \oplus J$ is the map $f_1(x) = (x, -x)$, and $f_2 : I \oplus J \to R$ is addition where $\ker(f_2) = \{(x, -x) | x \in I \cap J\}$. This is one example of the involvement of direct sums in exact sequences of module homomorphisms, but there is a more general case involving homomorphisms between any two modules and their direct sum.

Consider two $R-$modules, L and M, and their direct sum, $L \oplus M$. There is a short exact sequence

$$0 \longrightarrow L \xrightarrow{f_1} L \oplus M \xrightarrow{f_2} M \longrightarrow 0$$

where the injective map $f_1 : L \to L \oplus M$ is the embedding of $l \in L$ into $L \oplus M$, and the surjective map $f_2 : L \oplus M \to M$ is the projection of $x \in L \oplus M$ onto M, so that $f_2(f_1(l)) = 0$ for $l \in L$.

REMARK 4.1. [10] Given a sequence of $R-$module homomorphisms

$$\ldots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \ldots$$

we have $\text{im}(f_{i-1}) \subseteq \ker(f_i)$ if and only if the function composition $f_i(f_{i-1}(x)) = 0$ for $x \in M_{i-1}$.

Definition 4.2. [8] A short exact sequence

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

is said to *split on the right* if there is a homomorphism $g_2 : M_3 \to M_2$ so that the function composition $f_2 \circ g_2 = 1$. The sequence *splits on the left* if there is a homomorphism $g_1 : M_2 \to M_1$ so that $f_1 \circ g_1 = 1$. A sequence that splits on the left and the right *splits*, and is called a *splitting sequence*.

Theorem 4.3. The Five Lemma[8] Consider the following commutative diagram where both sequences of homomorphisms are exact:

$$\begin{array}{ccccccccc}
M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\
\downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \downarrow{\scriptstyle h_4} & & \downarrow{\scriptstyle h_5} \\
L_1 & \xrightarrow[g_1]{} & L_2 & \xrightarrow[g_2]{} & L_3 & \xrightarrow[g_3]{} & L_4 & \xrightarrow[g_4]{} & L_5
\end{array}$$

Consider the homomorphisms $h_i, 1 \leq i \leq 5$. If h_1 is surjective, h_2 and h_4 are bijective, and h_5 is injective, we can conclude that h_3 is an isomorphism.

Proof. [8] We make two separate claims that together form *The Five Lemma*:

CLAIM 1. *If h_2 and h_4 are surjective and h_5 is injective, then h_3 is surjective.*

CLAIM 2. *If h_2 and h_4 are injective and h_1 is surjective, then h_3 is injective.*

To prove (1), consider $x \in L_3$. Then $g_3(x) \in L_4$, and thus $g_3(x) = h_4(y)$ for some $y \in M_4$ since h_4 is surjective. Then, $g_4(g_3(x)) = g_4(h_4(y)) = 0$ by exactness at L_4. Since the diagram is commutative, we have $g_4(h_4(y)) = h_5(f_4(y))$. Therefore $g_4(g_3(x)) = h_5(f_4(y)) = 0$. Since $h_5(f_4(y)) = 0$, $f_4(y) \in \ker(h_5)$, and h_5 is injective, we know that $f_4(y) = 0$.
Then $y \in \ker(f_4) = \text{im}(f_3)$ by exactness at M_4. Thus $y = f_3(a)$ for some $a \in M_3$. Because the diagram is commutative, we use diagram chasing and substitutions to see that $g_3(x) = h_4(y) = h_4(f_3(a)) = g_3(h_3(x))$. Then, $x - h_3(a) \in \ker(g_3) = \text{im}(g_2)$. We let $x - h_3(a) = g_2(b)$ for some $b \in L_2$. Since h_2 is surjective, $b = h_2(m)$ for some $m \in M_2$, and by commutativity, $x - h_3(a) = g_2(b) = g_2(h_2(m)) = h_3(f_2(m))$. Thus, $x - h_3(a) = h_3(f_2(m))$, so $x = h_3(a + f_2(m))$. Therefore $x \in \text{im}(h_3)$, and since x is abritrary, h_3 is surjective.

