Modules: An Introduction

Dylan Poulsen
University of Puget Sound
Math 434

April 28, 2010

Contents

1 Introduction

A module, speaking loosely, is a vector space over a ring instead of over a field. This statement is justified by examining the defining axioms of a module (in this case we define a left R-module since multiplication in the ring R may not be commutative; similar axioms define a right R-module).

Definition. *A **left R-module** M over a ring R with unity 1_R is an abelian group with a scalar product*

$$\cdot : R \times M \to M,$$

where we write $\cdot(\alpha, m) = \alpha \cdot m$, defined for all $\alpha \in R$ and all $m \in M$ satisfying the following axioms.

- $\alpha \cdot (\beta \cdot m) = (\alpha\beta) \cdot m$
- $(\alpha + \beta) \cdot m = \alpha \cdot m + \beta \cdot m$
- $\alpha \cdot (m + n) = \alpha \cdot m + \alpha \cdot n$
- $1_R \cdot m = m$

where $\alpha, \beta \in R$ and $m, n \in M$.

If we examine the definition of a vector space given in Judson [4], we see the above axioms are completely the same with the exception that the field F has been replaced by a ring R. As is often the case in mathematics, a relaxation in defining axioms can lead to unexpected results. When studying linear algebra and vector spaces, for example, we develop a strong intuition for the concepts of linear independence and of bases. This intuition is immediately challenged when studying modules, as the following example illustrates.

1.1 Modules are not always like Vector Spaces

Consider the rational numbers $\mathbb{Q}$ as a $\mathbb{Z}$-module. We can check that $\mathbb{Q}$ is an $\mathbb{Z}$-module by noting that $\mathbb{Q}$ forms an abelian group under addition and by noting the four module axioms hold since for $a, b, c, d, m, n \in \mathbb{Z}$ and for $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$,

- $n\left(m\frac{a}{b}\right) = (nm)\frac{a}{b}$
- $(n + m)\frac{a}{b} = n\frac{a}{b} + m\frac{a}{b}$
- $n\left(\frac{a}{b} + \frac{c}{d}\right) = n\frac{a}{b} + n\frac{c}{d}$
- $1_{\mathbb{Z}}\frac{a}{b} = \frac{a}{b}$

where we use familiar properties of $\mathbb{Z}$ and $\mathbb{Q}$. We will now show that the $\mathbb{Z}$-module $\mathbb{Q}$ does not have a basis, where we use the definitions of linear independence and basis from linear algebra, with vector space replaced by module and scalar field replaced by ring. We will show for any number

of elements in $\mathbb{Q}$, they will not form a basis of $\mathbb{Q}$. A basis for $\mathbb{Q}$ cannot have one element, since if that were so then there would exist an element $a/b \in \mathbb{Q}$,$a, b \in \mathbb{Z}$, $b \neq 0$, such that for some $r \in \mathbb{Z}$,

$$r\frac{a}{b} = \frac{a}{b+1}. \tag{1}$$

This cannot be, however, since equation (1) above implies

$$r(b+1) = b$$

or,

$$r = \frac{b}{b+1}$$

which, since $b \neq 0$, implies $r \notin \mathbb{Z}$, a contradiction. Now, we will show two elements of $\mathbb{Q}$ cannot form a basis of $\mathbb{Q}$. Let $a_1/b_1, a_2/b_2 \in \mathbb{Q}$,$a_1/b_1 \neq a_2/b_2$, with $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and consider for $r_1, r_2 \in \mathbb{Z}$ the relation of linear dependence

$$r_1\frac{a_1}{b_1} + r_2\frac{a_2}{b_2} = 0.$$

If we let $r_1 = b_1a_2$ and let $r_2 = -b_2a_1$, then $r_1, r_2 \in \mathbb{Z}$ and this choice of scalars satisfy the relation of linear dependence above. Therefore any two elements of $\mathbb{Q}$ are linearly dependent, and therefore cannot form a basis for $\mathbb{Q}$. An induction argument shows that any number of elements greater than two in $\mathbb{Q}$ are linearly dependent, and therefore cannot form a basis for $\mathbb{Q}$.

