# FINITELY GENERATED MODULES OVER A PRINCIPAL IDEAL DOMAIN

BENJAMIN LEVINE

Abstract. We will explore classification theory concerning the structure theorem for finitely generated modules over a principal ideal domain and its consequences such as the Fundamental Theorem for Finitely Generated Abelian Groups and the Jordan Canonical Form for Matrices. We will explore the invariant factor form of the structure theorem for finitely generated modules over a principal ideal domain and relate it to the elementary divisor form of the structure theorem. We will also investigate the properties of principal ideal domains and unique factorization domains.

## Contents

## 1. Introduction

In this paper, we are interested in classifying finitely generated modules over a principal ideal domain and two of its special cases, specifically the fundamental theorem of finitely generated abelian groups and the Jordan canonical form theorem. We will use the fact that principal ideal domains are unique factorization domains to derive the elementary divisor form of the structure theorem and the Jordan canonical form theorem in sections 4 and 5 respectively. We will be able to find all of the abelian groups of some order $n$.

## 2. Principal Ideal Domains

We will first investigate the properties of principal ideal domains and unique factorization domains.

**Definition 2.1.** A **principal ideal domain** (**PID**) is an integral domain in which every ideal is **principal**. An ideal is **principal** if the ideal can be generated by a single element.

We assume that given an integral domain $R$ in the rest of the section.

**Examples 2.2.** : All ideals of $\mathbb{Z}$ are principal. Principal ideal domains include any field $k$ and the polynomial ring $k[x]$.

**Proposition 2.3.** *Let $R$ be a PID. Then, every nonempty set of ideals of $R$ has a maximal element.*

*Proof.* Let $S$ be the set of all proper ideals of $R$. It follows that $S$ is non-empty and it is partially ordered by inclusion. Let $I_1 \subseteq I_2 \subseteq ...$ be an arbitrary increasing chain of ideals in $S$. Let I=$\bigcup_n I_n$. Since the chain of $I_n$'s are nonempty, it follows that $I$ is nonempty. $I$ is an ideal. Since $R$ is a PID, $I = (a)$. We find that $a \in I = \bigcup_n I_n$ so $a \in I_n$ for some $n$. We get $I_n = I_{n+1} = ....$ Each chain of ideals has an upper bound. By Zorn's lemma, the nonempty set of $I'_n s$ of $R$ has a maximal element, the maximal ideal containing $I$. □

**Definition 2.4.** Let $r$ be a nonzero element of $R$ that is not a unit. The element $r$ is called **irreducible** in $R$, if whenever $r = ab$ with $a, b \in R$, at least one of $a$ or $b$ must be a unit in $R$. Otherwise, $r$ is **reducible**.

**Definition 2.5.** A nonzero element $p \in R$ is called **prime** if the ideal $(p)$ generated by p is a prime ideal.

We can relate the property of a prime element of a principal ideal domain with an irreducible element in a principal ideal domain through the following proposition.

**Proposition 2.6.** *In a Principal Ideal Domain, a nonzero element is prime if and only if it is irreducible.*

To prove Proposition 2.6, we will first prove the following lemma.

**Lemma 2.7.** *In an integral domain, a prime element is always irreducible.*

*Proof of Lemma 2.7.* If $p$ is a prime element, then $(p)$ is a prime ideal. Let $(p)$ be some arbitrary nonzero ideal such that $p = ab$ where $a, b \in R$. Clearly, $ab = p \in (p)$. By the definition of a prime ideal, it follows that either $p$ divides $a$ or $p$ divides $b$.

Without loss of generality, suppose $a \in (p)$. Then, $a = pm$ where $m \in R$. We see that $a = pm = abm$ so $bm = 1$. It follows that $b$ is a unit. Therefore, we have shown that in a integral domain a prime element is always irreducible. □

*Proof of Proposition 2.6.* Since a principal ideal domain is an integral domain, we can claim that any nonzero prime element in a principal ideal domain is irreducible from lemma 2.7.

Let $B$ be some arbitrary ideal that contains $(p)$. By assumption, $B = (b)$ is a principal ideal. Since $B$ contains $p$, $p \in (b)$. We can write $p = br$ where $r \in R$. Suppose that $p$ is irreducible. Then, either $b$ or $r$ must be a unit. This means that we will get $(b) = (p)$ or $(b) = (1)$. $(p)$ must be maximal. Since all maximal ideals in a principal ideal domain are prime ideals, it follows that $(p)$ must be a prime ideal. □

**Definition 2.8.** Two elements $a$ and $b$ differing by a unit are said to be **associates** in $R$ (i.e. $a = ub$).

**Definition 2.9.** A **unique factorization domain** (**UFD**) is an integral domain $R$ in which every nonzero element $r \in R$ that is not a unit has the following two properties:

(1) $r$ can be written as a finite product of irreducibles $p_i$ of $R$ (not necessarily distinct): $r = p_1 p_2 ... p_n$ and

(2) this decomposition is unique up to associates: if $r = r_1 r_2 ... r_m$ is another factorization of $r$ into irreducibles, then $m = n$ and there is some renumbering of the factors so that $p_i$ is associate to $r_i$ for $i = 1, 2, ..., n$.

**Proposition 2.10.** *Every Principal Ideal Domain is a Unique Factorization Domain.*

*Proof of Proposition 2.10.* First we show that the decomposition exists. Let $R$ be a arbitrary principal ideal domain. Suppose $\sum$ is the set of all elements in $R$ that do not admit a finite decomposition into a finite product of irreducibles. If $\sum$ is empty, we are done (for the existence part). If not, by Proposition 2.3, there is a maximal element $x$ in $\sum$ (in the sense the ideal generated by $x$ is maximal among all the ideals generated by a single element in $\sum$). By the assumption on $\sum$, $x$ cannot be irreducible (otherwise it has a decomposition into a finite product of irreducibles, namely $x = x$). So $x$ is reducible and we may write $x = yz$ with $y$, $z$ both not units. So $(x) \subsetneqq (y)$ and $(x) \subsetneqq (z)$. By maximality of $x$ in $\sum$, we have $y \notin \sum$ and $z \notin \sum$. So $y$ and $z$ can be written as finite products of irreducibles; as a result, $x$ can be written as a finite product of irreducibles, a contradiction. So $\sum$ must be empty and thus every $x \in R$ can be decomposed into a finite product of irreducibles.