To prove (2), we suppose $a \in \ker(h_3)$. By commutativity, we have $g_3(h_3(a)) = h_4(f_3(a))$. Since $a \in \ker(h_3)$, $h_4(f_3(a)) = g_3(0) = 0$. Since h_4 is injective, $f_3(a) = 0$. Thus $a \in \ker(f_3) = \text{im}(f_2)$, so $a = f_2(z)$ for some z. Then $0 = h_3(a) = h_3(f_2(z)) = g_2(h_2(z))$. Thus $h_2(z) \in \ker(g_2) = \text{im}(g_1)$, and $h_2(z) = g_1(u)$. Since h_1 is surjective, $u = h_1(v)$. Then, $h_2(z) = g_1(h_1(v))$. By commutativity, we have $g_1(h_1(v)) = h_2(f_1(v)) = h_2(z)$. Since h_2 is injective, we have that $z = f_1(v)$. Then, $a = f_2(f_1(v)) = 0$ by exactness. Therefore h_3 is injective. □

We are more interested in the version of The Five Lemma that applies to short sequences.

Corollary 4.4. ***The Short Five Lemma*** [8] *We consider a commutative diagram of short exact sequences, as below:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \\ 0 & \longrightarrow & L_1 & \xrightarrow[g_1]{} & L_2 & \xrightarrow[g_2]{} & L_3 & \longrightarrow & 0 \end{array}$$

It follows directly from The Five Lemma that if h_1 and h_3 are isomorphisms, so is h_2.

Now we can present a condition with which a module is isomorphic to the direct sum of modules.

Theorem 4.5. [6] Let R be a ring, and let M, N, and P be R-modules, with a short exact sequence of the form

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} P \longrightarrow 0$$

Then, the following are equivalent:

(i) There is a homomorphism $f' : M \to N$ so that $f'(f(n)) = n$ for all $n \in N$; the sequence splits on the left.

(ii) There is a homomorphism $g' : P \to M$ so that $g'(g(p)) = p$ for all $p \in P$; the sequence splits on the left.

(iii) There is an isomorphism $\phi : M \to N \oplus P$, and the sequence splits.

We can illustrate this theorem by applying The Five Lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & N & \longrightarrow & N \oplus P & \longrightarrow & P & \longrightarrow & 0 \end{array}$$

Then, we can see that $M \cong N \oplus P$, and we have some insight into the structure of the original exact sequence. We can regard f as the embedding of N into M, and g as the projection of M onto P.

5 Modules Over Principal Ideal Domains

As seen above in the discussion of torsion modules, modules over PIDs exhibit particularly nice properties, especially regarding direct sum isomorphisms. With the goal to introduce the *Fundamental Theorem of Modules over PIDs,* we explore some preliminary propositions.

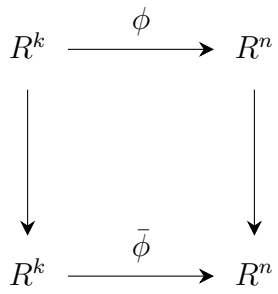
Proposition 5.1. [10] *Suppose R is a PID. Then every submodule of the module R^n is free with rank less than or equal to n.*

Proof. (By induction on n.) If $n = 1$, then every submodule $M \subseteq R$ is $M = rR$ for some $r \in R$. If $r = 0$, then $M = \{0\} \cong R^0$. If $r = 1$, then $M = rR \cong R^1$. Then, we assume that every submodule of R^{n-1} is free of rank less than or equal to $n-1$ for $n >1$. Let $K \subseteq R^n$ be a submodule, and define $\lambda : R^n \to R$ by $\lambda(a_1, \ldots, a_n) = a_n$ with $a_i \in R$ for $1 \leq i \leq n$. Then λ is a homomorphism where $\ker(\lambda) = R^{n-1} \oplus 0 \cong R^{n-1}$. So $\lambda(K) \subseteq R$, and $\lambda(K) = rR$ for some $r \in R$. If $r = 0$, then $K \subseteq \ker(\lambda) = R^{n-1}$, which implies by the induction hypothesis that K is free of rank less than or equal to $n - 1$. If $r \neq 0$, define $\phi : K \to \lambda(K)$ by $\phi(k) = \lambda(k)$ for $k \in K$. Then ϕ is an R-module epimorphism, and $\ker(\phi) \subseteq R^{n-1}$. By the induction hypothesis, $\ker(\phi) \cong R^m$ for some $m \leq n - 1$. There is an exact sequence