1.2 More Basic Examples

As the above example shows, although the module axioms seem like a minor relaxation in the vector space axioms, the result of this change can be surprising and rich. In fact, many objects which are studied in an introductory abstract algebra course turn out to be modules. For example, an abelian group G with group operation $+$ is an $\mathbb{Z}$-module with scalar multiplication defined as, for $g \in G$ and $n \in \mathbb{Z}$,

$$ng = \begin{cases} \underbrace{g + g + \ldots + g}_{n \text{ times}} \text{ if } n > 0 \\ 0 \text{ if } n = 0 \\ \underbrace{(-g) + (-g) + \ldots + (-g)}_{n \text{ times}} \text{ if } n < 0 \end{cases}$$

where $-g$ is the inverse of g. It can also be shown that left ideals of a ring R are R-modules, and that vector spaces are a special cases of modules when the ring R is actually a field.

1.3 Where We are Going

The primary goal of this paper is to build enough vocabulary and theorems to prove the representation theorem for a finitely generated module over a Principal Ideal Domain (PID). With this in hand, we will be able to show as simple corollaries the structure of finitely generated abelian

groups and the classification of finite vector spaces. We hope that showing major ideas in the abstract algebra course as corollaries to a theorem about modules will demonstrate the worth of studying modules.

2 Predictable yet Necessary Vocabulary

Many definitions about groups, rings and vector spaces carry over naturally to modules, as modules are just a generalization of the three concepts. In this section, we introduce precise definitions which should feel 'natural' to a student of abstract algebra. We start with the definition of a submodule. Just as with groups, rings and fields, when introducing algebraic objects, it is interesting and natural to investigate subsets of the original set which obey the same algebraic properties of the original set. This leads us to the following definition

Definition. *Let R be a ring and let M be an R-module. A subset N of M is an R-**submodule** of M if and only if N is a subgroup of the abelian group of M that is also an R-module with scalar multiplication $\cdot$ defined as it is on M such that $\alpha \cdot n \in N$ for all $\alpha \in R$ and $n \in N$.*

Some examples of submodules include subgroups of an abelian group, which are $\mathbb{Z}$-submodules, as well as ideals of a ring R, where we regard the ring R as an R-module. Since every subgroup of an abelian group is abelian and since every abelian subgroup is normal, we can define a quotient module much like we can form a quotient group.

Definition. *Let R be a ring and let M be an R-module and let N be an R-submodule of M. A **quotient module** M/N is the quotient group of the abelian group of M that is also an R-module with scalar multiplication $\circ$ defined by*

$$\alpha \circ (m + N) = \alpha \cdot m + N$$

for all $\alpha \in R$, $m + N \in M/N$.

We can check that scalar multiplication in the quotient submodule is well defined by noting if $m + N = m' + N$ then $m - m' \in N$ which implies $a \cdot m - a \cdot m' = a \cdot (m - m') \in N$ since N is a submodule and is hence closed under scalar multiplication. Therefore $a \cdot m + N = a \cdot m' + N$. Next, we recall that the concepts of homomorphism and isomorphism are very important in the study of groups, rings, fields and vector spaces. The following two definitions show that module homomorphisms and module isomorphisms behave much like we would expect given our experience with algebra.

Definition. *Let R be a ring and let M and N be R-modules. A function $f : M \to N$ is an R-module homomorphism if and only if the following conditions hold:*

- *$f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$*
- *$f(\alpha \cdot m) = \alpha \cdot f(m)$ for all $\alpha \in R, m \in M$.*

Definition. *Let R be a ring M and N be R-modules and let $f : M \to N$ be an R-module homomorphism. The function f is an R-module isomorphism if and only if f is one-to-one and onto.*

We end this section with the concept of a generator of a submodule. This is a generalization of the span of vectors in linear algebra and the concept of an ideal in ring theory.