Then, we show that the decomposition is unique up to associates in $R$ by induction on $m$ prime ideals. If $r = p$ where $p$ is a prime ideal, then it follows that another decomposition of $r$ will be the same since there is only one factorization of $r$. Assume, by way of the inductive hypothesis, that uniqueness holds for $m$ prime factors. Suppose $r_1...r_m r_{m+1} = r = u_1 p_1 ... p_n$. By the definition of a prime ideal, $r_{m+1}$ must divide one of the $p_i^{\prime} s$ on the right hand side so $r_{m+1} = u_1 p_i$. After cancelling the term $r_{m+1}$ on the left hand side, it follows from our inductive hypothesis that decomposition is unique up to associates for $m$ prime ideals. Hence, induction holds. □

We will now turn our attention toward the Chinese Remainder Theorem for Modules. This theorem will help us derive one form of the Structure Theorem for Finitely Generated Modules over a Principal Ideal Domain.

## 3. Chinese Remainder Theorem for Modules

As the name suggests, the Chinese remainder theorem is about remainders or residue classes. In number theory, the Chinese remainder theorem helps us find numbers that have the same remainder modulo $p_1$ and $p_2$ where $p_1$ and $p_2$ are relatively prime. Instead of remainders, we focus on residue classes or equivalence classes when describing the Chinese Remainder Theorem for Modules.

Assume that all rings in the rest of this paper have an identity element.

**Definition 3.1.** Let $R$ be a ring. A **left R-module** over $R$ is a set $M$ together with

1. a binary operation + on M under which M is an abelian group
2. an R-action on M (this is a map $R \times M \to M$) denoted by rm which satisfies the following:
   - (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 $r, s \in R$,$m \in M$, and
   - (d) 1m=m, for all $m \in M$.

**Definition 3.2.** Let $M$ be an $R$-module. A **R-submodule** of $M$ is a subgroup $N$ of $M$ that is closed under the action of the ring elements.

**Examples 3.3.**
1. Abelian groups, which are the same thing as a $\mathbb{Z}$-module
2. The field $\mathbb{R}$ is a $\mathbb{R}$-module, $\mathbb{Q}$-module, and $\mathbb{Z}$-module.
3. The free module of rank $n$ over $R$ as discussed in Example 4.2.

**Definition 3.4.** Let $M$ and $N$ be $R$-modules.

1. A map $\varphi : M \to N$ is an **R-module homomorphism** if the following statements hold:

(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** if $\varphi$ is injective and surjective. If $\varphi : M \to N$ is an $R$-module isomorphism, then the $R$-modules $M$ and $N$ are isomorphic and $M \cong N$.
(3) Let $\varphi : M \to N$ be a $R$-module homomorphism. Define **kernel** of $\varphi$ as the elements of $M$ that map to 0. It can also be denoted as $\ker \varphi = \{m \in M | \varphi(m) = 0\}$. The elements $n \in N$ such that $\varphi(m) = n$ where $m \in M$ is the **image** of $\varphi$.

Note that given any submodule $N$ of $M$, we can form a natural projection $\varphi : M \to M/N$ , which is a $R$-module homomorphism with kernel $N$. See Dummit [3] on pages 348-349 for a statement of this fact (Proposition 3) and a proof.

Note that the isomorphism theorems for groups also hold for modules. The first isomorphism theorem for modules is obtained from the first isomorphism theorem for abelian groups and by observing that the action of $R$ behaves as we expect.

**Theorem 3.5** (The First Isomorphism Theorem for Modules)**.** *Let $M$ and $N$ be $R$-modules and let $\varphi : M \to N$ be an $R$-module homomorphism. Then, $\ker \varphi$ is a submodule of $M$ and $M/\ker \varphi \cong \varphi(M)$.*

Not only can we generalize the first isomorphism theorem of groups to modules, but we can also generalize the idea of generators of a group to generators of a module.

**Definition 3.6.** Let $M$ be an $R$-module.

(1) Suppose $A \subset M$. Let $RA = \{\sum_{i=1}^{n} r_i a_i | r_i \in R, a_i \in A \text{ where } 1 \leq i \leq n\}$. If $A$ is a finite set such that $A = \{a_1, ..., a_n\}$, then $RA$ can be written as $Ra_1 + Ra_2 + ... + Ra_n$. $RA$ is the submodule of $M$ that is generated by $A$. If there is a submodule $N$ such that $N = RA$, then $A$ is the **set of generators** of the submodule $N$.
(2) A submodule $N$ of $M$ is **finitely generated** if there exists a finite subset $A \subset M$ such that $N = RA$.

We are ready to prove the following the statement, which will help us prove the Chinese remainder theorem for modules.

**Proposition 3.7.** *For any ideal $I$ of $R$, let $IM = \{\sum_{finite} a_i m_i | a_i \in I, m_i \in M\}$ be the collection of all finite sums of elements of the form $am$ where $a \in I$ and $m \in M$. (Note that $IM$ is a submodule of $M$). Let $A_1, A_2, ...., A_k$ be any ideals in the ring $R$. Then, the map*

$$M \to M/A_1M \times ...... \times M/A_kM$$

$$defined\ by\ m \mapsto (m + A_1M, ....., m + A_kM)$$

*is an $R$-module homomorphism with kernel $A_1M \cap A_2M \cap .... \cap A_kM$.*

*Proof.* Let $\varphi : M \to M/A_1M \times ...... \times M/A_kM$ be a map defined by $m \mapsto m + A_1M, ....., m + A_kM$. We can rewrite this as $\varphi(m) = [m]$ where $[m] \in M/A_iM$.

We will show that this is a $R$-module homomorphism.

(1) Let $x, x' \in M$. We know $\varphi(x + x') = [x + x']$=$[x]$ + $[x']$ by the definition of a equivalence class. It follows that $\varphi(x + x') = \varphi(x) + \varphi(x')$.

(2) Let $r \in R$ and $x \in M$. Then, $\varphi(rm)$=$[rx]$=$r[x]$. Since $r[x] = r\varphi(x)$, it follows that $\varphi(rx) = r\varphi(x)$.

Since (1) and (2) hold, it follows that $\varphi$ is an $R$-module homomorphism. Next, we show that $\varphi$ is a map with kernel $A_1M \cap A_2M \cap ... \cap A_kM$.

