Modules Over Principal Ideal Domains

Brian Whetter

April 24, 2014

1 Introduction

This paper has two main goals. The first is to generalize many of the notions of a vector space (learned in a introductory linear algebra course), to modules. The second is to look at modules over Principal Ideal Domains (PID's) specifically, in order to prove a generalized version of the Fundamental Theorem of Finitely Generated Abelian Groups. The paper heavily relies on Joseph Rotman's *Advanced Modern Algebra*, and streamlines the presentation of modules, leaving out material that does not relate directly to our goal. Throughout the paper I will assume the reader has knowledge of basic linear algebra, group, and ring theory.

2 Modules

Here we present many fundamental definitions to modules. Along the way, we will highlight analogous definitions from vector spaces. The first part of the paper will be full of definition, but once in place, we will have a language to generalize our important results from group theory. First though, we must address what a module is.

A module can be thought of as a generalization of a vector space. Instead of requiring a field for scalers however, all that is needed is a ring.

Definition. If R is a commutative ring, then an R-**module** is an abelian group M equipped with a scalar multiplication $R \times M \to M$, denoted by $(r, m) \to rm$, such that the following axioms hold for all $m, m' \in M$ and all $r, r', 1 \in R$:

M1 $r(m + m') = rm + rm'$

M2 $(r + r')m = rm + r'm$

M3 $(rr')m = r(r'm)$

M4 $1m = m$.

Note that according to this definition, a vector space would also be a module, since a field is just a special type of ring. We can also define a module over a ring R which is not commutative, but for the purpose of this paper we will focus only on commutative rings. Additionally, we assume all of our rings have a multiplicative identity.

Example 1. If we let $R = \mathbb{Z}$, and let G be an abelian group, then we can form a $\mathbb{Z}$-module using exponentiation as our scalar multiplication. This example quickly highlights how abelian groups and modules are related.

Example 2. Every commutative ring R is a module over itself where scaler multiplication is just the regular ring multiplication.

Here we give a more exotic example.

Example 3. If k is a field, then $k[x]$ is a commutative ring. We can create a $k[x]$-module related to a linear transformation. Given a linear transformation $T : V \to V$, where V is a finite dimensional vector space over k. Define scaler multiplication $k[x] \times V \to V$ in the following way. Take $f(x) = \sum_{i=0}^{m} c_i x^i \in k[x]$, then

$$f(x)v = \left(\sum_{i=0}^{m} c_i x^i \right) v = \sum_{i=0}^{m} c_i T^i(v)$$

where T^0 is the identity map 1_v, and T^i is the composite of T with itself i times if $i \geq 1$. We now denote V when viewed as a $k[x]$ module by V^T. These modules are important for proving canonical forms of matrices.

Another important notion is similar to the homomorphism of groups or rings.

Definition. If R is a ring and M and N are R-modules, then a function $f : M \to N$ is an R-**homomorphism** or an R-**map** if for all $m, m' \in M$ and all $r \in R$,

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

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

In the case where f is a bijection, we have an R-**isomorphism** and write $M \cong N$. Note that if M and N are vector spaces, and f is a bijection, that this is simply the definition of vector spaces being isomorphic.

Just as there are subspaces of vector spaces, there is the more general submodule of modules.

Definition. If M is an R-module, then a **submodule** N of M, is a subgroup of N of M such that $rn \in N$ whenever $n \in N$ and $r \in R$.

If N is a submodule of M, we write $N \subseteq M$. If $N \neq M$ it is called proper and we write $N \subsetneq M$.

We also have a generalization of a span from linear algebra.

Definition. If M is an R-module and $m \in M$, then the **cyclic submodule generated by m** or $\langle m \rangle$, is

$$\langle m \rangle = \{rm : r \in R\}.$$

If we want to allow for more then one generator, we say the submodule generated by a set X is

$$\langle X \rangle = \left\{ \sum_{\text{finite}} r_i x_i : r_i \in R \text{ and } x_i \in X \right\}.$$

If a module M can be generated by a finite set, it is **finitely generated**. If we think back on the vector space $\mathbb{C}^n$ from linear algebra, it is finitely generated, because it is a finite dimensional vector space. The term finitely generated is really no different, except in this case our scalers are from a ring that is not necessarily a field.

Just like in group theory, or in linear algebra, we have special sets contained in the domain and the codomain of a homomorphism.

Definition. If $f : M \to N$ is an R-map between R-modules, then the **kernel** of f

$$\ker f = \{m \in M : f(m) = 0\}$$

and **image** of f

$$\text{im} f = \{n \in N : \text{there exists an } m \in M \text{ with } n = f(m)\}$$

Just as the kernel forms a subgroup and subring, the kernel of an R-map is a submodule. This naturally leads to quotient modules.