Definition. *Let R be a ring, let M be an R-module and let S be an subset of M. We define the* ***submodule of*** *M* ***generated by*** *S by*

$$\langle S \rangle = \{\sum_{i=1}^{n} a_i s_i | n \in \mathbb{N}, a_i \in R, s_i \in S, 1 \leq i \leq n\}.$$

Definition. *Let R be a ring, let M be an R-module and let S be an subset of M. We define the* ***generators of*** *$\langle S \rangle$ to be the elements of S. We say M is* ***finitely generated*** *if and only if $M = \langle S \rangle$ where S is a finite set. Finally, we say M is* ***cyclic*** *if and only if $M = \langle \{m\} \rangle$ for some $m \in M$.*

Definition. *Let R be a ring, let M be a finitely generated R-module and let S be an subset of M. We define the* ***rank*** *of M to be the minimum number of generators of M. We denote the rank of M by rank(M).*

We note that the concept of a cyclic R-module generalizes the concept of a cyclic group since an abelian group is cyclic if and only if it is a cyclic $\mathbb{Z}$-module. We also note that in a PID R regarded as an R-module, every R-submodule has a rank of one since submodules correspond to ideals and since every ideal can be written as a principal ideal.

3 Predictable yet Necessary Theorems

We have the three isomorphism theorems for both groups and rings. Since modules generalize both abelian groups and rings, we expect to have three isomorphism theorems for modules as well. We will state and prove the first isomorphism theorem, which we will use later in this paper, and we will just state the second and third isomorphism theorems for modules since their proofs are similar to the proofs of the second and third isomorphism theorems for groups.

Theorem 1. ***(First Isomorphism Theorem)*** *Let R be a ring and let M and N be R-modules and let $f : M \to N$ be an R-module homomorphism. Then $M/Ker(f) \cong Im(f)$.*

Proof. From the first isomorphism theorem for groups, we have that $\hat{f} : M/\text{Ker}(f) \to \text{Im}(f)$ defined by $\hat{f}(m + \text{Ker}(f)) = f(m)$ is a well defined isomorphism of abelian groups. We just need to verify that $\hat{f}$ is an R-module homomorphism. Note that for all $\alpha \in R$ and for all $m \in M$

$$\hat{f}(\alpha \circ (m + \text{Ker}(f))) = \hat{f}(\alpha \cdot m + \text{Ker}(f)) = f(\alpha \cdot m) = \alpha \cdot f(m) = \alpha \cdot \hat{f}(m + \text{Ker}(f))$$

□

Theorem 2. ***(Second Isomorphism Theorem)*** *Let R be a ring, let M be an R-module and let N and P be R-submodules of M. Then*

$$(N + P)/P \cong N/(N \cap P).$$

Theorem 3. ***(Third Isomorphism Theorem)*** *Let R be a ring, let M be an R-module and let N and P be R-submodules of M with $P \subset N$. Then*

$$M/N \cong (M/P)/(N/P)$$

4 Direct Products

We are working toward a theorem about the representation of finitely generated modules over a PID, which is a generalization of the fundamental theorem of finite abelian groups. Just as we required a notion of the direct product of groups in order to state the fundamental theorem of finite abelian groups, we will also require a notion like a direct product for modules in order to state the representation theorem. This motivates the following definition.

Definition. *Let R be a ring and let $M_1 \dots M_n$ be a finite number of R-modules. Define addition, denoted by $+$, and scalar multiplication, denoted by $\circ$, on the Cartesian product $M_1 \times \dots \times M_n$ by, for $x_i, y_i \in M_i$, $i \in \mathbb{N}$, $1 \leq i \leq n$,*

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

and for $\alpha \in R$

$$\alpha \circ (x_1, \dots, x_n) = (\alpha \cdot x_1, \dots \alpha \cdot x_n)$$

*then the Cartesian product $M_1 \times \dots \times M_n$ is an R-module with addition $+$ and scalar multiplication $\circ$ which we call the **direct sum** of $M_1 \dots M_n$. We denote the direct sum of $M_1 \dots M_n$ by*

$$M_1 \oplus \dots \oplus M_n$$

The following theorem will be useful in the next section

Theorem 4. *Let R be a ring, let M be an R-module, and let $M_1, \dots, M_n$ be submodules of M such that*