Since $A_1M \cap A_2M \cap ... \cap A_kM$ represents the smallest submodule generated by the ideals $A_1, A_2, ..., A_k$, it follows that if we choose some arbitrary element $i \in A_1M \cap A_2M \cap ... \cap A_kM$ we get $\varphi(i) = [0]$. Hence, $A_1M \cap A_2M \cap ... \cap A_kM \subseteq \ker\varphi$. Let $x$ be an arbitrary element of $\ker\varphi$. Then, $\varphi(x) = [0]$. This means that each of the residues in the direct product must equal 0. That is, $\varphi(x)$ must be contained in $A_1M$, $A_2M$, ..., $A_kM$. Therefore, $x \in A_1M \cap A_2M \cap ... \cap A_kM$. $\ker\varphi \subseteq A_1M \cap A_2M \cap ... \cap A_kM$. It follows that kernel of $\varphi$ is $A_1M \cap A_2M \cap ... \cap A_kM$. □

**Definition 3.8.** The ideals $A_1, ..., A_j$ are **pairwise comaximal** if $A_i + A_j = R$ for all $i \neq j$.

Now, we are ready to state and prove the Chinese Remainder Theorem for Modules.

**Proposition 3.9.** *Assume further that the ideals $A_1, ...., A_k$ are pairwise comaximal. Then,*

$$M/(A_1....A_k)M \cong M/A_1M \times ..... \times M/A_kM.$$

*Proof.* We will prove this by induction on $k$ by showing that $\varphi$ in the previous problem is surjective and $A_1M \cap A_2M \cap ... \cap A_kM = (A_1....A_k)M$. We know from proposition 3.7 that $\varphi$ is a $R$-module homomorphism with kernel

$$A_1M \cap A_2M \cap ... \cap A_kM.$$

We start with our base case, $k = 2$. We will use the fact that the ideals are pairwise comaximal. Let $A$ and $B$ be two arbitrary pairwise comaximal ideals. Then, there must exist some elements

$$x \in A \; and \; y \in B \; such \; that \; x + y = 1.$$

It follows that $x \equiv 1 \; mod \; B$ and $y \equiv 1 \; mod \; A$.

Choose some arbitrary element $(m_1 \; mod \; AM, m_2 \; mod \; BM) \in M/AM \times M/BM$. We want to show that $\varphi$ is surjective for $n = 2$ by showing that $m_2x+m_1y$ maps to $(m_1 \; mod \; AM, m_2 \; mod \; BM)$.

$$\varphi(m_2x + m_1y) = \varphi(m_2x) + \varphi(m_1y)$$

since $\varphi$ is a well defined $R$-module homomorphism. We get $\varphi(m_2x) + \varphi(m_1y) = m_2\varphi(x) + m_1\varphi(y)$. Then, $m_2\varphi(x) + m_1\varphi(y) = m_2(0, 1) + m_1(1, 0)$. By the definition of $\varphi$ and multiplication, we get

$$(0, m_2 \; mod \; BM) + (m_1 \; mod \; AM, 0)$$

$$= (m_1 \; mod \; AM, m_2 \; mod \; BM)$$

, which is exactly what we wanted. Hence, $\varphi$ is surjective.

Since $(AB)M \subseteq AM$ and $(AB)M \subseteq BM$, $ABM \subseteq AM \cap BM$. Let $m \in AM \cap BM$. Then,

$$m = am_1 = bm_2$$

where $a \in A, b \in B$ and $m_1, m_2 \in M$. Then, $m = 1 \cdot m = (x + y) \cdot m$

$$= xm + ym = xbm_2 + yam_1 \in ABM.$$

So $ABM = AM \cap BM$. By Theorem 3.5, it follows that $M/(AB)M \cong M/AM \times M/BM$. We use induction and the case of the product of two ideals. We will let $A = A_1$ and $B = A_2 \times ... \times A_k$.

**Inductive Step** Assume that for all $i \in \{2, ...., k\}$, there exists elements $x_i \in A_1$ and $y_i \in A_i$ such that $x_i + y_i = 1 = (x_2 + y_2) \dots (x_k + y_k)$. Due to addition of residue classes, we know that $x_i + y_i \equiv y_i \; mod \; A_1$. This means that $(x_2 + y_2)...(x_k + y_k) \in A_1 + (A_2...A_k)$. Using this fact and Theorem 3.5, it follows that $M/(A_1....A_k)M \cong M/A_1M \times ..... \times M/A_kM$ by induction.

□

This basic understanding of quotient modules, module theory, and the Chinese Remainder Theorem will help us understand and prove the main result of the paper, the Structure Theorem for Finitely Generated Modules over a Principal Ideal Domain.

## 4. Finitely generated modules over a principal ideal domain

**Definition 4.1.** An $R$-module $F$ is **free** on a subset $A$ of $F$ if for all $x \in F$ which are nonzero, there exists unique $r_1, ...., r_n \in R$, which are all nonzero, and there exists unique $a_1, a_2, ...., a_n \in A$ such that $x = r_1 a_1 + ..... + r_n a_n$ holds for $n \in \mathbb{Z}^+$. $A$ forms a **basis** or a **set of generators** in $F$. $|A|$ is the **rank** of $F$.

**Example 4.2.** Suppose we have a ring $R$. Let $n$ be a natural number. An example of a free module is $R^n$, which has a rank $n$ over $R$.

**Definition 4.3.** Let $N$ be some submodule of $M$. The **annihilator** of $N$ in $R$ is set

$$\{r \in R | rn = 0 \; for \; all \; n \in N\}.$$

In particular, the annihilator of $N$ is a two-sided ideal in $R$.

**Definition 4.4.** An element $m$ of an $R$-module is called a **torsion** element if $rm = 0$ for some nonzero $r \in R$. The set of torsion elements is given by

$$Tor(M) = \{m \in M | rm = 0 \text{ for some nonzero r } \in R\}.$$

It is easy to see that $Tor(M)$ is a $R$-submodule of $M$. If we let $R$ be an integral domain, then it follows that $r \in R$ has no zero divisors. Suppose we let $x, y \in Tor(M)$. Then, $Tor(M)$ is nonempty since $0 \in$ Tor(M). Let $r, s \in R$ be nonzero such that $rx = 0$ and $sy = 0$. Therefore, it follows that $rs(x + y) = 0$. Since $R$ is an integral domain, $rs \neq 0$ so $x + y \in Tor(M)$. If $t \in R$ is arbitrary, then $r(tx) = t(rx) = 0$ so $tx \in Tor(M)$. It follows that $Tor(M)$ is a submodule of $M$.