Definition. If N is a submodule of an R-module M, then the **quotient module** is the quotient group M/N (N is normal in M since the underlying group is abelian) with scalar multiplication defined as

$$r(m + N) = rm + N.$$

We omit the proof showing that the multiplication operation is well-defined. The **natural map** $\pi : M \to M/N$ defined as $\pi(m) = m + N$ is analogous to the natural homomorphisms found in group and ring theory. Just like in group and ring theory, there are isomorphism theorems for modules. We prove the first isomorphism theorem to demonstrate how easily it extends from group theory, but do not focus on the others because they are analogous to the group and ring versions.

Theorem 1 (**First Isomorphism Theorem of Modules**). *If $f : M \to N$ is an R-map of modules, then there is a unique R-isomorphism*

$$\phi : M/\ker f \to imf$$

which can be written as

$$\phi(m + \ker f) = f(m).$$

Proof. Since M and N are R-modules, M and N can be seen simply as abelian groups. As abelian groups, we can apply the first isomorphism of groups. Namely, ϕ defined above is a unique isomorphism of groups. We only must check that ϕ is also an R-map. But since f is an R-map, given $r \in R$ and $m, n \in M$ we have

$$\phi(m + n + \ker f) = f(m + n) = f(m) + f(n) = \phi(m + \ker f) + \phi(n + \ker f)$$

and

$$\phi(r(m + \ker f)) = \phi(rm + \ker f) = f(rm) = rf(m) = r\phi(m + \ker f).$$

□

The proof above should illustrate that since groups play a large part in the underlying nature of modules, theorems regarding groups can be easily extended.

Now that we have the isomorphism theorems, we can derive this important fact regarding cyclic modules

Proposition 2. *An R-module M is cyclic if and only if $M \cong R/I$ where I is some ideal.*

Proof. We begin by proving the forward direction. If M is cyclic, then $M = \langle m \rangle$ for some $m \in M$. Recall that from Example 2 that a ring is a module over itself. Now we claim the function $f : R \to M$ defined as $f(r) = rm$ is an R-map. Since M is a module we have

$$f(r + r') = (r + r')m = rm + r'm = f(r) + f(r')$$

and

$$f(rr') = (rr')m = r(r'm) = rf(r').$$

Now note that f is surjective since M is cyclic, and that the kernel of f is some ideal I. So using the first isomorphism theorem of modules, we have $M \cong R/I$.

Now starting from the other direction, we have $R/I \cong M$. But R/I is generated by $1+I$, and so in order to be isomorphic to R/I, M must be cyclic as well. □

Just as there are direct sums of vector spaces, groups, and rings, there is a direct sum for modules.

Definition. If S and T are R-modules, then their **direct sum**, $S \sqcup T$, is the cartesian product $S \times T$ with operations acting on each coordinate. Namely for $s, s' \in S$, $t, t' \in T$ and $r \in R$

$$(s, t) + (s', t') = (s' + t', t + t')$$

and

$$r(s, t) = (rs, rt).$$

Definition. If S and T are submodules of a module M, then M is their **internal direct sum** if $M \cong S \sqcup T$ where

(i) $S + T = M$ and $S \cap T = \{0\}$

(ii) Each $m \in M$ has a unique expression of the form $m = s + t$ where $s \in S$ and $t \in T$.

If these conditions hold, then we write $M = S \oplus T$.

The internal direct sum can be generalized further with the following proposition.

Proposition 3. *Let M be a module and $M = S_1 + \cdots + S_n$ where each S_i is a submodule of M meaning each $m \in M$ can be expressed as*

$$m = s_1 + \cdots + s_n$$

where each $s_i \in S_i$. Then $M = S_1 \oplus \cdots \oplus S_n$ if and only if for each i

$$S_i \cup \langle S_1 + \cdots + \widehat{S_i} + \cdots + S_n \rangle = \{0\}$$

where $\widehat{S_i}$ means S_i has been omitted from the sum.

Proof. See Rotman Proposition 7.19. □

We finish this section on modules by introducing a special type of module that will be useful later when proving properties of modules over PID's

Definition. An R-module F is called a **free R-module** if F is isomorphic to a direct sum of multiple R's. More specifically, given an index set I (which can possibly be infinite)

$$F = \sum_{i \in I} R_i$$

where $R_i = \langle b_i \rangle \cong R$ for all i. A **basis** of F is $B = \{b_i : i \in I\}$. The number of elements in the basis is called the **rank** of F

3 Modules Over Principle Ideal Domains

Now we begin restricting our interests specifically to modules over PID's. The goal is to prove a generalized theorem of the Fundamental Theorem Of Finite Abelian Groups. We start by first restricting ourselves to integral domains, and then eventually, our hypothesis will require a PID as our ring. In anticipation, recall the definition of a PID.