- $M = M_1 + \dots + M_n$
- *for $1 \leq i \leq n$,*
$$M_i \cap (M_1 + \dots + M_{i-1} + M_{i+1} + \dots + M_n) = \{0\}$$

then

$$M \cong M_1 \oplus \dots \oplus M_n.$$

Proof. Define a map $f_i : M_i \to M$ by $f_i(x) = x$ for all $x \in M_i$ and let $f : M_1 \oplus \cdots \oplus M_n \to M$ by

$$f(x_1, \ldots, x_n) = f_i(x_1) + \cdots + f_n(x_n) = x_1 + \cdots + x_n.$$

It can easily be shown that f is an R-module homomorphism. By the first condition in the hypotheses, we have that f is onto. Now take $(y_1, \ldots, y_n) \in \text{Ker}(f)$. Then $y_1 + \cdots y_n = 0$, and we have

$$y_i = -y_1 - \cdots - y_{i-1} - y_{i+1} - \cdots - y_n$$

and thus

$$y_i \in M_i \cap (M_1 + \cdots + M_{i-1} + \cdots M_{i+1} + \cdots + M_n) = \{0\}$$

by the second hypothesis. Thus $(y_1, \ldots, y_n) = 0$, so that $\text{Ker}(f) = \{0\}$ and thus f is one-to-one. Therefore f is an isomorphism and the proof is complete. □

5 Free Modules

Recall Example 1.1, where we showed that not every module has a basis. The power of a basis lies in its ability to express an infinite set with a finite collection of elements. This is such a nice property that we will restrict our attention to modules with bases. First, we formalize the language from linear algebra we used in the first example.

Definition. *Let R be a ring and let S be a subset of the R-module M. We say S is **linearly independent over** R if*

$$\lambda_1 x_1 + \ldots \lambda_n x_n = 0$$

implies that $\lambda_i = 0$, where $\lambda_i \in R$ and $x_i \in S$ for $i \in \mathbb{N}$, $1 \leq i \leq n$.

Definition. *Let R be a ring and let S be a finite subset of the R-module M. Then S is a **basis** of M if and only if $M = \langle S \rangle$ and S is linearly independent over R.*

Now that the notion of basis is formalized, we can formalize the notion of a free module.

Definition. *Let R be a ring and let M be an R-module. Then M is **free** if and only if M has a basis.*

We will now show that free modules act a lot like vector spaces, but recall that not every module is free. Suppose that M is a free module with basis v_i, $i \in \mathbb{N}$, $1 \leq i \leq n$. Now examine the submodule generated by v_j, $\langle \{v_j\} \rangle$, for some $j \in \mathbb{N}, 1 \leq j \leq n$. As we have discussed, we can view R as an R-module. Define a function $\phi_j : R \to \langle \{v_j\} \rangle$ by

$$\phi_j(r) = rv_j.$$

We note that ϕ_j is a homomorphism since $\phi_j(a_1 r_1 + a_2 r_2) = (a_1 r_1 + a_2 r_2)v_j = a_1 r_1 v_j + a_2 r_2 v_j = a_1 \phi_j(r_1) + a_2 \phi_j(r_2)$. ϕ_j is in fact an isomorphism since the map is clearly onto and since $\{v_j\}$ is

a linearly independent set, the kernel of ϕ_j is 0, which means the map is one-to-one. Since the v_i generate M, it is the case that $M = \langle\{v_1\}\rangle + \ldots + \langle\{v_n\}\rangle$ and that

$$\langle\{v_i\}\rangle \cap (\langle\{v_1\}\rangle + \cdots + \langle\{v_{i-1}\}\rangle + \langle\{v_{i+1}\}\rangle + \cdots + \langle\{v_n\}\rangle) = \{0\}$$

by the linear independence of the v_i. By Theorem 4, we have that M is a direct sum of the submodules generated by the v_i. But $\langle\{v_i\}\rangle$ is isomorphic to R, which leads to the following interpretation of a free module: *A free module is a direct sum of isomorphic copies of the ring* R. Therefore, we can interpret a free module as a list of n elements of R (relative to a basis), with scalar multiplication and addition performed component-wise, which is exactly how we think of a vector in a vector space.