**Definition 4.5.** A submodule $N$ of $M$ is called a **torsion submodule** if $N \subset Tor(M)$.

**Theorem 4.6.** *Let $R$ be a Principal Ideal Domain, let $M$ be a free $R$-module of finite rank $n$ and let $N$ be a submodule of $M$. Then, $N$ is a free module of rank at most $n$.*

*Proof.* Let's use induction on the rank $n$ of $M$. Suppose that $n = 1$. Then, $M \cong R$. Since $N$ is a submodule of $M$, $N$ must be a principal ideal, say $(\alpha)$. If $\alpha = 0$, then it follows that $N = 0$ and $N$ must have a free rank of 0. Suppose that $\alpha \neq 0$. Then, we can construct an $R$-module homomorphism $r \mapsto r\alpha$, which is an $R$-module isomorphism $R \cong N$. Showing that the homomorphism is surjective and injective follows immediately. $N$ is free on one generator $(\alpha)$. Hence, $N$ is free of rank 1 so the base case holds.

Assume, by way of induction, that the theorem holds for all modules whose free rank is at most $n - 1$. Let $x_1, x_2, ..., x_n$ be any basis of a free $R$-module $M$. Define a surjective natural projection homomorphism $\pi_n : R^n \to R$ with operations $(x_1, ...., x_n) \mapsto x_n$. The kernel of the homomorphism is a submodule that consists of all n-tuples $(x_1, ..., x_{n-1}, 0)$. It is a free submodule with $n - 1$ free generators. Suppose we restrict the domain of $\pi_n$ to $N$,i.e., $\bar{\pi_n}\restriction_N : N \to R'$ where $R' \subseteq R$. Clearly, $\ker \bar{\pi_n}$ is a submodule of the $\ker \pi_i$. Since $R' \subset R$ is free, we can say that $N \cong \ker \bar{\pi_n} \oplus R'$. Since the restriction map can have at most n-1 free generators in the kernel and 1 free generator in the image of $\bar{\pi_n}$, it follows that $N$ can have a free rank of at most $n$.

□

**Theorem 4.7.** *Let $R$ be a Principal Ideal Domain, let $M$ be a free $R$-module of finite rank $n$ and let $N$ be a submodule of $M$. Then, there exists a basis $y_1, y_2, y_3, ...., y_n$ of $M$ such that $a_1y_1, ...., a_my_m$ is a basis of $N$ where $a_1, ...., a_n$ are elements of $R$ with the divisibility relation $a_1|a_2|....|a_n$*

*Proof.* We will follow the proof of Theorem 4.7 in a similar manner as in Dummit [3] on pages 460-462. Assume $N \neq 0$. Suppose we have an $R$-module homomorphism that maps our module $M$ to $R$. We know from definition that the image $\varphi(N)$ of the submodule $N$ is a $R$-submodule of $\varphi(M)$ and is an ideal. Since every ideal in $\varphi(N)$ is principal, it follows that $\varphi(N)$=$(a_\varphi)$ where $a_\varphi \in R$. We can take the set $\sum = \{(a_\varphi)\text{where } \varphi \in Hom_R(M, R)\}$, which gives us the set of all principal ideals of all $R$-module homomorphisms from $M$ to $R$. This set is nonempty since $0 \in \{(a_\varphi)\text{where } \varphi \in Hom_R(M, R)\}$. Using proposition 2.3, let $u$ be an $R$-module homomorphism such that $a_u$ is maximal. Let $a_u = a_1$ be this maximal element. Let $w$ be a generator of $N$ that maps to a generator $a_u = a_1$ under the homomorphism $u$: $u(w) = a_1$.

We want to show that $a_1$ is nonzero. Let $x_1, ..., x_n$ be any basis of the free $R$-module $M$. Let $\pi_i$ be an arbitrary $R$-module natural projection homomorphism defined by $\pi_i(x_1, ...., x_i, ..., x_m) = x_i$. Since $N \neq 0$, there must exist an $i$ such that $\pi_i(N) \neq 0$. Since $a_1$ is maximal and $\sum$ contains more than the trivial ideal, $a_1$ is nonzero.

Next, we will show that $a_1$ generates $\varphi(w)$ for all $R$-modules $\phi$ that map from $M$ to $R$. Let $d$ be a generator of the principal ideal generated by $\varphi(w)$ and $a_1$. Then, $d = r_1a_1 + r_2\varphi(w)$ where $r_1, r_2 \in R$. If we let $\phi = r_1a_1 + r_2\varphi$ be an $R$-module homomorphism, we get $\phi(w) = d$ so $d \in \phi(w)$. It follows that $(d) \subseteq \phi(N)$. Since $(a_1) \subseteq (d) \subseteq \phi(N)$ and $a_1$ is maximal, $d$=$a_1$. Therefore, $a_1$ generates $\phi(w)$.

Since $a_1$ divides any $R$-module homomorphism that maps from $M$ to $R$, $a_1$ divides any natural projection $R$-module homomorphism $\pi_i(x)$ where $1 \leq i \leq n$. Let $\pi_i(w) = a_1b_i$ where $b_i \in R$ with $1 \leq i \leq n$. Define $w_1 = \sum_{i=1}^{n} b_ix_i$. From our natural projection, we realize that $w = a_1w_1$. Since $a_1 = u(w) = u(a_1w_1) = a_1u(w_1)$, we get $u(w_1) = 1$.

To show that $u_1$ is a basis vector of $M$ and $a_1u_1$ is a basis vector for $N$, we will prove the following claims:

(1) $M = Rw_1 \oplus \ker u$
(2) $N = Ra_1w_1 \oplus N \cap \ker u$

We will first show $M = Rw_1 \oplus \ker u$. Let $x \in M$ such that $x = u(x)w_1 + (x - w_1u(x))$. We get $x - w_1u(x) = x - u(x)w_1$. $x - w_1u(x) \in \ker u$ because

$$u(x - w_1u(x)) = u(x) - u(w_1)u(x) = u(x) - u(x) = 0.$$

Any element in our module $M$ can be written as a sum of elements in $Rw_1$ and $\ker u$. We need to verify uniqueness. That is, we will show that the only element that lies in the intersection of $Rw_1$ and $\ker u$ is 0. Suppose that $rw_1$ (an element of $Rw_1$) is also an element of $\ker u$. Since $0 = u(rw_1) = ru(w_1) = r$, 0 is the only element that belongs to the intersection of $Rw_1$ and $\ker u$. We have proven that $M = Rw_1 \oplus \ker u$.