$$0 \longrightarrow \ker(\phi) \longrightarrow K \longrightarrow \lambda(K) \longrightarrow 0$$

where ϕ is the mapping from K to $\lambda(K)$. Since $\lambda(K)$ is free, the sequence splits. Therefore $K \cong \ker(\phi) \oplus \lambda(K) \cong R^m + R \cong R^{m+1}$, with $m + 1 \leq n$. □

Proposition 5.2. [10] *Let R be a PID. Fix integers $1 \leq k \leq n$, and consider R-modules R^k and R^n. Let $\phi : R^n \to R^n$ be a module monomorphism. There is a commutative diagram of group homomorphisms*

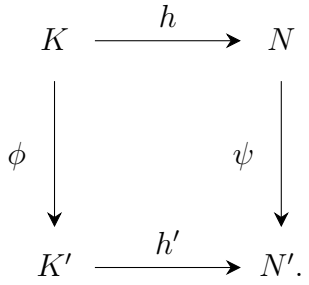


such that the matrix representing the homomorphism $\bar{\phi}$ is diagonal.

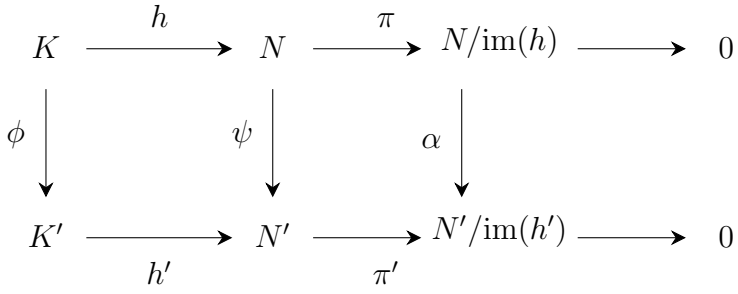
The proof of this proposition is quite involved, but can be viewed in Sean Sather-Wagstaff's *Rings, Modules, and Linear Algebra* ([10]).

We need one more result before we can explore the *Fundamental Theorem.*

Proposition 5.3. [10] *Let R be a ring. Consider the commutative diagram of group homomorphisms*



Then there is a unique module homomorphism $\alpha : N/\mathrm{im}(h) \to N'/\mathrm{im}(h')$ that makes the following diagram commute, where π and π' are the canonical epimorphisms $\pi(x) = x+ \mathrm{im}(h)$ and $\pi'(x') = x'+ \mathrm{im}(h')$ for $x \in N$, $x' \in N'$:



Then, if ψ is surjective, so is α. If ψ is injective and ϕ is surjective, α is injective.

Proof can be found in [10].

Now we are ready to present the final theorem of this report, which follows from these propositions together with Theorem 3.9 and Theorem 3.10 regarding free modules and torsion modules.

Theorem 5.4. The Fundamental Theorem of Modules Over PIDs [10] Suppose R is a PID and M is a finitely generated R-module. Then M is isomorphic to the direct sum of cyclic R-modules,

$$M \cong R/x_1R \oplus \cdots \oplus R/x_kR \oplus R^{n-k}$$

with $x_i \in M$.