In linear algebra, a key theorem states that every basis of a vector space has the same cardinality, which allows the dimension of a vector space to be well defined. If we have a commutative ring, or more generally a Noetherian ring, as our underlying ring for our free module, then every basis has the same cardinality, which means it has a well-defined rank. Examples which violate this property exist, but are sufficiently detailed and lengthy to omit.

We conclude the discussion of free modules by noting that given a ring R, any finite R-module N can be expressed as the R-homomorphic image of a free R-module. Take a set of generators $\{y_i | 1 \leq i \leq k, k \in \mathbb{N}\}$ of N (or all of N if a proper subset of generators cannot be found). Now construct a free R-module with k basis elements $\{x_i | 1 \leq i \leq k, k \in \mathbb{N}\}$. Finally, for each i, $1 \leq i \leq k$, map each x_i to each y_i. Applying the first isomorphism theorem to this statement, if we 'mod out' by the kernel of the homomorphism, then any finite R-module is isomorphic to a quotient R-module of a free module.

6 Matrices and Smith Normal Form

Now that we have an interpretation of free modules which agrees with our interpretation of vectors, we naturally want to know if matrices have a 'nice' interpretation in terms of free modules. Just as matrices in linear algebra represent homomorphisms between vector spaces, matrices in the study of modules represent homomorphisms between free modules.

6.1 Example: Turning homomorphisms into matrices

Let R be a ring, let M be a free R-module with $\text{rank}(M) = m$ and basis $\{v_1, \ldots, v_m\}$ and let N be a free R-module with $\text{rank}(N) = n$ and basis $\{w_1, \ldots w_n\}$. Let $f : M \to N$ be an R-module homomorphism. Then for some $j \in \mathbb{N}$,$1 \leq i \leq m$, $f(v_i) \in N$ and therefore can be written as a linear combination of basis elements of N

$$f(v_i) = \sum_{j=1}^{n} a_{ij} w_j$$

where $a_{ij} \in R$. If we let a_{ij} be the entry in row i, column j of a matrix, then we have a matrix representation of the homomorphism.

We note that matrix multiplication as we know it can be viewed as a composition of free R-module homomorphisms if and only if R is commutative. Since commutative rings also have a well-defined rank, we will restrict our attention to commutative rings from now on.

6.2 Motivation for Smith Normal Form

We motivate the Smith normal form with the problem of trying to relate basis elements $\{x_1, \dots x_n\}$ of a free R-module M of rank n to the generators $\{u_1, \dots, u_m\}$ with $m \leq n$ of a finitely generated submodule. The generators of the submodule will naturally have a representation relative to the basis elements. We would like to have a particularly nice form. Just as in linear algebra, we can change bases from $x = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}^T$ to $y = \begin{pmatrix} y_1 & \dots & y_n \end{pmatrix}^T$ with multiplication by an invertible matrix P so that $y = Px$. We can also change the generators from $v = \begin{pmatrix} v_1 & \dots & y_m \end{pmatrix}^T$ to $w = \begin{pmatrix} w_1 & \dots & w_m \end{pmatrix}^T$ with multiplication by an invertible matrix Q. Since the generators are linear combinations of the basis elements, we have that

$$U = AX$$

where A is a matrix of the coefficients of the basis elements in the linear combination. By the definitions above, we have

$$V = QU = QAX = QAP^{-1}Y$$

so the new matrix of coefficients is QAP^{-1}. The crux of Smith normal form is that there is a very nice choice for Q and P such that the new generators relate nicely with the new basis elements. More precisely, The Smith normal form of the matrix of coefficients $B = QAP^{-1}$ has the property that $b_{ij} = 0$ for $i \neq j$ and $b_{ii} = b_i \neq 0$ for $i = j$. Additionally, $b_i | b_{i+1}$ for all i. Therefore each generator is a scalar multiple of a new basis element.