Next, we will verify (2) using a similar procedure as in (1). Since $a_1$ generates $u(x')$ for any $x' \in N$, we can write $u(x')$ as a multiple of $a_1$. Let $u(x') = ca_1$ where $c \in R$. Using a similar decomposition as in (1), we get $x' = u(x')w_1 + x' - u(x')w_1 = ca_1w_1 + (x' - ca_1w_1)$. We get $x' - ca_1w_1 \in N \cap \ker u$ because

$$u(x' - ca_1w_1) = u(x') - ca_1u(w_1) = ca_1 - ca_1(1) = 0.$$

We will finally show uniqueness using a similar procedure as the first claim. Suppose that $ra_1w_1$ (an arbitrary element of $Ra_1w_1$) is an element of the $N \cap \ker u$. Then, we find that

$$\begin{aligned} 0 &= u(ra_1w_1) \\ &= ra_1u(w_1) \\ &= ra_1. \end{aligned}$$

Since $a_1$ is a nonzero maximal ideal, it follows that $r$=0. Hence, we have shown that $N = Ra_1w_1 \oplus (N \cap \ker u)$.

Let's use induction on $n$, i.e. the rank of $M$. Since $\ker u$ has rank less than $n$, it follows that $\ker u$ is a free module. Since $M = Rw_1 \oplus \ker u$, it follows that the free rank of $\ker u$ is $n-1$. Assume by way of induction that $\ker u$ is a module that has a submodule $N \cap \ker u$. Then, there exists a basis $w_2, w_3, ...., w_n \in \ker u$ such that $a_2w_2, ...., a_nw_n$ is a basis of $N \cap \ker u$ where $a_2, ..., a_m \in R$ under the assumption that $a_2|a_3|...|a_n$. It follows from dimension counting of the direct sums in (1) and (2) that $w_1, w_2, ..., w_n$ is a basis for $M$ and $a_1w_1, ...., a_nw_n$ is a basis of $N$.

We will be done if we show that $a_1|a_2$. Suppose $\varphi$ is a homomorphism from $M$ to $R$ such that $\varphi(y_1) = \varphi(y_2) = 1$ and $\varphi(y_i) = 0$ for any $y_i$ with $i$ greater than 2 on a basis of $M$. We find that $\varphi(a_1y_1) = a_1\varphi(y_1) = a_1(1) = a_1$ so $a_1 \in \varphi(N)$. By the definition of a generator, it follows that $(a_1) \subseteq \varphi(N)$.

We obtain the result $\varphi(a_2y_2) = a_2\varphi(y_2)$=$a_2 \cdot 1$=$a_2$ so $a_2 \in \varphi(N)$. By the definition of a generator, it follows that $(a_2) \subseteq \varphi(N)$.

Since $(a_1)$ is maximal (not $a_2$), it follows that $(a_2) \subseteq (a_1)$. It follows immediately by definition that $a_1|a_2$. □

**Proposition 4.8.** *Let $R$ be any ring, let $A_1, A_2, ..., A_m$ be $R$-modules. In addition, suppose that $B_i$ is a submodule of $A_i$, $1 \leq i \leq m$. Then*

$$(A_1 \oplus A_2 \oplus ... \oplus A_m)/(B_1 \oplus B_2 \oplus .... \oplus B_m) \cong (A_1/B_1) \oplus (A_2/B_2) \oplus ... \oplus (A_m/B_m).$$

Note that finite direct sums are the same as finite direct products.

*Proof.* Construct a map $\phi : (A_1 \oplus A_2 \oplus ... \oplus A_m)/(B_1 \oplus B_2 \oplus .... \oplus B_m) \to (A_1/B_1) \oplus (A_2/B_2) \oplus ... \oplus (A_m/B_m)$ whose operations are defined to be $\phi([a_1 + a_2 + .... + a_n]) = [a_1] \oplus [a_2] \oplus .... \oplus [a_n]$ where $[a_i] \in A_i/B_i$. We will first prove that this mapping is a well-defined homomorphism.

Suppose we have $a_1 + a_2 + .... + a_n - a_{n+1} + .... + a_{2n} = b_1 + b_2 + ... + b_n$

By uniqueness of the direct sum, $a_i - a_{n+i} = b_i$. It follows that this map is well defined.

Next, we show that $\phi$ is a homomorphism.

(1) Let $x, y \in \frac{\oplus_{i=1}^n A_i}{\oplus_{i=1}^n B_i}$ such that $x = [\oplus_{i=1}^n a_1]$ and $y = [\oplus_{i=1}^n a_1']$ where $[\oplus_{i=1}^n a_i] \in \frac{\oplus_{i=1}^n A_i}{\oplus_{i=1}^n B_i}$ and $[\oplus_{i=1}^n a_i'] \in \frac{\oplus_{i=1}^n A_i}{\oplus_{i=1}^n B_i}$. It follows that $\phi(x + y) = \phi([\oplus_{i=1}^n (a_i + a_i')]) = \oplus_{i=1}^n [a_i + a_i']$= $\phi([\oplus_{i=1}^n a_i']) + \phi([\oplus_{i=1}^n a_i]) = \phi(x) + \phi(y)$ (by uniqueness of direct sum).

(2) Let $r \in R$ and $x \in \frac{\oplus_{i=1}^n A_i}{\oplus_{i=1}^n B_i}$ such that $x = [\oplus_{i=1}^n a_1]$. If $x = [\oplus_{i=1}^n a_i] \in \frac{\oplus_{i=1}^n A_i}{\oplus_{i=1}^n B_i}$, then $\phi(rx) = \phi([\oplus_{i=1}^n ra_i]) = \oplus_{i=1}^n [ra_i] = r \oplus_{i=1}^n [a_i]$ by the multiplicative property of an equivalence class. We know that $r \oplus_{i=1}^n [a_i] = r\phi([\oplus_{i=1}^n a_i]) = r\phi(x)$.

After having shown that $\phi$ is a $R$-module homomorphism, we check that $\phi$ is an $R$-module isomorphism. The obvious surjection $\oplus_{i=1}^n A_i \mapsto \oplus_{i=1}^n A_i/B_i$ has kernel $\oplus_{i=1}^n B_i$ by easy check. Then, we show that $\phi$ is injective. Suppose that $\phi(a) = \phi([\oplus_{i=1}^n a_i])$=[0]. We know that $[\oplus_{i=1}^n a_i] \in \ker \phi$.

By the definition of an equivalence class, it follows that $\oplus_{i=1}^{n} a_i \in \oplus_{i=1}^{n} B_i$. Then, $[\oplus_{i=1}^{n} a_i] = [0]$. Hence, $\phi$ is injective.