Proof. [10] Let $\{m_1, \ldots, m_n\}$ be a generating set for M. Then the map $f : R^n \to M$ defined by $f(r_1, \ldots, r_n) = \sum_i r_i m_i$ is a well-defined surjective group homomorphism that expresses elements of R^n as linear combinations of the generators of M. Because $\ker(f) \subseteq R^n$, Proposition 5.1 yields an isomorphism $\phi : R^k \to \ker(f)$, so $R^k \cong \ker(f)$ for some $k \leq n$. Define $\lambda : \ker(f) \to R^n$ to be the natural inclusion mapping. Then, the function composition of ϕ and λ is $h : R^k \to R^n$. Since ϕ is an epimorphism and λ is a monomorphism, h is a monomorphism. Then, Proposition 5.2 yields a commutative diagram of group homomorphisms

$$\begin{array}{ccc} R^k & \xrightarrow{\quad h \quad} & R^n \\ \downarrow & & \downarrow \\ R^k & \xrightarrow{\quad h' \quad} & R^n \end{array}$$

where the homomorphism h' can be represented by a diagonal matrix; that is, $[h'] = (x_{i,j})$ where $x_{i,j} = 0$ for $i \neq j$. We let $f_1, \ldots, f_n \in \mathbb{Z}^n$ be the standard basis. Then,

$$\begin{aligned} M &\cong R^n/\ker(f) \\ &= R^n/\mathrm{im}(h) \\ &\cong R^n/\mathrm{im}(h') \\ &= R^n/(x_{1,1}f_1, \ldots, x_{k,k}f_k)R \\ &\cong R/x_{1,1}R \oplus \cdots \oplus R/x_{k,k}R \oplus \mathbb{Z}^{n-k}. \end{aligned}$$

□

6 Conclusion

Examining the direct sum of modules is a way to decompose the structure of modules into more basic pieces, so it makes sense to ask the question of when a module is directly decomposable. In order to answer this question, we look at torsion modules, free modules, splitting sequences, and finitely generated modules over principal ideal domains. We have seen that any module with a basis is the direct sum of copies of its base ring, that a splitting sequence of module homomorphisms implies an isomorphism to a direct sum of modules, and that any arbitrary finitely generated module over a principal ideal domain is isomorphic to the direct

sum of cyclic modules. This last result is suggestive of the Fundamental Theorem of Finitely Generated Abelian Groups, which states that any finitely generated abelian group is isomorphic to the direct product of cyclic abelian groups. This is, of course, not a coincidence, as modules are abelian groups, so the the Fundamental Theorem of Modules over PIDs is essentially a generalization of the Fundamental Theorem of Finitely Generated Abelian Groups. Modules are very interesting structures and are a natural topic to study following linear algebra, group theory, and ring theory, as they extend and sometimes generalize the properties of the algebraic structures studied in these fields.

References

[1] Benson Farb and R. Keith Dennis. *Graduate Texts in Mathematics: Noncommutative Algebra.* Springer-Verlag, 1993.

[2] Ivan Fesenko. *Rings and Modules.* University of Nottingham.
https://www.maths.nottingham.ac.uk/personal/ibf/als3/leno.pdf

[3] James P. Jans *Rings and Homology.* Holt, Rinehart and Winston, Inc. 1964.

[4] J Prasad Senesi. *Modules Over a Principal Ideal Domain.* University of California, Riverside.
http://math.ucr.edu/ prasad/PID%20mods.pdf

[5] Keith Conrad. *Modules Over a PID.* University of Connecticut.
http://www.math.uconn.edu/ kconrad/blurbs/linmultialg/modulesoverPID.pdf

[6] Keith Conrad. *Splitting of Short Exact Sequences for Modules.* University of Connecticut.
http://www.math.uconn.edu/ kconrad/blurbs/linmultialg/splittingmodules.pdf

[7] Leonard Evens. *A Graduate Algebra Text.* Northwestern University, 1999.
http://www.math.northwestern.edu/ len/d70/chap5.pdf

[8] Robert B. Ash. *Abstract Algebra: The Basic Graduate Year.* University of Illinois at Urbana-Champaign.
http://www.math.uiuc.edu/ r-ash/Algebra/Chapter4.pdf

[9] Robert Wisbauer. *Foundations of Module and Ring Theory.* Gordon and Breach Science Publishers, Reading, 1991.
http://reh.math.uni-duesseldorf.de/ wisbauer/book.pdf

[10] Sean Sather-Wagstaff. *Rings, Modules, and Linear Algebra.* North Dakota State University, 2011.