We quickly note that we have to be careful when we say invertible matrix. The inverse of a matrix with entries in a ring R must also have entries in a ring R. Therefore, if we are working with a matrix over the integers, we require the inverse of the matrix to also have entries in the integers. This restricts the invertible matrices over the integers to those with determinant ± 1. In a general integral domain, this restricts the invertible matrices to those with a determinant equal to a unit.

6.3 Smith Normal Form

We now restrict our the attention of our base ring from commutative rings to principal ideal domains. We will show how to obtain the Smith normal form in a PID by an example with the principal ideal domain of the integers. We will not prove that the Smith normal form exists, but our procedure should indicate that the process which we use to obtain the Smith normal form will cease after finitely many steps. We use elementary row and column operators on the matrix to take it into Smith normal form. If we do all the row operations to an identity matrix, and do all the column operators to another identity matrix, we can find the matrices P and Q which change the basis and the generators. Let us assume we have an $\mathbb{Z}$-module M with basis $\{x_1, x_2, x_3, x_4\}$. Let K

be a $\mathbb{Z}$-submodule K generated by v_1, v_2 and v_3 where $v_1 = 2x_1+x_2-3x_4-x_4$, $v_2 = x_1-x_2-3x_3+x_4$ and $v_3 = 4x_1 = 4x_2 + 16x_4$. Then we have the coefficients matrix

$$A = \begin{pmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{pmatrix}.$$

We will now bring A into Smith normal form. We will indicate the operations used and the effects on A and on two identity matrices.

$$\begin{array}{ccccc} & I_3 & & A & & I_4 \\ = & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ \xrightarrow{R_1 \leftrightarrow R_2} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & -3 & 1 \\ 2 & 1 & -3 & -1 \\ 4 & -4 & 0 & 16 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ \xrightarrow{-2R_1+R_2;-4R_1+R_3} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} & \begin{pmatrix} 1 & -1 & -3 & 1 \\ 0 & 3 & 3 & -3 \\ 0 & 0 & 12 & 12 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ \xrightarrow{C_1+C_2;3C_1+C_3;-1C_1+C_4} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 3 & -3 \\ 0 & 0 & 12 & 12 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 3 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ \xrightarrow{-C_2+C_3;C_2+C_4} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 12 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ \xrightarrow{-C_3+C_4} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 0 \\ 0 & -4 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 2 & -2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ = & Q & B & P^{-1}. \end{array}$$

Note that we first brought the smallest integer to the $(1, 1)$ entry, then made every other entry in the 1st row and 1st column equal to zero. We then repeated the process for the $(2, 2)$ entry.It

is straightforward to check that $QAP^{-1} = B$, as desired. We therefore have a new basis for M $\{y_1, y_2, y_3, y_4\}$ and the generators for K are $w_1 = y_1, w_2 = 3y_2$ and $w_3 = 12y_3$. Since the w_i generate K and the y_i, and hence the w_i, are linearly independent, the w_i form a basis for K. Therefore K is a free $\mathbb{Z}$-submodule. It should be no surprise that we implicitly use the Euclidean algorithm in the conversion to Smith normal form, and hence the process can be extended to any Euclidean domain.

7 Structure Theorem for Finitely Generated Modules Over a PID

We now have enough vocabulary and theorems built up to prove the main structure theorem for finitely generated modules over a PID. Once we have this in hand, we will see two known results fall out as corollaries: the fundamental theorem of finite abelian groups and the classification of finite dimensional vector spaces. We begin with a formalization of the consequences of Smith Normal Form.