Therefore, we obtain the isomorphism $(A_1 \oplus A_2 \oplus ... \oplus A_m)/(B_1 \oplus B_2 \oplus .... \oplus B_m) \cong (A_1/B_1) \oplus (A_2/B_2) \oplus ... \oplus (A_m/B_m)$. □

**Definition 4.9.** A left $R$ module is a **cyclic submodule C** if there exists an $x \in C$ such that $C = Rx$.

We have the $R$-module homomorphism $\phi : R \mapsto C$ where $\phi(r) = rx$. The map $\phi$ is surjective by easy check.

It follows that $R/\ker\phi \cong C$ from Theorem 3.5. When $R$ is a PID, $\ker\phi = (c)$ is a principal ideal and $C \cong R/(c)$. In particular, $(c)$ is the annihilator of $C$ (which can be verified easily from Definition 4.3).

These facts and definitions allow us to state the structure theorem for finitely generated modules over a principal ideal domain.

**Theorem 4.10.** *(Structure Theorem, Existence: Invariant Factor Form) Let $R$ be a principal ideal domain and let $M$ be a finitely generated $R$-module.*

*(1) $M \cong R^r \oplus (R/a_1) \oplus (R/a_2) \oplus .... \oplus (R/a_m)$ for some integer $r \geq 0$ and nonzero elements $a_1, a_2, ..., a_m$ of $R$ which are not units in $R$ satisfy the divisibility relations $a_1|a_2|....|a_m$.*

*(2) $M$ is torsion free if and only if $M$ is free.*

*(3) In the decomposition in (1), $Tor(M) \cong R/(a_1) \oplus R/(a_2) \oplus ... \oplus R/(a_m)$.*

*Proof.* We will first prove part 1. Let $x_1, ..., x_n$ be our set of generators of $M$ of minimal cardinality (since by assumption $M$ is a finitely generated $R$-module) and $R^n$ has a free $R$-module of rank $n$ such that its basis vectors are $r_1, ...., r_n$.

Construct a homomorphism, say $\varphi$, that maps $R^n$ to $M$, where $\varphi(r_i) = x_i$ for $1 \leq i \leq n$. Essentially, we are mapping a set of generators of $R^n$ to a set of generators in $M$. This map is well-defined.

In order to use Theorem 3.5, we need to show that $\varphi$ is surjective. Since any element of $M$ can be written as a linear combination of its generators, it follows that $\varphi$ is surjective.

Using the First Isomorphism Theorem of modules, we find that $R^n/\ker\varphi \cong M$. It follows from Theorem 4.7 that there exists a basis $u_1, ...., u_n$ for $R^n$ such that we can form a basis for the $\ker\varphi$ consisting of $a_1u_1, a_2u_2, ..., a_mu_m$ where $a_1, ...., a_n \in R$ such that $a_1|a_2|a_3|...|a_m$.

Since $R^n = \oplus_{i=1}^{n} Ru_i$ and $\ker\varphi = \oplus_{i=1}^{n} Ra_iu_i$, we obtain the isomorphism $M \cong R^n/\ker\varphi \cong \frac{\oplus_{i=1}^{n} Ru_i}{\oplus_{i=1}^{m} Ra_iu_i}$.

It follows that we will have a free module in the direct sum. We realize that

$$M \cong \bigoplus_{i=1}^{m} \frac{Ru_i}{Ra_iu_i} \oplus R^{n-m}.$$

It follows that $\frac{Ru_i}{Ra_iu_i} \cong R/(a_i)$ since the $u_i$ generate $R^n$. We get

$$M \cong \oplus_{i=1}^{m} R/(a_i) \oplus R^{n-m}.$$

If any of the $a_i$'s are arbitrary units, it follows that $R/(a_i) = 0$ since $a_i$ generates $R$. We can remove all of the terms where the $a_i's$ are units in the direct sum since each of the modules mod $a_i$ equals 0.

It follows immediately that $R/(a)$ is a torsion $R$-module provided any nonzero $a \in R$. $M$ is free when $M \cong R^r$. $M$ is torsion-free since there are zero torsion $R$-modules. When $M$ is torsion-free,

$Tor(M)$=0. $M$ must be isomorphic to a free module $R^r$ so $M$ must be a free module. Part 2 of Theorem 4.10 holds.

Part 3 of Theorem 4.10 follows immediately from the definition of $Tor(M)$. □

For further purposes such as constructing consequences of the invariant factor form of the structure theorem, we should define an important concept.

**Definition 4.11.** The integer $r$ in Theorem 4.10 is the **free rank** of M. The elements $a_1, a_2, ..., a_m \in R$ (defined up to multiplication by units in $R$) are the **invariant factors** of $M$.

We can use the Chinese Remainder Theorem for Modules to derive another form of the existence part of the fundamental theorem. By decomposing the annihilator $a$ into powers of prime ideals, we can simplify the isomorphism. This simplification is especially useful due to the fact that some of the annihilators can also be zero.

**Theorem 4.12.** *Let $R$ be a PID and let $M$ be a finitely generated $R$-module. We get the following isomorphism:*
$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus .... \oplus R/(p_n^{\alpha_n})$.
*In the above isomorphism, $r \geq 0$ is an integer and $p_1^{\alpha_1}, ...p_n^{\alpha_n}$ are positive powers of primes in $R$.*

Note that some of these primes can be repeated.

*Proof.* Assume Theorem 4.10 is true. We can prove Theorem 4.12 by deriving it from the invariant factor form. Since $R$ is a principal ideal domain, it follows that $R$ is a Unique Factorization Domain. Assume the annihilator $a$ is nonzero. We can write $a = up_1^{\alpha_1}...p_n^{\alpha_n}$ where the $p_i$'s are distinct primes in $R$ and $u$ is a unit. We know from the uniqueness of the prime factorization in a Unique Factorization Domain that the $p_1^{\alpha_1}, ..., p_n^{\alpha_n}$ must be uniquely defined. We want to show that the ideals are pairwise comaximal. If $i \neq j$, $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = (1)$ since distinct primes are coprime to one another. Therefore, we arrive at the result that $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = R$. This means that the ideals generated by powers of distinct primes are pairwise comaximal. $(a) \in ker\varphi$ as defined in Theorem 4.10. We find that $(a)$ must be the least common multiple of the distinct powers of primes since the intersection of all these comaximal ideals is the smallest ideal containing these powers of distinct primes. Using Proposition 3.9, we get $R/(a) \cong R/(u \cap p_1^{\alpha_1} \cap ... \cap p_n^{\alpha_n}) \cong R/(up_1^{\alpha_1} \times ... \times p_n^{\alpha_n}) \cong R/(u) \oplus R/(p_1^{\alpha_1}) \oplus .... \oplus R/(p_n^{\alpha_n})$. Since $R/(u) = 0$ (since $u$ generates $R$), it follows that $R/(a) \cong R/(p_1^{\alpha_1}) \oplus ... \oplus R/(p_n^{\alpha_n})$. Substituting this isomorphism into the invariant factor form, we get $M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus .... \oplus R/(p_n^{\alpha_n})$. □