Definition. A **principle ideal domain** or PID, is an integral domain D in which every ideal is principle (so each ideal can be written in the form $\langle a \rangle = \{da : d \in D\}$).

Note also, that any PID is also a unique factorization domain, meaning that any element can be written in terms of irreducible elements, and that this factorization is unique up to multiplication by units.

Now that we have reviewed, we start by first generalizing the idea of order from groups to modules.

Definition. If M is an R-module, and $m \in M$, then its **annihilator** is

$$\text{ann}(m) = \{r \in R : rm = 0\}.$$

If $\text{ann}(m) \neq \{0\}$ then we say m has a finite order, otherwise m has infinite order.

In Proposition 2, we showed that an R-module M is cyclic if and only if $M \cong R/I$ where I is an ideal. Given $m \in M$, we $\langle m \rangle$ is itself a module. Using a similar proof strategy, the map $f : R \to \langle m \rangle$ defined as $f(r) = rm$ is a $\langle m \rangle$-map, and so

$$\langle m \rangle \cong R/\text{ann}(m)$$

since $\text{ann}(m)$ is simply the kernel of f.

Definition. If M is an R-module, and R is an integral domain, then its **torsion submodule** tM is defined by

$$tM = \{m \in M : m \text{ has finite order}\}.$$

Next we need to show that tM is indeed a submodule.

Proposition 4. *If R is an integral domain and M is an R-module, then tM is a submodule of m.*

Proof. Recall that since R is an integral domain, it has no 0 divisors. Now all we must do is show that tM is closed under both addition and multiplication as defined in M. Take $m, m' \in M$, then we know there exists nonzero elements $r, r' \in R$ such that $rm = 0$ and $r'm' = 0$ since m and m' have finite order. Now $rr'(m + m') = 0$, and since there are no 0 divisors, $rr' \neq 0$. So $m + m' \in tM$.

Now take $s \in R$ and $m \in tM$. Then again there exists an r such that $rm = 0$. So

$$r(sm) = (rs)m = (sr)m = s(rm) = 0$$

and so $sm \in tM$ as well. □

Now we define two special types of modules that depend on the annihilator of each element.

Definition. If R is an integral domain and M is an R-module, then M is **torsion** if $tM = M$, or M is **torsion-free** if $tM = \{0\}$.

In other words, a module is torsion if each element has finite order, and torsion free if each element has infinite order.

We now give a method of "moding out" the elements of finite order in a module. We can do this by taking the quotient module of a module M and its torsion submodule tM. If we perform this same process to an isomorphic module, the resulting quotient module will be isomorphic as well. Below we state these ideas more formally.

Proposition 5. *Let M and M' be R-modules, where R is an integral domain.*

(i) *M/tM is torsion-free and*

(ii) *if $M \cong M'$, then $tM \cong tM'$ and $M/tM \cong M'/tM'$*

Proof. Take $m + tM \neq 0$. This means $m \notin tM$ and so m has infinite order in M. Now we assume $m+tM$ has finite order and strive for a contradiction. Since $m+tM$ has finite order, there exists an $r \neq 0$ such that $r(m + tM) = rm + tM = 0$, which would imply $rm \in tM$. But then there exists an $s \in R$ such that $s(rm) = (sr)m = 0$. Since R is an integral domain, $sr \neq 0$, and this would mean m has a finite order, but by assumption it had an infinite order. Thus the order of $m + tM$ must be infinite, and M/tM is torsion free.

Now we prove the second part of the statement. If ϕ is an isomorphism between M and M', then examine $\phi(m)$ where $m \in tM$. Then there exists an $r \in R$ such that $rm = 0$. So $r\phi(m) = \phi(rm) = 0$ since an isomorphism sends 0 to 0 so $\phi(m) \in tM'$. This implies $\phi(tM) \subseteq tM'$. But, similarly $\phi^{-1}(tM') \subseteq tM$, and so ϕ must be a bijection.

Finally, $\bar{\phi} : M/tM \to M'/tM'$ defined by $\bar{\phi}(m+tM) = \phi(m)+tM'$ is an isomorphism. □

Now we are set up to begin proving theorems directly related to the classifying finitely generated modules. First we establish a link between torsion modules and finitely abelian groups. Before giving a precise terminology for how to decompose a module, we need to address the three following statements.