Theorem 5. *Let R be a PID, let M be a free R-module with rank$(M) = m \geq 1$ and let K be an R-submodule of M. Then K is a free R-submodule and there exists a basis $\{y_1, \ldots, y_m\}$ of M and nonzero scalars $a_1, \ldots a_n \in R$ such that $n \leq m$, $a_i | a_{i+1}$ for $1 \leq i \leq n$, $i \in \mathbb{N}$ and $\{a_1 y_1, \ldots, a_n y_n\}$ is a basis for K.*

We omit the proof of this theorem, but the result should agree with the discussion following the array of row and column operators in the previous section. We now prove the structure theorem for finitely generated modules over a PID.

Theorem 6. *Let R be a PID and let M be a finitely-generated R-module. Then there are ideals $I_1 = \langle a_1 \rangle, \ldots I_n = \langle a_n \rangle$ of R such that $I_n \subset \cdots \subset I_1$ and*

$$M \cong R/I_1 \oplus \cdots \oplus R/I_m.$$

and hence M is a direct sum of cyclic modules.

Proof. By the last paragraph of Section 5, we have that M is the image of a free module N of rank n under the homomorphism f. Let $K = \text{Ker}(f)$ so that K is a submodule of N. By Theorem 5, we have a basis $\{y_1, \ldots y_n\}$ for N and a corresponding basis $\{a_1 y_1, \ldots, a_m y_m\}$ for K, with $m \leq n$ such that $a_i | a_{i+1}$ for $1 \leq i \leq m$. Set $a_j = 0$ for $m \leq j \leq n$. So far we have

$$M \cong N/K \cong \frac{\langle y_1 \rangle \oplus \cdots \oplus \langle y_n \rangle}{\langle a_1 y_1 \rangle \oplus \cdots \oplus \langle a_n y_n \rangle}.$$

Now, consider the homomorphism $\phi : \langle y_1 \rangle \oplus \ldots \oplus \langle y_n \rangle \to \langle y_1 \rangle / \langle a_1 y_1 \rangle \oplus \ldots \oplus \langle y_n \rangle / \langle a_n y_n \rangle$ given by

$$\phi((r_1 y_1, \ldots, r_n y_n)) = (r_1 y_1 + \langle a_1 y_1 \rangle, \ldots, r_n y_n + \langle a_n y_n \rangle).$$

Then clearly $\text{Im}(\phi) = \langle y_1\rangle/\langle a_1y_1\rangle \oplus \cdots \oplus \langle y_n\rangle/\langle a_ny_n\rangle$. We also have that $\text{Ker}(\phi) = (r_1^*a_1y_1, \ldots, r_n^*a_ny_n) \cong \langle a_1y_1\rangle \oplus \cdots \oplus \langle a_ny_n\rangle$ for $r_1^*, \ldots r_n^* \in R$ since

$$\phi((r_1^*a_1y_1, \ldots, r_n^*a_ny_n)) = (r_1^*a_1y_1 + \langle a_1y_1\rangle, \ldots, r_n^*a_ny_n + \langle a_ny_n\rangle) = (0 + \langle a_1y_1\rangle, \ldots, 0 + \langle a_ny_n\rangle).$$

By the first isomorphism theorem, we have

$$N/\text{Ker}(\phi) \cong \frac{\langle y_1\rangle \oplus \cdots \oplus \langle y_n\rangle}{\langle a_1y_1\rangle \oplus \cdots \oplus \langle a_ny_n\rangle} \cong \langle y_1\rangle/\langle a_1y_1\rangle \oplus \cdots \oplus \langle y_n\rangle/\langle a_ny_n\rangle \cong \text{Im}(\phi).$$