**Definition 4.13.** Let $R$ be a Principal Ideal Domain and $M$ be a finitely generated $R$-module as in Theorem 4.12. The prime powers $p_1^{\alpha_1}, ..., p_n^{\alpha_n}$ (defined up to multiplication by units in $R$) are the **elementary divisors** of $M$.

We now state the uniqueness part of the structure theorem for finitely generated modules over a principal ideal domain for the invariant factor decomposition.

We first begin with a lemma.

**Lemma 4.14.** *Let $R$ be a PID and let $m$ be a maximal ideal in $R$. Let $F$ denote the field $R/(m)$. Assume that $M$ is free of rank $n$. Then, $M/mM \cong F^r$.*

*Proof.* Let $M$=$R^r$. Create a natural projection homomorphism $\varphi : R^r \to (R/(m))^r$. This is a well defined map with operations $\varphi(\beta_1, ..., \beta_n) = (\beta_1 \text{mod m}, ..., \beta_n \text{mod m})$. The projection is surjective (We leave it to the reader to prove that). In addition, $\varphi(x) = (0, ..., 0)$ whenever all of the $\beta_i$'s are a multiple of $m$. This means that $\varphi$ has kernel $mR^r$, which is an $r$-tuple in which every coordinate of $R^r$ is a multiple of $m$. Using the First Isomorphism Theorem for Modules, we get that $R^r/mR^r \cong (R/(m))^r \cong F^r$. Substituting $M$ for $R^r$, we get $M/mM \cong F^r$. □

**Theorem 4.15.** *Let $R$ be a PID. Two finitely generated $R$-modules $M_1$ and $M_2$ are isomorphic if and only if they have the same free rank and the same list of invariant factors.*

*Proof.* If two finitely generated $R$-modules $M_1$ and $M_2$ have the same free rank and the same list of invariant factors, then it is clear that $M_1$ and $M_2$ are isomorphic.

Suppose that two finitely generated $R$-modules $M_1$ and $M_2$ are isomorphic. Since we can construct an isomorphism from $M_1$ to $M_2$, then $Tor(M_1) \cong Tor(M_2)$. Let $r_1$ be the free rank of $M_1$ and $r_2$ be the free rank of $M_2$. The quotients of $M_1$ and $M_2$ by their torsion parts are free of ranks $r_1$ and $r_2$, and they are isomorphic. So $r_1 = r_2$.

Showing that two finitely generated $R$-modules $M_1$ and $M_2$ that are isomorphic have the same list of invariant factors uses similar logic. Since $M_1 \cong M_2$, $Tor(M_1) \cong Tor(M_2)$. Then, $Tor(M_1) \cong R/(a_1) \oplus ... \oplus R/(a_m) \cong R/(b_1) \oplus ... \oplus R/(b_n) \cong Tor(M_2)$. Since $R$ is a UFD, it follows that the decomposition of $Tor(M_1)$ into the direct sum of cyclic submodules is unique up to associates. As a result, $m = n$ and we can renumber the factors such that the $p_i$'s are associate to the $q_i$'s for $i = 1, ..., n$. Hence, $M_1$ and $M_2$ have the same list of invariant factors. □

Unsurprisingly, there is a uniqueness part of the structure theorem for finitely generated modules over a principal ideal domain for the elementary divisor form.

**Theorem 4.16.** *Let $R$ be a PID. Two finitely generated $R$-modules $M_1$ and $M_2$ are isomorphic if and only if they have the same free rank and the same list of elementary divisors.*

*Proof.* If two finitely generated $R$-modules $M_1$ and $M_2$ have the same free rank and the same list of elementary divisors, then it is clear that $M_1$ and $M_2$ are isomorphic.

We already proved that two isomorphic finitely generated $R$-modules have the same free rank in Theorem 4.15 (Note that a maximal ideal in a principal ideal domain is the same as a prime ideal). See Dummit [3] on page 466 for the induction proof showing that two isomorphic finitely generated $R$-modules have the same list of elementary divisors. □

The structure theorem of finitely generated modules has great implications especially regarding the classification of abelian groups and representation theory. The idea of classifying similar structures such as groups, rings, and fields represents one of the motifs of abstract algebra.

## 5. Consequences of the structure theorem for finitely generated modules over a principal ideal domain

Taking $R = \mathbb{Z}$, we first specialize to prove the fundamental theorem for finitely generated abelian groups.

Suppose we let $n \in \mathbb{Z}$ and $a \in G$ be an arbitrary element of some abelian group.

$$na = \begin{cases} a + a + .... + a \ (n \ times) & n > 0 \\ 0 & n = 0 \\ -(a + a + ... + a) \ (n \ times) & n < 0 \end{cases}$$

There is an action of $\mathbb{Z}$ on $G$. As a result, $na$ is a $\mathbb{Z}$-module. It can be verified easily that abelian groups are the same as $\mathbb{Z}$-modules.