Theorem 6. *If R is a PID, then every finitely generated torsion-free R-module M is free*

Proof. See Rotman, Theorem 9.3. □

Theorem 7.

(i) *If R is a PID, then every finitely generated R-module M is a direct sum*

$$M = tM \oplus F$$

where F is a finitely generated free R-module

(ii) *If M and M' are finitely generated R-modules, where R is a PID, then $M \cong M'$ if and only if $tM \cong tM'$ and* $\operatorname{rank}(tM) = \operatorname{rank}(tM')$.

Proof. See Rotman, Corollary 9.5. □

Proposition 8. *An abelian group G is finite if and only if it is a finitely generated torsion $\mathbb{Z}$-module.*

Proof. Begin by noting that G is referred to in this proof both as a group and a module. But looking back at example 1, it should be clear that this is not a mistake, but a realization that the scalar multiplication from $\mathbb{Z}$ sends elements of G back to elements of G.

Now first assume G is a finite group. In this case, G is obviously finitely generated. Also, from Lagrange's Theorem, we know the order of each element must divide the order of a group. This tells us that the order of each $g \in G$ is finite, and so G must be torsion. (Note here that the order of each element in a group is the same as the smallest nonzero r in the annihilator of M, since R is simply the integers).

Now assume G a finitely generated $\mathbb{Z}$ module, and so $G = \langle x_1 \ldots, x_n \rangle$ where each $x_i \in G$. Then since each x_i is an element of a torsion group, there exists an $d_i \in \mathbb{Z}$ for each x_i such that $d_i x_i = 0$. Then for any $g \in G$, we can write

$$g = m_1 x_1 + \cdots + m_n x_n$$

where $0 \leq m_i < d_i$ for each i. We can then conclude $|G| \leq \prod_i d_i$ which is a finite number. □

Next we define a construct that allows us to break a module down into different components.

Definition. Let R be a PID and M be and R-module. If $P = \langle p \rangle$ is a nonzero prime ideal in R, then M is $\langle p \rangle$-**primary** if for each $m \in M$, there is an $n \geq 1$ such that $p^n m = 0$. M's $\langle p \rangle$-**primary component** is

$$M_p = \{m \in M : p^n m = 0 \text{ for some } n \geq 1\}.$$

Now we can properly state an important decomposition theorem. Its proof is nearly identical to the analogous theorem for finite abelian groups, but translated into the language of modules.

Theorem 9 (**Primary Decomposition of Modules**)**.** *Every finitely generated torsion R-module M, where R is a PID, is a direct sum of its P-primary components. More succinctly,*

$$M = \sum_P M_P$$

Proof. If $m \in M$ is nonzero, it gives rise to an order ideal $\text{ann}(m) = I \subseteq R$. Since R is a PID, this means $I = \langle d \rangle$ where d for some $d \in R$. Since R is a PID, it is also a UFD, and so we we can uniquely factor d. This means that there are positive exponents e_i such that

$$d = p_1^{e_1} \cdots p_n^{e_n}$$

where each p_i is irreducible and no two are associates. Since p_i is irreducible, $\langle p_i \rangle = P_i$ is a prime ideal for each i. Now define $r_i = d(p_i^{e_i})^{-1}$, then $p_i^{e_i} r_i = d$. Now

$$p_i^{e_i}(r_i m) = (p_i^{e_i} r)m = (d)m = 0$$

and so $r_i m \in M_{P_i}$ for each i. By the way each r_i was constructed, they have no common factor, and so $\gcd(r_1, \ldots, r_n) = 1$. Drawing upon knowledge of UFD's, we can then write 1 as a linear combination of the r_i's. Namely there are elements $s_1, \ldots, s_n \in R$ such that $1 = \sum_i s_i p_i$. Then using the fact that each r_i are in ideals P_i and m can be distributed, we get

$$m = \sum_i s_i r_i m \in M_{P_1} + \cdots + M_{P_n}.$$

We have now shown that each element in M can be written in terms of the primary components. What lefts to be shown is that we have a direct sum. According to Proposition 3, all we must do to complete the proof is show that

$$M_{P_i} \cap H_i = \{0\}$$

where $H_i = M_{P_1} + \cdots + \widehat{M_{P_i}} + \cdots + M_{P_n}$. Assume $m \in M_{P_i} \cap H_i$, we will try and show $m = 0$. Let $m \in M_{P_i} \cap H_i$, then $m \in M_P$ and so there exists an $l \geq 0$ such that $p_i^l m = 0$. But because $m \in H_i$ as well, there exists a $u = p_1^{g_1} \cdots \widehat{p_i^{g_i}} \cdots p_n^{g_n}$ such that $um = 0$. But since p_i^l and u are relatively prime, there exists elements $s, t \in R$ such that $sp_i^l + tu = 1$. Now

$$m = (sp_i^l + tu)m = sp_i^l m + tum = 0$$

since $p_i^l m$ and um are each equal to 0. □

The next proposition establishes that if two modules are isomorphic, then the components of their decomposition (given in Theorem 9), are also isomorphic.