We now note that $\langle y_i\rangle/\langle a_iy_i\rangle \cong R/\langle a_i\rangle$ by applying the first isomorphism theorem to the family of maps $\theta_i : R \to \langle y_i\rangle/\langle a_iy_i\rangle$ defined by

$$\theta_i(r) = ry_i + \langle a_iy_i\rangle$$

for $1 \leq i \leq n$. Therefore let $I_i = \langle a_i\rangle$. Then the fact that $a_i|a_{i+1}$ implies $I_{i+1} \subset I_i$ by Lemma 16.7 in Judson [4]. Putting everything together, we have

$$M \cong N/K \cong \frac{\langle y_1\rangle \oplus \cdots \oplus \langle y_n\rangle}{\langle a_1y_1\rangle \oplus \cdots \oplus \langle a_ny_n\rangle} \cong (\langle y_1\rangle/\langle a_1y_1\rangle) \oplus \cdots \oplus (\langle y_n\rangle/\langle a_ny_n\rangle) \cong R/I_i \oplus \cdots \oplus R/I_n$$

where $I_n \subset \cdots \subset I_1$ as desired. □

Corollary 1. *Let V be a vector space of dimension n over a field F. Then since F is a field, it has no proper ideals, so $V \cong F \oplus \cdots \oplus F \cong F^n$. This is the classification of vector spaces according to dimension.*

Corollary 2. *Let $R = \mathbb{Z}$. We have that any finite abelian group (recall that every abelian group is a $\mathbb{Z}-$module) can be written as the direct sum (direct product with Judson's language [4]) of n cyclic groups of the form $\mathbb{Z}/\langle a_i\rangle \cong Z_{a_i}$ which have order a_i, where $a_i|a_{i+1}$ for $1 \leq i \leq n$. This is equivalent to the fundamental theorem of finite abelian groups, as the example below shows.*

7.1 Example of Corollary 2

To find all groups of order $540 = 2^23^35$ (see Judson Chapter 7 Example 3), we note that the order of a direct sum is the product of the individual summands, so a decomposition into a direct sum satisfies $a_1 \ldots a_m = 540 = 2^23^35$ and $a_i|a_{i+1}$ for $1 \leq i \leq m$. Therefore each a_i must be of the form $2^j3^k5^l$ with $0 \leq j \leq 2$, $0 \leq k \leq 3$, $0 \leq l \leq 5$ and the sum of the exponents of 2, for example, in each prime factorization of each a_i, must be 2. This corresponds to choosing partitions of each exponent of each prime. There are two partitions of 2, three partitions of 3 and one partition of 1, so we have $(2)(3)(1) = 6$ possible groups. In the form of the theorem, these groups are given by

$$\mathbb{Z}_{540}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{270}$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_{180}$$

$$\mathbb{Z}_6 \oplus \mathbb{Z}_{90}$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{60}$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{30}$$

which can be reduced to the form given in Judson by noting that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ when $\gcd(m, n) = 1$.

8 Conclusion

Modules are weak generalizations of ideals, abelian groups and vector spaces. Although modules are not always like vector spaces, we found that free modules possessed vector-like properties which made them more familiar. Using the Smith normal form of a matrix over a PID and some basic isomorphism theorems, we were able to prove the structure theorem for finitely generated modules over a PID. This theorem generalizes the classification of vector spaces and the fundamental theorem of finite abelian groups. These are not the only interesting examples that follow from the structure theorem. With some more work, we could view linear transformations from one vector space to another as modules over the polynomial ring $F[x]$, where F is the field of scalars for the vector spaces in question. This leads to many canonical forms, including Jordan canonical form. We hope this introduction has sparked an interest in modules and will motivate the reader to study them further.

9 Bibliography

References

[1] W.A. Adkins and S.H. Weintraub, *Algebra: an approach via module theory*, Graduate Texts in Mathematics, **136**, Springer-Verlag, New York, 1992.

[2] R.B. Ash *Abstract Algebra: The Basic Graduate Year*, `http://www.math.uiuc.edu/~r-ash/Algebra.html`, 2002.

[3] T.S. Blyth *Module Theory: an approach to linear algebra*, Clarendon Press, Oxford, 1977.

[4] T.W Judson *Abstract Algebra: Theory and Applications*, `http://abstract.ups.edu`, 1997.

[5] J. Lambek *Lectures on Rings and Modules*, Blaisdell Publishing Company, Waltham, Massachusetts, 1966.

[6] D. Surowski *Workbook in Higher Algebra*, `http://www.math.ksu.edu/~dbski/book.pdf`, 1992.