**Theorem 5.1.** *(The Fundamental Theorem of Finitely Generated Abelian Groups) Let $G$ be a finitely generated abelian group. Then the following hold:*

*(1) $G \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_s\mathbb{Z}$ for some integers $r, n_1, n_2, ....., n_s$ that satisfy the following: (a) $r \geq 0$ and $n_j \geq 2$ for all $j$, and (b) $n_{i+1}|n_i$ for $1 \leq i \leq s-1$*

*(2) The expression obtained in (1) is unique: If $G \cong \mathbb{Z}^t \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus .... \oplus \mathbb{Z}/m_u\mathbb{Z}$, where $t$ and $m_1, m_2, ..., m_u$ satisfy (a) and (b) (ie, $t \geq 0, m_j \geq 2$ for all $j$ and $m_{i+1}|m_i$ for $1 \leq i \leq u-1$), then it follows that $t = r$, $u = s$, and $m_i = n_i$ for all $i$.*

*Proof.* Since $G$ is a finitely generated abelian group, it follows that $G$ is a finitely generated $\mathbb{Z}$-module. We know that the ring of integers $\mathbb{Z}$ is a principal ideal domain. When we substitute $\mathbb{Z}$ for $R$ in part 1 of Theorem 4.10, we realize immediately that part (1) of The Fundamental Theorem of Finitely Generated Abelian Groups holds. Note that the division of the invariant factors is reversed from Theorem 4.10 for purposes of finding two isomorphic abelian groups of a given order quickly and efficiently. Part(2) holds as a consequence of Theorem 4.15. □

It is important to note that $\mathbb{Z}^r$ is a free abelian group of rank $r$. In addition, we call the integers $n_1$, $n_2$, ..., $n_s$ the **invariant factors** of $G$.

Suppose we want to find all abelian groups of order 4. There are two abelian groups of order 4: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The list of all the abelian groups of order 4 and their invariant factors is in Table 1.

| Invariant Factors | Abelian Groups |
|---|---|
| $2, 2$ | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ |
| $4$ | $\mathbb{Z}/4\mathbb{Z}$ |

Table 1

The point of the decompositions $M \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_s\mathbb{Z}$ is that the $n_1, ..., n_s$ are unique. For example, $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ since the former has an invariant factor of 4 while the latter has invariant factor 2,2.

Now we apply the structure theorem to the polynomial ring $F[x]$ over a field $F$ to get some application in linear algebra. Let $F[x]$ be a polynomial ring over a field $F$, $V$ be a finite dimensional vector space over a field $F$, $T$ be a linear transformation from $V$ to $V$, and $x$ be a variable.

Since $F[x]$ is a polynomial ring over a field $F$, $F[x]$ must be a principal ideal domain. Clearly, $V$ has free rank 0 as an $F[x]$-module. Since $V$ has finite dimension over $F$, it must be finitely generated as a $F$-module. As a result, $V$ is finitely generated as a $F[x]$-module.

In addition, it is easy to show that the $F[x]$-submodules of $V$ are $T-invariant$ subspaces of $V$ (since $V$ is sent to itself through the ring action of $x$ and $F[x]$-submodules are subspaces of $V$). We will specialize to $F = \mathbb{C}$. We are assuming that $F$ is algebraically closed so that the only prime ideals of $F[x]$ are of the form $x - \lambda$. Letting $R = F[x]$ in Theorem 4.12 (3), we can write the vector space $V$ as a direct sum of finitely many cyclic $F[x]$ modules of the form $F[x]/(x-\lambda)^p$ where $\lambda \in F$.

Multiplication by $x$ defines a linear transformation from $F[x]/(x-\lambda)^p$ to itself. We view a basis of $F[x]/(x-\lambda)^p$ as an $F$ vector space. Let $\{1, \bar{x} - \lambda, ..., (\bar{x} - \lambda)^{p-1}\}$ be a basis of $F[x]/(x-\lambda)^p$.

We will use the fact that $x$= $(x - \lambda) + \lambda$ and $(x - \lambda)^p = 0$ in the following calculations. Multiplication by $x$ defines a linear operator on $F[x]/(x-\lambda)^p$ which transforms the basis as follows:

$$1 \mapsto 1 \cdot \bar{x} = (\bar{x} - \lambda) + \lambda$$

$$\bar{x}-\lambda \mapsto \bar{x}(\bar{x}-\lambda) = ((\bar{x}-\lambda)+\lambda)(\bar{x}-\lambda) = (\bar{x}-\lambda)^2 + \lambda(\bar{x}-\lambda)$$
$$\vdots$$
$$(\bar{x}-\lambda)^{n-2} \mapsto \bar{x}(\bar{x}-\lambda)^{n-2} = ((\bar{x}-\lambda)+\lambda)(\bar{x}-\lambda)^{n-2} = (\bar{x}-\lambda)^{n-1} + \lambda(\bar{x}-\lambda)^{n-2}$$
$$(\bar{x}-\lambda)^{n-1} \mapsto \bar{x}(\bar{x}-\lambda)^{n-1} = ((\bar{x}-\lambda)+\lambda)(\bar{x}-\lambda)^{n-1} = (\bar{x}-\lambda)(\bar{x}-\lambda)^{n-1}) + \lambda(\bar{x}-\lambda)^{n-1} = \lambda(\bar{x}-\lambda)^{n-1}$$

The linear transformation is represented by a square matrix, which is a $n \times n$ **Jordan block** with eigenvalue $\lambda$, of the form

$$A_\lambda = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix}.$$

Suppose the elementary divisors are $(x-\lambda_1)^{p_1}, ..., (x-\lambda_m)^{p_m}$. Since we are taking a direct sum of submodules that are $T$-invariant subspaces of $V$, we can take the union of the bases of each of the Jordan blocks to get a basis of $V$ allowing us to obtain a square matrix:

$$B = \begin{pmatrix} A_{\lambda_1} & & & \\ & A_{\lambda_2} & & \\ & & \ddots & \\ & & & A_{\lambda_m} \end{pmatrix}.$$

This gives us a special case of the Jordan canonical form theorem.

**Theorem 5.2.** *Let $F$ be an algebraically closed field and $B$ be a square matrix with entries in $F$. Then, $B$ is similar over $F$ to a direct sum of elementary Jordan matrices, one for each elementary divisor of $B$. Each elementary divisor of $B$ is a power $(x-\lambda)^e$ of some monic linear polynomial $x-\lambda$; the corresponding matrix summand is the $e \times e$ elementary Jordan matrix with diagonal entries all equal to the scalar $\lambda$.*

**Acknowledgments.** I want to thank my mentors Xiao Wang and Jingren Chi as well as Dr. Laszlo Babai for recommending this research topic as well as recommending abstract algebra books for me to self-study. I wouldn't have been successful without their advice on the paper. I also want to thank Dr. Peter May for his support and mentorship during the REU.

## References

[1] Birkhoff, Garrett, and Saunders 1. MacLane. Algebra. MacLane. New York: Macmillan, 1967.
[2] Broué, Michel. Some Topics in Algebra: An Advanced Undergraduate Course at PKU. Berlin: Springer, 2014. Print.
[3] Dummit, David S., and Richard M. Foote. Abstract Algebra. 3rd ed. N.p.: John Wiley & Sons, 2004