Proposition 10. *Two finitely generated torsion modules M and M' over a PID are isomorphic if and only if $M_P \cong M'_P$ for every nonzero prime ideal P.*

Proof. We start with the forward direction. Let $f : M \to M'$ be an R-map. If we take $m \in M_P$ where $P = \langle p \rangle$, then $p^k m = 0$. So because f is an R-map,

$$p^k f(m) = f(p^k m) = f(0) = 0$$

which implies $p^k f(m) \in M'_P$. This means for each P, $f(M_P) \subseteq M'_P$. Since f is an isomorphism, f^{-1} is as well, and a similar argument gets $f^{-1}(M'_P) \subseteq M_P$. This implies M_P and M'_P are isomorphic.

Alternatively, if we have $M_P = M'_P$ for all P, then we can define an isomorphism between M and M'. Let ϕ_p denote the isomorphism between M_P and M'_P. Then using our primary decomposition (Theorem 9), we can define $\phi : M \to M'$ as

$$\phi(m) = \phi\left(\sum_P m_P\right) = \sum_P \phi_P(m_P).$$

□

Now we are finally able to give our main result.

Theorem 11 (**Basis Theorem**). *If R is a PID, then every finitely generated module R-module M is a direct sum of cyclic modules in which each cyclic summand is isomorphic to R or is primary.*

Proof. Given a module R-module, M, we can apply Corollary 7 (i) to write $M = tM \oplus F$ where F is a finitely generated free R-module. Now we only need to focus on the tM part of M. But tM is trivially a finitely generated torsion module. So we can apply our decomposition theorem (Theorem 9) to write $tM = \sum_P tM_P = \sum_P M_P$ since M_P is already torsion. What remains to be shown is that each M_P is a cyclic module (see Rotman Theorem 5.18 for the analogous proof for abelian groups). □

Corollary 12. *Each finitely generated abelian group is a direct sum of cyclic groups , each of prime power order or infinite.*

Proof. This quickly follows from the fact that $\mathbb{Z}$ is a PID. So in the particular case where R in Theorem 11 is $\mathbb{Z}$, our $\mathbb{Z}$-module is the same from Example 1, where scaler multiplication is simply exponentiation. In this case, a module M is p-primary if for each $m \in M$ there is an $n \geq 1$ such that $m^{p^n} = 0$, or in the language of groups, each m has prime power order. □

Note Corollary 12 is equivalent to Judson's statement of the Fundemental Theorem of Fundemental groups. Note that a direct sum of modules, is a direct product of groups.

Theorem 13 (**Judson: Fundamental Theorem of Finitely Generated Abelian Groups**). *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1^{\alpha 1}} \times \mathbb{Z}_{p_2^{\alpha 2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where the p_i's are primes (not necessarily distinct).

As a final note, we mention Rotman gives a different formulation of the Fundamental Theorem of Finitely Generated Groups/Modules that is actually slightly stronger. The exact formulation requires additional vocabulary (namely elementary divisor).

Theorem 14 (**Rotman: Fundamental Theorem of Finitely Generated Modules**). *If R is a PID, then two finitely generated R-modules are isomorphic if and only if their torsion submodules have the same elementary divisors and their free parts have the same rank.*

The basic intuition here, is that two finitely generated modules are isomorphic only if their decompositions are the same (up to permuting the orders).

Conclusion

The first section of this paper was devoted to introducing basic definitions of modules and highlighting the analogous properties to vector spaces, a familiar notion from a basic linear algebra course. When a ring R is a field, a vector space is merely a special type of module. Submodules become subspaces, R-isomorphisms become vector space isomorphisms etc. Additionally, many of the theorems from groups such as the isomorphism theorems also apply to modules. In fact, many groups can be viewed as modules directly.

The second half of the paper focused on developing specific knowledge regarding modules of PID's to create a generalization of the Fundamental Theorem of Finitely Generated Abelian Groups. Although generalizing is an end in and of itself in mathematics, the generalized theorem also has important results. Theorem 14, when applied to $k[x]$-modules (as in Example 3), can be used to derive rational and Jordan canonical forms.

References

1 *Advanced Mordern Algebra* by Joseph Rotman

2 *Abstract Algebra theory and applications* by Thomas Judson